НОВИ ГЛОБАЛНИ БЕЗБЕДНОСНИ ЗАКАНИ:

КОНЦЕПТИ, АКТЕРИ И ИДНИ ПЕРСПЕКТИВИ

Проф. д-р Тања МИЛОШЕВСКА

Проф. д-р Тања МИЛОШЕВСКА

НОВИ ГЛОБАЛНИ БЕЗБЕДНОСНИ ЗАКАНИ: КОНЦЕПТИ, АКТЕРИ И ИДНИ ПЕРСПЕКТИВИ

Скопје, 2025

Проф. д-р Тања МИЛОШЕВСКА

НОВИ ГЛОБАЛНИ БЕЗБЕДНОСНИ ЗАКАНИ: КОНЦЕПТИ, АКТЕРИ И ИДНИ ПЕРСПЕКТИВИ

Рецензенти

Проф. д-р Оливер Бакрески
Институт за безбедност, одбрана и мир, Филозофски факултет – Скопје
Проф. д-р Рина Киркова Танеска
Институт за безбедност, одбрана и мир, Филозофски факултет – Скопје

Издавач
Универзитет "Св. Кирил и Методиј"–Скопје, Филозофски факултет – Скопје

Уредник
Проф. д-р Оливер Бакрески

Техничка обработка
Трајче Милошевски

Лектор
Мартина Жужеловска

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

355.02:005.334]:343.341(100)"20"
343.9:004.8(100)"20"

МИЛОШЕВСКА, Тања
Нови глобални безбедносни закани [Електронски извор] : концепти, актери и идни перспективи / Тања Милошевска. - Скопје : Универзитет "Св. Кирил и Методиј"–Скопје, Филозофски факултет, 2025

Начин на пристапување (URL):
https://repository.ukim.mk/handle/20.500.12188/34410 - Текст во PDF формат, содржи 132 стр. - Наслов преземен од екранот. - Опис на изворот на ден 09.12.2025. - Фусноти кон текстот. - Библиографија: стр. 116-132

ISBN 978-608-238-261-6

а) Безбедносни закани, глобални -- Тероризам -- 21 в. б) Сајберкриминал -- Вештачка интелигенција -- 21 в.

COBISS.MK-ID 67633413

СОДРЖИНА

ВОВЕД

Современата безбедносна средина се карактеризира со сложеност, динамичност и постојана трансформација на формите и методите на закани. Во ерата на глобализацијата, дигитализацијата и брзиот технолошки развој, традиционалните безбедносни концепти се соочуваат со сериозни предизвици што бараат нови пристапи и интегрирани решенија.

Монографијата **„Нови глобални безбедносни закани: концепти, актери и идни перспективи“** има за цел да ги истражи токму овие процеси, преку анализа на современите феномени што го обликуваат безбедносниот пејзаж на 21 век.

Современиот свет се соочува со комплексна и динамична безбедносна реалност во која границите меѓу традиционалните и новите форми на закани се сè повеќе заматени. Глобализацијата, дигиталната трансформација и брзиот технолошки развој создадоа нови можности за напредок, но истовремено и нови ризици што го менуваат карактерот на безбедноста на национално, регионално и меѓународно ниво.

Во таков контекст, концептот на глобална безбедност престана да се сведува само на класичните воени и политички прашања, и денес опфаќа поширок спектар на феномени – од радикализација и насилен екстремизам, преку организиран криминал и кибернапади, до злоупотреба на напредни технологии и нови хибридни облици на закани. Овие процеси го наметнуваат прашањето за способноста на државите, општествата и поединците да се приспособуваат, да предвидуваат и да изградат отпорност кон ризиците што произлегуваат од глобалната меѓузависност.

Безбедноста денес не може да се гледа како статичен концепт, туку како динамичен систем на односи меѓу различни актери – државни институции, меѓународни организации, приватен сектор и граѓанско општество. Сите тие имаат улога во создавањето и одржувањето безбедна и стабилна средина. Притоа, предизвикот не е само да се реагира на заканите, туку да се развие превентивна безбедносна култура, базирана на знаење, доверба и интегриран пристап кон ризикот.

Покрај физичките и територијалните димензии, безбедноста во 21 век има и силна когнитивна, информациска и морална компонента. Манипулацијата со информации, дезинформациските кампањи и злоупотребата на технологијата станаа ефикасни инструменти за дестабилизација и влијание врз јавното мислење, што дополнително ја комплицира глобалната безбедносна слика.

Во вакви околности, се поставува потребата за критичко преиспитување на постојните модели на национална и меѓународна безбедност, како и развивање нови концепти на отпорност, соработка и превенција. Анализата на глобалните безбедносни предизвици денес не е само академска обврска, туку и општествена потреба – бидејќи разбирањето на заканите претставува првиот чекор кон нивно ефективно спротивставување.

Оваа монографија има за цел да придонесе кон продлабочување на научната и стручната дебата за природата, динамиката и идните перспективи на новите глобални безбедносни закани, поттикнувајќи развој на политики и практики што ќе обезбедат стабилност, одржливост и заштита на демократските вредности во еден постојано менлив глобален контекст.

ГЛАВА I

КОНЦЕПТУАЛНА РАМКА ЗА РАДИКАЛИЗАМ И НАСИЛЕН ЕКСТРЕМИЗАМ

Во текот на изминатата деценија, радикализацијата се појави како можна најупорна концептуална рамка за разбирање на модификациите на насилство на микрониво. За насилниот екстремизам и тероризам може да се тврди дека се во функција на општеството – колку што е реалност на екстремистички групи или поединци што се впуштаат во насилство поради идеолошки мотивации. Радикализација преку еволуирање или прифаќање екстремистички верувања што го оправдуваат насилството е еден од можните патишта за вмешаност во тероризмот, но секако не е единствениот. Информираните политики и практики за ублажување и спречување на ширењето на насилниот екстремизам бараат разбирање на овие видови варијации, а не само за општите трендови. Анализата на наративите што ги користат сегашните радикални и насилни екстремистички групи покажува дека социоекономските, политичките и личните незадоволства ефективно се користат за да се поколеба јавното мислење, да се дисеминираат пораки, да се добијат нови регрути и да се поттикнат симпатии. Овие наративи генерално се споени со карактеристични термини вградени во прашања за политичка нестабилност, социоекономска стагнација, граѓански судири и, во некои случаи, војна. Целта на оваа Глава е јасно да се разбере односот помеѓу овие поими, за да може превенцијата од насилство и/или закана од насилство да биде поуспешна.

Радикализацијата кон насилен екстремизам е сложен и повеќеслоен процес што се одвива на различни нивоа (индивидуално, организациско и системско).

Клучен момент во процесот на радикализација е „катализатор настан“ кога личноста станува приемчива за можноста за нови идеи и радикални погледи на светот.

Терористите и радикализираните групи личат на санта мраз. Само мало малцинство радикали користат стратегиско насилство за да привлечат медиумско внимание. Мнозинството екстремисти не се видливи и користат ненасилни методи, кои се поефикасни во остварувањето на нивните наведени цели. Под нивото на „водата“ има база за поддршка што повремено се согласува со дејствата на најпосветените милитанти и уште поголемо „тивко малцинство“ со аверзија кон таргетирање неборци.

Контратероризмот мора да го таргетира видливиот дел од сантата мраз, додека контрарадикализацијата треба да се насочи кон подводниот дел од сантата мраз, кој е многу поголем, а не обратно (Muro, 2016).

Терминологија

(Насилен) Екстремизам

Која било идеологија што се спротивставува на темелните вредности и начела на друштвото. Многумина го разликуваат политичкиот од верскиот екстремизам. Додека насилниот екстремизам може да се поврзе со која било политичка или верска идеологија, поимот обично се изедначува со верскоинспирирано, и особено со насилство што е со недржавна исламистичка основа. На некој начин, ова истражување паѓа во истата замка, бидејќи посебно се фокусира на шаблоните преку кои одредени поединци се радикализираат преку прифаќање на исламските идеологии инспирирани од салафисти/ вахабисти и се приклучуваат на џихадските организации како странски борци во Ирак и Сирија. Меѓутоа, низ целиот процес на истражување експлицитно ги препознавме, и се обидовме да ги откриеме, заедничките интеракции меѓу исламистичкиот насилен екстремизам и другите форми на политички (на пр., екстремно десничарски, националистички) екстремизам, кои придонесуваат кон нивната заемна радикализација (Aroua, 2018).

Иако екстремистите не е неопходно да учествуваат во насилства, фразата насилен екстремизам се користи во контексти кога екстремистичките гледишта се придружени со оправдување и употреба на екстремно насилство (како злосторства) против оние што не го делат истото убедување или идеологија. Насилниот екстремизам може да се изрази од поединци или групи, преку говори или медиумски известувања, преку извршување изолирани дејства на насилство во име на екстремистички идеологии или физичко приклучување кон насилни групи (Aroua, 2018).

Радикализација

Процес на идеолошка и/или бихевиорална промена во пораст што води кон залагање за поекстремни и потенцијално насилни светогледи и дејства.

Поимот „радикализација“ се однесува на процесот во кој едно лице сè повеќе се залага и поддржува екстремистички идеи. Радикализацијата, вообичаено, не резултира само од едно влијание, туку резултира од сложена мешавина на фактори и динамики. Се работи за концепт што е различно толкуван. Во некои случаи, терминот се користи на начин на кој се сугерира имплицитна врска помеѓу радикални идеи и насилство. Ова е проблематично не само од причина што не сите што имаат радикални (или екстремистички) идеи нема да се впуштат или поддржат насилно дејство, туку и поради фактот што тие имаат право да имаат сопствени идеи – без оглед на нивната природа, а тоа е заштитено во меѓународното право како основно човеково право (OSCE, 2019).

Кумулативно/реципрочна радикализација

Поимите „кумулативен“ екстремизам и „реципрочна“ радикализација ја изразуваат забелешката дека сегашната политичка поларизација не се случува во вакуум, но сè почесто е одговор на постапките и дискурсот на друга група, на пример десничарските националистички групи. Ова е од големо значење во јавна расправа што е сè уште склона да ги смета радикализмот и екстремизмот како вродени карактеристики на одредена религија (често исламот).

Отпорност (Непогоденост)

Отпорноста подразбира свесност за проблемот од разни засегнати страни во една заедница и нивно здружено дејствување против одредена појава. Исто така, ги вклучува ставот на заедницата кон таква појава и нивната реакција во пресрет на појавување на дејство на насилен екстремизам или настани перципирани како такви што водат кон неговото појавување. Никогаш не е апсолутно својство, туку системска и променлива карактеристика.

Ранливост (Погоденост)

Погодена заедница е онаа врз која влијаеле идеолошките и/или физичките форми на насилен екстремизам, како што се: продорна радикална идеологија, идеолошки мотивирани насилни дејства, зачестеност/случаи на странски борци што потекнуваат од заедницата и присуство на чинители што ја негуваат ранливоста кон насилен екстремизам (Morina at all, 2019).

Како што е истакнато од Холмер и Бауман (2018), „групите на насилен екстремизам често ги приврзуваат своите агенди кон динамиката на постојан конфликт и бараат прибежиште и можност во средини што се лошо управувани и склони кон конфликти. Разбирањето на главните причини и динамиката што им овозможува на таквите групи да процветаат бара објектив на анализа на конфликти релевантни алатки за анализа на конфликти.

Алатките од макониво што ги испитуваат насилните екстремистички организации, без да ги земат предвид нивните односи со друга конфликтна динамика, ризикуваат да поддржат тесно замислени интервенции за справување/превенирање на насилен екстремизам што немаат влијание и одржливост.“

ОБСЕ има посебна и интенционална терминологија за овие концепти: насилен екстремизам и радикализација што водат кон тероризам. „Радикализација што води кон тероризам“ се однесува на „динамичниот процес во кој едно лице на крајот прифаќа терористичко насилство како можно, па дури и легитимен курс на дејствување. Иако не мора да значи, ова можеби на крајот ќе го наведе лицето да се заземе за терористички активности, да дејствува во нивна поддршка или да се вклучи во нивно извршување“ (OSCE, 2018).

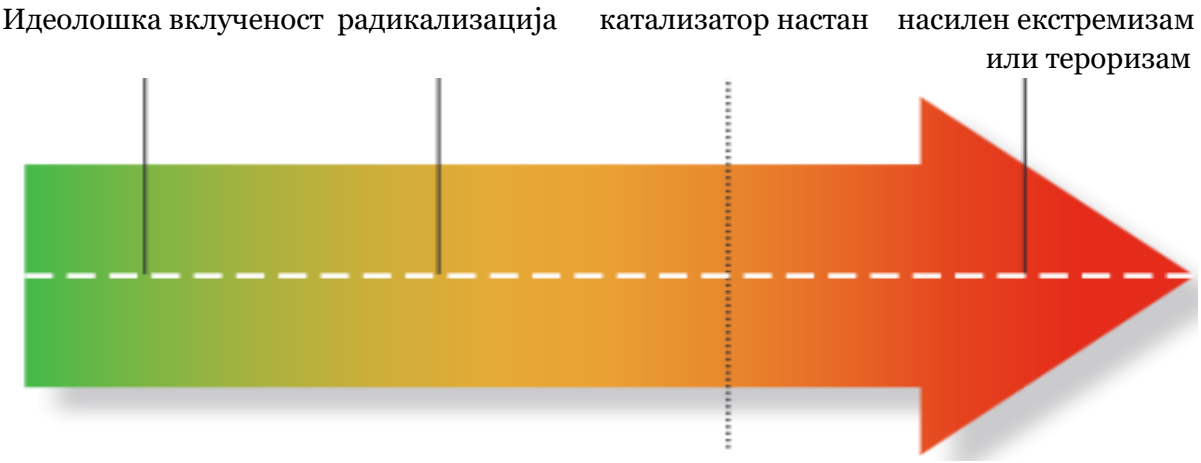
Постојат многу дефиниции за радикализација, но овој труд е конкретно заинтересиран за процесот со кој поединците се „радикализираат до насилство“.

И тоа не на секаков вид насилство, туку на специфичен тип на политичко насилство, имено, нелегитимно насилство насочено против цивили и неборци, познато и како тероризам. Како што тврди Шмид, она што генерално се подразбира под радикализација е „индивидуалниот или групниот процес на растечка посветеност за вклучување во акти на политички тероризам“ (Schmid, 2013). Конечно, работната дефиниција за „насилна радикализација“ е дадена од Експертската група за насилна радикализација на Европската комисија што ја дефинира како „социјализација кон екстремизам што се манифестира во тероризам“ (Expert Group, 2008).

Додека насилната радикализација постепено се префрли на врвот на антитерористичката агенда на ЕУ, таа беше придружена со релативно ембрионално разбирање на процесите и меѓусебното влијание на факторите што придонесуваат за усвојување радикални идеи и однесување. Терминот „радикализација“ беше внесен во дискусијата за политиката по координираните самоубиствени бомбашки напади во Мадрид (2004) и Лондон (2005), кои беа насочени кон цивилите што го користеа јавниот транспортен систем и резултираа со 191 и 52 жртви соодветно. Неколку од напаѓачите во двата инциденти беа домашни терористи што или биле родени или социјализирани во земјата и усвоиле нов идентитет во кој борбите на нивните муслимански татковини одиграле моќна улога во поттикнувањето гнев против Западот. За властите, наскоро стана приоритет да имаат појасна слика за тоа како младите мажи од муслиманско имигрантско потекло се радикализирале на Запад и биле зафатени од заводливата култура на одметник на насилен џихад (Muro, 2016).

Радикализацијата како процес

Единственото нешто за што експертите за радикализација се согласуваат е дека радикализацијата е процес (Schmid, 2013). Како што е наведено на сликата, основното разбирање на овој когнитивен процес ќе повлече постепено усвојување екстремистички идеи и ќе заврши, доколку се заврши, во практиката на насилен екстремизам или тероризам.



Слика: Радикализацијата како процес

Сликата покажува дека радикализацијата најдобро се гледа како процес на промена, лична и политичка трансформација од една состојба во друга. Да се стане радикализиран е постепен процес што бара прогресија низ различни состојби и не се случува ниту брзо, ниту лесно. Така, едно лице не станува радикално преку ноќ иако влијанието на „катализаторниот настан“ може да го забрза процесот. Настанот на катализаторот е опишан од Quintan Wiktorowicz (2004; 2005) како „когнитивно отворање“ што го прави лицето поприемчиво за можноста за нови идеи и погледи на светот. Овој шокантен настан или лична криза ја разнишува сигурноста на поединецот во претходно одржаните верувања, го поттикнува да го преоцени целиот свој живот и да стане отворен за радикална промена на вредностите и однесувањето. Во случајот на терористичките организации ИРА или ЕТА, новите регрути го оправдуваа приклучувањето кон етнонационалистичките терористички групи повикувајќи се на убивање (или мачење) пријатели и роднини од страна на државата, и затоа може да се претпостави дека тероризмот бил чин на одмазда. Во поново време, постојат докази дека криминалците што се приклучиле на џихадистичките организации како ИСИС и ал-Каеда сфатиле дека нивното криминално однесување било штетно и дека треба да прекинат со своето минато и да ги надоместат своите „гревови“. Оваа „точка од која нема враќање“ го обезбеди образложението за нивното вртење кон религијата и ја оправда вмешаноста со салафистите следбеници на ултраконзервативната сунитска гранка на исламот.

Настанот катализатор може да има повеќе форми:

- ✓ економски (губење работа, блокирана општествена мобилност);
- ✓ општествени (отуѓување, дискриминација, расизам);
- ✓ политички (меѓународни конфликти) и
- ✓ лични (смрт на близок).

Дополнително, постои долга листа на предизвикувачи (вистински или согледани) што можат да го иницираат прогресивното движење кон насилен екстремизам.

1.1 Поттикнувачки фактори на насилниот екстремизам

Најпопуларниот приод, досега, за проучување на појавата на насилниот екстремизам е да се групираат основните причини и поттикнувачки фактори во две главни категории:

1) притискачки фактори или структурни услови (пр. сиромаштија, незадоволства, недостаток на пристап до политичките процеси или правдата, долготраен конфликт); и

2) привлекувачки фактори или директни двигатели како што се идеолошки повик или финансиски и социјални придобивки од приклучувањето кон насилна група.

На микрониво, сегашната агенда на истражување на насилниот екстремизам има тенденции да се фокусира на индивидуалните особини на радикализираните млади, на пример, преку истражување на улогата на когнитивните склоности во формирањето маладаптивни, високоризични начини на размислување (Allan et al. 2015; Dandurand, 2015). Објаснувањата на макрониво за структурните причини на насилниот екстремизам се во изобилие. Најчесто цитираните основни причини на насилниот екстремизам опфаќаат политичко угнетување, општествено исклучување, државна репресија, релативна депривација, сиромаштија и глобализација (Dandurand, 2015, Desta, 2016). Овие структурални објаснувања означија поместување од препишување на насилниот екстремизам само или првенствено на верските убедувања. Научниците исто така ја истакнуваат улогата на формирањето на идентитетот како движечка сила за процесите на радикализација (Schmitt, 2017; Search for Common Ground, 2017) и идентификуваат други двигатели како што се родови улоги и чест (Atran, 2006). Исто така истражувана е улогата на образованието, каде што дисфункционалните образовни системи не им овозможуваат на поединците критички да се ангажираат со предочената информација – посебно меѓу малцинските популации. Недостатокот на соодветно верско образование може понатаму да ги поттикне поединците да бараат поедноставена „вистина“ – да се исполнуваат со верски индоктринации за исламот (или други системи на верување) – што му овозможува простор на екстремистичкиот наратив да дејствува.

Форми и манифестирање

Радикализацијата што води кон насилство не е нова појава. Таа може да има различни форми во зависност од контекстот и временскиот период и може да биде поврзана со различни причини или идеологии. Во минатиот век, многу земји страдаа од насилство од различни форми, вклучувајќи, меѓу другото, урбано насилство, појава на насилна супкултура, десно и левичарско екстремистичко насилство, националистичко и религиозно мотивирано насилство. Следниве описи се засноваат на Извештајот на Центарот за спречување на радикализација што води до насилство (2018).

Десничарското екстремистичко насилство е форма на насилна радикализација поврзана со фашизмот, расизмот, врховизмот и ултранационализмот. Оваа форма на радикализација што води до насилство се карактеризира со насилна одбрана на расен, етнички или псевдонационален идентитет, а исто така е поврзана со радикално непријателство кон државните власти, малцинствата, имигрантите и/или левичарските политички групи.

Левичарското екстремистичко насилство е форма на радикализација што води кон насилство што се фокусира првенствено на антикапиталистичките барања и повикува на трансформација на политичките системи што се сметаат за одговорни за производство на социјални нееднаквости, и што на крајот може да користат насилни средства за да ја

унапредат својата кауза. Оваа категорија вклучува анархистички, маоистички, троцкистички и марксистичко-ленинистички групи што користат насилство за да се залагаат за својата кауза.

Политичко-религиското екстремистичко насилство е форма на радикализација што доведува до насилство поврзано со политичко толкување на религијата и одбраната, со насилни средства, на верски идентитет за кој се смета дека е нападнат (преку меѓународни конфликти, надворешна политика, социјални дебати итн.).

Екстремистичкото насилство на едно прашање во суштина е форма на насилна радикализација мотивирана од единствено и специфично прашање. Оваа категорија ги вклучува следните групи доколку користат насилство: радикални групи за заштита на животната средина или правата на животните, движења против глобализацијата, екстремисти против абортусот, насилство поврзано со спорт, одредени антитранс и антифеминистички движења и ултраиндивидуалистички или независни екстремистички движења што користат насилство за да ги промовираат своите каузи. Убијците чии мотиви се делумно или целосно идеолошки може исто така спаѓаат во оваа категорија.

Опсегот на насилни дејства и манифестации што произлегуваат од радикализацијата што доведува до насилство може да варира од вербално насилство до терористички напади, вклучувајќи пожари и оштетување јавни добра, насилни собири, физичка агресија, активности од типот на мафија и убиства. Некои форми на насилство (на пр., вербално насилство) може да бидат почетна фаза и да поттикнат други потешки и опасни форми (на пр., физичко насилство или убиства) (Glaser, 2017).

Траектории и чекори на радикализација што водат кон насилство

Иако постојат различни индивидуални траектории и патеки кон радикализација што водат до насилство, можно е да се идентификуваат шест чекори низ кои може да поминат младите додека се подложени на процесот на насилна радикализација. Патеките на секој човек може да бидат сосема различни, а премините од една до друга можеби не се толку јасни, но овие шест чекори помагаат да се разберат некои од личните патишта кон формирање радикални верувања и свртување кон насилни акти зошто поединци може да се вклучат или да се одделат во процесот на радикализација. Важно е да се нагласи дека не сите поединци што поминуваат преку првите фази го достигнуваат нивото на насилна радикализација. Исто така, можно е да се движите помеѓу „чекорите“ и да се оди напред-назад во овој модел. Моделот Могадам (Moghaddam, 2005, International Centre for the Prevention of Crime, 2015) има за цел да покаже дека радикализацијата што води кон насилство е резултат на многу поголеми процеси во општеството. Не ги опфаќа сите можни форми на насилство – наместо тоа, ги опфаќа важните делови од процесите на радикализација што водат кон насилство.

Траекториите на радикализација што доведува до насилство се артикулирани во овој модел околу следните шест чекори, засновани на метафора на качување по скали до катови на зголемено прифаќање на насилството, и може да помогне во подобро објаснување во која фаза на насилна радикализација се наоѓа лицето, како и кои интервенции да бидат соодветни на секое ниво.

Приземје: Психолошка интерпретација на материјалните и социјалните услови

► Субјективна перцепција на лишеност, неправда, социјална неподвижност.
► Закани за идентитетот.
► Влијание на медиумите кои шират чувство на неправда.

Прв кат: Предвидени опции против нефер третман

Овие опции се:

► перцепција за недостаток или ограничени можности за социјална мобилност и алтернативни начини за подобрување на состојбата,
► перцепција на правните постапки како неправедни и пристрасни.

Овие опции генерираат чувство на неправда и нелегитимност на важечкиот нормативен систем. На тој начин, почувствуваната агресија се проектира кон другиот, кој се смета за одговорен за проблемите, со што се овозможува преминот на вториот кат.

Втор кат: Агресија

Вториот кат се карактеризира со поместување на агресијата, која во оваа фаза е вербална и физичка. Ова се рефлектира со директна или индиректна поддршка на групи или организации што се залагаат и промовираат визија за „ние против нив“.

Трет кат: Морална посветеност

Тоа е чекор каде што насилната група или организација се чини дека го поддржува процесот на ангажирање преку убедување и оправдување на средствата за да се постигне идеално општество. Таа користи тактика на изолација, припадност, доверливост и страв.

Овие организации се позиционирани на две нивоа:

► макониво, како единствена опција за промена на светот или реформирање на општеството;
► микониво, како засолниште за револтираните, незадоволните, маргинализираните и другите луѓе што се наоѓаат во слични ситуации.

Четврти кат: Категорично размислување и легитимност на насилната група или организација – Регрутирање

► Влегување во насилната група или организација и почеток на „тајната“ интрасоцијализација.
► Групата го промовира дихотомното размислување „ние против нив“ и ја зголемува изолацијата.

Петти кат: Насилниот чин и механизмите на инхибиција

Ова е оперативна фаза, каде што поединци се опремени да вршат насилни дејства. Тие ги добиваат потребните ресурси за да ги спречат механизмите што спречуваат преземање насилни дејства:

►социјална категоризација, која се користи за идентификување на целта и на непријателот;

►влошување на разликите помеѓу интрагрупата и дополнителната група;

►спречување каков било механизам на инхибиција (Garcia, Pasic, 2018).

По анализата на облиците и манифестациите на радикализација што доведуваат до насилство, факторите што влијаат и траекториите, може да се заклучи дека не постои апсолутно јасна причинско-последична врска на радикализацијата, туку тоа е сложен процес што е различен за секој случај.

Бидејќи причинско-последичната врска може да се протолкува различно, терминот и логиката на „превенција“ се проблематични од гледна точка на општествените науки. Во оваа смисла, „превенцијата“ во ова истражување попрецизно би значела „адресирање на радикализацијата пред таа да стане насилна“, наместо „да се избегне“ или „да се осигури дека тоа нема да се случи“ (Garcia, Pasic, 2018).

1.2. Инструменти за превенција на насилен екстремизам и рана детекција на радикализација

Постојат многу дефиниции за радикализација, но овој прирачник е конкретно заинтересиран за процесот со кој поединците се „радикализираат до насилство“. И тоа не на секаков вид насилство, туку на специфичен тип на политичко насилство, имено, нелегитимно насилство насочено против цивили и неборци, познато и како тероризам. Како што тврди Шмид, она што генерално се подразбира под радикализација е „индивидуалниот или групниот процес на растечка посветеност за вклучување во акти на политички тероризам“ (Schmid, 2013). Конечно, работната дефиниција за „насилна радикализација“ е дадена од Експертската група за насилна радикализација на Европската комисија што ја дефинира како „социјализација кон екстремизам што се манифестира во тероризам“ (European Commission’s Expert Group on Violent Radicalization (2008).

Како што е истакнато од Холмер и Бауман (2018), „групите на насилен екстремизам често ги приврзуваат своите агенди кон динамиката на постојан конфликт и бараат прибежиште и можност во средини што се лошо управувани и склони кон конфликти. Разбирањето на главните причини и динамиката што им овозможува на таквите групи да се развијат бара објектив на анализа на конфликти и релевантни алатки за анализа на конфликти. Алатките од макрониво што ги испитуваат насилните екстремистички организации, без да ги земат предвид нивните односи со друга конфликтна динамика, ризикуваат да поддржат тесно замислени интервенции за справување/превенирање на насилен екстремизам што немаат влијание и одржливост.“ Во прилог табела со

наведени причини за насилен екстремизам и можни видови интервенции што може да бидат спроведени од страна на општините.

ОБСЕ има посебна и интенционална терминологија за овие концепти: насилен екстремизам и радикализација што водат кон тероризам. „Радикализација што води кон тероризам“ се однесува на „динамичниот процес во кој едно лице на крајот прифаќа терористичко насилство како можно, па дури и легитимен курс на дејствување. Иако не мора да значи, ова можеби на крајот ќе го наведе лицето да се заземе за терористички активности, да дејствува во нивна поддршка или да се вклучи во нивно извршување“ (OSCE, 2018).

ПРИЧИНИ ЗА НАСИЛЕН ЕКСТРЕМИЗАМ	**ВИДОВИ НА ИНТЕРВЕНЦИИ**
СТРУКТУРНИ	
Политички: репресија, политичко исклучување, геополитички настани	✓ Проекти за граѓанство и демократија ✓ Постконфликтно помирување
Културни: дискриминација, стигматизација, идентитетски конфликти	✓ Кохезија на заедницата ✓ Образование и меѓуверски проекти
Социоекономски: економска депривација, нееднаквост	✓ Ублажување на сиромаштијата ✓ Обука и поддршка за вработување
ОПШТЕСТВЕНИ/ГРУПИ	
Групна припадност, потрага по идентитет, перципирана закана по идентитетска група	✓ Спортски и рекреативни проекти ✓ Проекти за зајакнување на младите
ИНДИВИДУАЛНИ	
Авантура, одмазда, статус, материјални стимулации, екстремистичка идеологија	✓ Менторство и советување ✓ Верска писменост
ОВОЗМОЖУВАЧКИ	
Регрутери, социјални мрежи поврзани со екстремистички групи	✓ Упатување и информативни услуги ✓ Контранаративни иницијативи

Табела 4. Причини за насилен екстремизам и видови интервенции

Класификација на насилните екстремисти

Постојат повеќе видови на насилен екстремизам. Европските и другите држави ширум светот беа подложени на различни видови на насилен екстремизам во изминатите децении. Ова насилство беше спроведено од десницата, левичарското насилство и други видови на политичко, социјално, верско и друго идеолошко поврзано насилство. Заедничко за сите овие видови на насилни дејствија е фактот што овие незаконски насилни дејствија се преземаат за да се реализира и/или продолжува одредена идеолошка цел.

Не сите насилни екстремисти имаат исти карактеристики – некои можеби биле осамени актери, додека други можеби биле членови на екстремистичка група – некои можеби имале историја на претходна обука и ангажирање во насилни екстремистички акти, додека други можеби биле уапсени поради планирање да се вклучат во некоја насилна акција во сопствената држава или во странство, без претходно искуство или капацитет во однос на насилни дејства. Некои насилни екстремисти се харизматични лидери, други се следбеници. Некои имаат капацитет да регрутираат, додека други се ранливи на таква активност за регрутирање. Некои насилни екстремисти претходно биле криминални престапници; други немаат познато криминално минато. Разбирањето на овие индивидуални карактеристики е важно за ефективно реагирање на поединечни насилни екстремистички престапници.

Ќе напомнеме дека постојат различни видови класификација на екстремистите, односно постои различна класификација за различни цели. Меѓутоа, како една од поважните класификации на насилните екстремисти во три категории може да ја издвоиме онаа од Советот на Европа (Council of Europe Handbook, 2016):

1) оние што се **идеолози и водачи** и што може да бидат лица за радикализирање;
2) оние што се **следбеници** и се ранливи на зголемена радикализација;
3) оние што се **криминални опортунисти** и заинтересирани за сопствена добивка и се здружуваат со насилни екстремисти со цел на некој начин да се здобијат со лична корист.

Иако дефиницијата за насилен екстремизам вклучува придржување до идеолошки цели, некои поединци се повеќе мотивирани од потрагата по смисла во своите животи, други се принудени од други да се вклучат или можеби имаат потреба од социјална припадност.

Насилниот екстремизам и радикализација претставуваат негирање на демократијата и на човековите права. Чувствата на неправда и фрустрација за нивната социјална исклученост се меѓу главните причини што придонесуваат за ранливоста на младите луѓе и ја зголемуваат нивната подготвеност да се

придржуваат на екстремистички, понекогаш насилни групи, кои нудат очигледна социјална сигурност за нив.

Владата на Северна Македонија формираше комитет што ќе се занимава со ова прашање заедно со стратегија што подоцна ќе биде наречена „Национална стратегија за спречување на насилен екстремизам“ и акциски план што предвидува како различните актери и засегнати страни ќе бидат вклучени во развојот на таквите активности. Националната стратегија на Северна Македонија за спречување на насилен екстремизам дава единствен фокус на превентивните активности и дефинира четири стратегиски приоритети:

1. **Да се превенираат** тековите на странски терористички борци и милитанти и коренитите причини за радикализација и екстремизам;
   Цели:
- ✓ Зајакнати институционални капацитети,
- ✓ Подигнување на јавната свест,
- ✓ Силна и отпорна заедница,
- ✓ Спречување на радикализација преку интернет.

2. **Да се заштитат** граѓаните, нивниот имот, клучната и критичната инфраструктура од јасни и присутни, како и потенцијални и растечки закани;
   Цели:
- ✓ Проактивни институции во контекст на заштита на основните вредности, човековите права и слободи,
- ✓ Зголемување на довербата кај релевантните институции и граѓаните за заштита од радикализација и насилен екстремизам.

3. **Да се гонат/извршуваат** заканите од насилен екстремизам и тероризам во нивниот корен, во безбедните засолништа и местата каде што претставуваат јасна опасност за граѓаните и инфраструктурата; тие закани правосудно да се гонат активно, но фер и транспарентно, како и конзистентно со владеењето на правото;
   Цел:
- ✓ Воспоставување сет на мерки за рано откривање на радикализација.

4. **ДА се одговори** активно, агресивно, но секогаш на начини што се транспарентни и конзистентни со владеењето на правото, во духот на солидарноста и на начини што ги минимизираат последиците од терористички напад, преку подобрување на способностите на институциите да се справуваат со состојбата по напад, координација на одговорот и на потребите на жртвите.

Цели:
- ✓ Дерадикализација,
- ✓ Реинтеграција преку ресоцијализација и рехабилитација,
- ✓ Координација и соработка

Ова е долгорочен процес што вклучува различни актери на различно ниво, почнувајќи од заедницата до меѓународните партнери и креатори на политики. Бидејќи оваа активност бара пристап од повеќе засегнати страни, важно е да се разберат различните стратегии и пристапи што се развиени за одредени области, регионални, национални итн.

Инструменти за превенција од насилен екстремизам

Инструмент за ризик од екстремизам ERG22+

Насоките за ризик од екстремизам ERG22+ се производ на владини студии на Обединетото Кралство во врска со процесот на радикализирање и биле донесени како алатка за процена од оперативната група за служби за интервенирање и стартувала во 2011 година. Се заснова врз 22 примарни фактори на радикализам и се користи во Рамката Channel Vulnerability Assessment (CVA).

Овој инструмент е клучен елемент на стратегијата за превенирање (homeoffice.gov.uk). Тоа е пристап од повеќе агенции за заштита на луѓето изложени на ризик од радикализација. Се користи постојната соработка помеѓу локалните власти, законските партнери (како што се образовниот и здравствениот сектор, социјалните услуги, услугите за деца и млади и услугите за управување со престапници), полицијата и локалната заедница за:

• идентификување поединци што се изложени на ризик да бидат вовлечени во тероризам;

• да ги процени природата и степенот на тој ризик; и

• да се развие најсоодветен план за поддршка за засегнатите лица.

Инструментот е за заштита на децата и возрасните да не бидат вовлечени во извршување активности поврзани со тероризам. Станува збор за рана интервенција за заштита и оттргнување на луѓето од ризикот со кој се соочуваат пред да се случи незаконитоста. Не треба да се претпоставува дека карактеристиките наведени подолу нужно укажуваат дека некое лице или е посветено на тероризам или може да стане терорист. Рамката за оценување вклучува три димензии: ангажираност, намера и способност, кои се разгледуваат одделно.

1. Ангажман со група, причина или идеологија

Инструментот идентификува потреби, чувствителност, мотивации и контекстуални влијанија што заедно го мапираат индивидуалниот пат кон тероризмот. Тие може да вклучуваат:

• Чувство на жалење и неправда;

• Чувство под закана;

• Потреба за идентитет, значење и припадност;

• Желба за статус;

• Желба за возбуда и авантура;

• Потреба да се доминира и да се контролираат другите;

• Подложност кон индоктринација;

• Желба за политички или морални промени;

• Опортунистичка вклученост;

• Вклучување на семејството или пријателите во екстремизам;

• Се наоѓате во транзициски период од животот;

• Под влијание или контролирање од група;

• Релевантни проблеми со менталното здравје.

2. Намера да предизвикаат штета

Не сите оние што се ангажирани од група, причина или идеологија развиваат намера да предизвикаат штета, така што оваа димензија се разгледува одделно. Факторите на намера го опишуваат начинот на размислување што е поврзан со подготвеноста да се користи насилство и се осврнуваат на тоа што би направил поединецот и до која цел. Тие може да вклучуваат:

• Преголема идентификација со група или идеологија;

• Размислување „тие и ние“;

• Дехуманизација на непријателот;

• Ставови што оправдуваат навреда;

• Штетни средства за постигнување на целта;

• Штетни цели.

3. Способност да предизвикаат штета

Не се способни да го сторат тоа сите оние што имаат желба да предизвикаат штета во име на група, причина или идеологија, а заговорите за предизвикување широка штета бараат високо ниво на лична способност, ресурси и вмрежување за да бидат успешни. Затоа, она за што е способно поединецот е клучно внимание при проценатa на ризикот од штета на јавноста. Факторите може да вклучуваат:

• Индивидуални знаења, вештини и компетенции;

• Пристап до мрежи, финансирање или опрема;

• Криминална способност.

IR46-Islamic Radicalization

IR46 е инструмент за структурна професионална процена, пред да настане кривично дело, за поединци што може да бидат подложни на исламистичка екстремистичка идеологија, попрецизно, инструмент што се применува единствено за исламистички екстремизам.

Се заснова врз четири фази и на Скалила до тероризмот (Staircase to Terrorism) на Могадам (2005). Поделен е во две колони: идеологии (намери) и социјален контекст (способности). Севкупно, овој модел обезбедува 46 индикатори што создаваат основа за повеќеагенциска процена на ризик во која секој индикатор се оценува преку мултидисциплинарно, структурирано и професионално расудување.

VERA-2 (Violent Extremist Risk Assessment)

VERA-2 (Pressman, 2009) претставува процена на ризик што развива специфични индикатори што комбинираат:

- верувања и ставови за да се поддржи идеологијата;
- настаните што претходеле и што ги обликуваат идеите и верувањата на лицето;
- заложба и мотивација и капацитет на поединецот за да планира и да изврши екстремистички напад.

<u>Извештај за процена на ризик</u>
1. Презентирање проблеми на насилство
2. Позадина и историја
3. Мотивација, цел и други карактеристики на насилството
4. Претходна воена, паравоена обука за употреба на оружје
5. Ангажирање во програми за дерадикализација/отпуштање
6. Процена на успехот на програмирање на разделување
7. Умереност во идеолошката посветеност на насилството
8. Природа на веројатно насилство
9. Контекстуални, социјални и други фактори што влијаат на веројатноста за насилство
10. Процена на веројатноста за насилство

Потоа овие елементи се одмеруваат наспроти заштитните индикатори што го ублажуваат ризичното однесување.

Десет ставки во Факторот ставови се оценети. Утврдено е дека овие ставки се важни за мотивацијата за насилна радикализација и прекршоци поврзани со тероризам.

(1) Приврзаност кон идеологија што го оправдува насилството

Ако субјектот е посветен на политичка, верска идеологија или кауза каде што употребата на насилство за постигнување на целта е морално оправдана и легитимирана, тогаш субјектот ќе добие оцена „висока“ за оваа ставка. Ако нема придржување кон употреба на насилство за постигнување идеолошки цели, тогаш субјектот добива оцена „ниска“. Ако има прифаќање за употреба на насилство во некои ситуации, но не и во други, тогаш субјектот ќе добие оцена во „среден опсег“. Оцената за оваа ставка се одредува според нивото на посветеност на идеологијата и на употребата на насилство за постигнување на посакуваните цели.

(2) Перцепција на неправда и поплаки

Перцепцијата на субјектот за неправдата и поплаките, исто така, може да се оцени како „ниска“, „средна“ или „висока“. Ако субјектот има силни чувства дека тој или неговата идентификувана група биле предмет на неправда и тој/таа има високо ниво на поплаки, тогаш субјектот добива оцена „висока“ за оваа ставка. Ако нема перцепција за неправда или поплаки, тогаш субјектот добива „ниска“ оцена. Ако постои одредена перцепција за неправда и поплаки, но тоа не се оценува како претерано, тогаш субјектот добива оцена во „среден опсег“.

3) Идентификување на причината за неправдата

Ако субјектот ја идентификувал целта за која се верува дека е причина за неправда со специфичност и сигурност, тој ќе биде оценет со „високо“ на оваа ставка. Ако субјектот не идентификувал одредена цел или причина за неправда, тогаш оваа ставка ќе биде оценета како „ниска“. Ако постои одредена идентификација, но недостасува специфичност и целта е нејасна, тогаш оваа ставка е оценета во „среден опсег“.

(4) Дехуманизација на идентификуваната цел

Доколку постои дехуманизација на целта со соодветна специфичност на целта (поединец, група), тогаш оваа ставка се оценува како „висока“. Доколку нема дехуманизација на целта, ставката е оценета како „ниска“. Ако постои одредена дехуманизација, но постои двосмисленост или е забележана загриженост за загуба на животи, тогаш оваа ставка е оценета во „среден опсег“.

(5) Внатрешно маченичество

Оваа ставка се однесува на внатрешната реалност на субјектот и прифаќањето на неопходноста да се биде подготвен да се умре за каузата и дека таквото маченичество е и пожелно и благородно. Доколку субјектот ја

интернализирал и ја прифатил неопходноста за маченичтво, предметот се оценува како „високо“. Ако постои прифаќање на потребата да се биде подготвен да се умре, но идејата за маченичтво не е цврсто вградена во свеста на субјектот, личноста е оценета како „среден опсег“. Ако постои прифаќање на потребата да се бориме за каузата, но не и за маченичтво за каузата, тогаш субјектот добива оцена „ниска“.

(6) Отуѓување од општеството и отфрлање на вредностите

Чувството на значителна отуѓеност и/или одвоеност од граѓанското општество со истовремено отфрлање на демократските вредности и норми на секуларното мултикултурно општество е доволно за да се добие „висок“ рејтинг за оваа ставка. Ако субјектот изразува ограничено отуѓување од општеството и неговите вредности, ставката е оценета како „ниска“. Доколку субјектот отфрла некои демократски и плуралистички вредности на општеството и се гледа дека има значително отуѓување од општеството, ставката се оценува во опсегот „среден“.

(7) Омраза, фрустрација, прогонство

Личноста што покажува високо ниво на омраза, лутина, фрустрација и прогон поврзани со неговиот/нејзиниот поглед на светот е оценет како „високо“ на оваа ставка. Оваа омраза и фрустрација се поврзани со идеолошкиот став на поединецот. Минимално ниво на омраза, фрустрација, гнев и чувство на прогон е оценето како „ниско“. Одредена фрустрација и гнев се оценети во „среден опсег“.

(8) Потреба за групно поврзување и припадност

Предмет што има силна потреба да биде дел и прифатен од група е оценет како „високо“ на оваа ставка. Релативното отсуство на оваа потреба е оценето како „ниско“. Одредена желба за прифаќање и поврзување, но не и прекумерна потреба е оценета во „среден опсег“. Оваа ставка е поврзана со личната идентификација бидејќи групното поврзување е поврзано со личниот идентитет.

(9) Колективен идентитет

Ако субјектот покажува идентитет што е непријателски настроен кон националниот колективен идентитет, нема чувство на припадност кон општеството на живеење и покажува збунета или негативна лојалност, тогаш тој/таа е оценет/а со „високо“ на оваа ставка. Ако субјектот не покажува проблеми со колективниот идентитет, предметот е оценет како „низок“. Присуството на некои колективни идентитетски прашања, како што е елаборирано погоре, резултира со рејтинг во „среден опсег“.

(10) Емпатија

Многу ниската емпатија за оние што се надвор од сопствената група може да се оцени дека е во низок, среден или висок опсег. Ако субјектот нема емпатија

за оние надвор од неговата/нејзината група, тогаш оценатa за оваа ставка е „висока“. Ако е присутна емпатија за оние надвор од неговата/нејзината група, тогаш оценатa за оваа ставка е „ниска“. Ако постои одредена емпатија за другите надвор од групата на субјектот, оценатa е во „среден опсег“.

Контекстуални фактори на ризик

Контекстуалните фактори на ризик го земаат предвид влијанието на пријателите, семејството и опкружувањето на оваа тема. Во прирачникот контекстуалните фактори на ризик се проширени за да се вклучат и други влијанија на оваа тема, како што се интернет, обука и социјални контакти од екстремистички верски, политички, етнички или други идеолошки мотивирани групи. Вклучува и фактори поврзани со геополитичките ситуации и владините одговори што можат да предизвикаат насилни одговори.

Контекстуалните фактори се важни за одредување на ризикот бидејќи повеќето терористи не планираат самостојно напади. Насилната намера без други човечки контакти, експертиза, лидерство, планови, финансиска и техничка поддршка обично резултира со неактивност. Екстремистичката идеологија е поддржана во „групното размислување“. Ова може да биде во форма на поддршка од колеги, студиски групи, поддршка од заедницата и пристап до материјали, финансии и лидерство. Интернетот стана важен иницијатор и поддршка за екстремистичките идеи и служеше како врска за екстремистичките групи. Во други случаи, обуката се спроведува или во земјата или во странство. Контекстуалните фактори се втората категорија на VERA.

(1) Корисник на екстремистички веб-страници

Ако субјектот е редовен и посветен учесник и/или корисник на екстремистички веб-локации вклучувајќи ги и оние што промовираат и даваат инструкции за правење бомби, рејтингот е „висок“. Ако субјектот не користи интернет или други средства за да се поврзе со екстремисти или екстремистички веб-страници што промовираат и оправдуваат употреба на насилни дејства за постигнување идеолошки цели, рејтингот е „низок“. Ако субјектот знае за екстремистички веб-страници, но не е редовен учесник или корисник на екстремистичките страници, оценатa е „среден опсег“.

(2) Поддршка на заедницата за насилна акција

Ако субјектот живее во заедница каде што има силна поддршка за насилни дејства за продолжување на религиозните или политички цели или има силна привржаност кон врсничка група или студиска група со која има силна врска и каде што има силна поддршка за насилни активности за понатаму верските, политичките или идеолошките цели, тогаш рејтингот е „висок“. („Поддршката од врсниците за насилна акција“ оценета во оваа ставка се разликува од сопствената потреба на субјектот за врсничка група или врсничка поврзаност што беше проценета во претходниот дел .) Ако субјектот живее во заедница каде

што нема поддршка за насилство за да се унапредат идеолошките цели и не е вклучен во група што поддржува употреба на насилство, тогаш оценатa за оваа ставка е „ниска“ Ако има силна заедница поддршка за идеологијата, но ниска или неконзистентна поддршка за насилство, тогаш рејтингот е со „среден опсег“.

(3) Директен контакт со насилни екстремисти

Ако субјектот е во контакт со три или повеќе „насилни“ екстремисти или е дел од група што вклучува радикални екстремисти, рејтингот е „висок“. Доколку субјектот не е во контакт со радикални/насилни екстремисти, оценатa е „ниска“. Ако субјектот има еден или двајца врсници/контакти што се насилни екстремисти, оценатa е во „среден опсег“.

(4) Гнев кон владините политички одлуки, постапки или друг гнев насочен кон власта

Оваа ставка се однесува на степенот на гнев што го чувствува субјектот кон надворешнополитичките одлуки и/или дејства на една земја кога таквото дејство е против неговите/нејзините политички/идеолошки или религиозни ставови. Ако има силно ниво на гнев и непријателство, рејтингот е „висок“. Ако субјектот има силно несогласување со постапките на владата без високи нивоа на гнев, рејтингот е „низок“. Ако има умерен гнев и непријателство, но гневот е контролиран, тогаш оценатa е во „среден опсег“.

Историски фактори на ризик

Историските фактори се третата категорија на предмети на VERA. Во HCR-20[1] и SAVRY[2], историјата на насилство е еден од најцврстите предвидувачи на идното насилство. Насилството во овие други алатки се однесува на чин на акумулација или физичко насилство што е доволно сериозно за да предизвика повреда на друго лице или лица како што се исеченици, модрини, скршеници

[1] HCR-20 става голем акцент на историските податоци при проценатa на ризикот. Историските податоци се сидрото на проценитe на ризикот (Webster et al, 1997). Ова може да биде случај за општите криминалци, но робусноста на историските податоци за насилниот екстремизам не е докажана. Покрај тоа, историските предмети што се применуваат за насилните екстремисти ќе се разликуваат од оние што се користат за општ криминал поради различните историски реалности.

[2] SAVRY е алатка за оценување на насилството меѓу младите во традицијата на HCR-20. SAVRY беше дизајниран да се користи со деца од 12 до 18 години. Тоа е водич наместо формален тест или скала. SAVRY е дизајниран да одговори на реалноста дека адолесценцијата е време на значајни промени на интелектуално, социјално и емоционално ниво. Borum, R., Bartel, P., & Forth, A. (2006). SAVRY: *Professional Manual for Structured Assessment of Violence Risk in Youth*. Lutz, FL: Psychological Assessment Resources Inc.
Повеќето млади што се насилни во адолесценцијата не опстојуваат на насилничко однесување во зрелоста и карактеристиките на личноста и однесувањата во адолесценцијата се помалку стабилни низ времето, контекстите и ситуациите. Како резултат на тоа, се препорачуваат повторени администрации на SAVRY со текот на времето. Cauffman, E. E., & Steinberg, L. (2000). (Im) maturity of judgment in adolescence: Why adolescents may be less culpable than adults. *Behavioral Sciences and the Law, 18*, 1-21.

или смрт. Тоа вклучува сексуално насилство и други форми на семејно насилство.

Екстремистичкото насилство не е поврзано со домашен гнев, сексуални желби, губење контрола или финансиска добивка. Екстремистичкото насилство мотивирано од идеологија може да се движи од целни атентати до насилни акти од апокалиптична или катастрофална природа дизајнирани да предизвикаат масовни жртви на цивилите. Во некои случаи насилството може да се окарактеризира како она каде што уништувањето и хаосот се цел сами по себе. Терористичкото насилство може да се гледа како „фанатично насилство“ каде што крајниот резултат е да се донесат политички промени, одбрана на идентитетот или решавање прашање на достоинство. Концептот на „праведно убиство“ треба да се земе предвид при проценатa на ризикот на насилните екстремисти (Morgan, 2004).

Следниве се вклучени во делот за историски фактор на ризик на VERA:

(1) Рано изложување на насилство

Првата точка се однесува на раната изложеност на субјектот на насилство. Ако субјектот бил изложен на поддршка за насилни дејства поврзани со политички, националистички, етнички, верски конфликти без разлика дали живеел во демократска земја од раѓање или не, ставката треба да биде оценета „високо“. Ако субјектот не бил изложен, ниту наишол на поддршка за насилство во домот или надвор од домот, предметот треба да биде оценет со „ниско“. Ако субјектот бил изложен на значително семејно насилство, но не и на поддршка на политичко насилство, ставката треба да се бодува во „среден опсег“.

(2) Поддршка од семејството и пријателите за насилна акција

Втората точка се однесува на поддршката што семејството или блиските пријатели ја покажале за насилни дејства. Ако еден или двајцата родители, браќа, сестри, братучеди или чичковци или блиски пријатели биле вклучени во тепачка или собирање средства за насилни причини, или се промотори на насилни дејства, ставката се оценува „високо“. Ако семејството или блиските пријатели не поддржуваат насилни дејства, ставката се оценува со „ниска“. Ако има поддршка за некоја насилна акција, но немало директно учество од семејството или пријателите, ставката се бодува во „среден опсег“.

(3) Претходно кривично дело насилство

Оваа ставка е поврзана со претходното вклучување на субјектот во насилни дејства што може или не може да бидат идеолошки мотивирани. Ако субјектот бил уапсен за претходно криминално насилство, рејтингот е „висок“. Доколку нема претходни апсења за насилство поврзано со криминал, ставката се оценува со „ниска“. Ако има извештаи за насилни инциденти на училиште, на работа, дома или на друго место, но овие извештаи не резултирале со апсење, ставката се бодува во „среден опсег“.

(4) Воена или паравоена обука

Ако субјектот имал паравоена обука што е легитимна воена обука од недржавно спонзорирана, добиената оцена е „висока“ Доколку субјектот немал искуство или обука во вооружување, оцената е „ниска“. Ако субјектот имал одредена обука, но не бил дел од воена или паравоена програма за обука спонзорирана од државата, рејтингот е „среден дострел“.

(5) Патување надвор од земјата за обука и борби под недржавно спонзорирање

Ако субјектот отпатувал во странство за да учествува во паравоена обука или учествувал во недржавно санкционирани кампови за обука за оружје и тактички, воен или насилен отпор, се доделува „висок“ рејтинг. Доколку немало обука во странство, се дава „ниска“ оцена. Ако субјектот имал намера да отпатува во странство за таква обука, но не можел да го стори тоа, оцената е во „среден опсег“.

(6) Глорификација на насилното дејство

Оваа ставка е поврзана со издигнувањето на насилството за согледана благородна кауза како одговор на религиозните или националистичките верувања. Ако субјектот бил и останува посветен на ставот дека насилството е легитимно и убивањето е дел од благородната мисија што е морално оправдана, тогаш оцената за оваа ставка е „висока“. Ако нема глорификација или легитимирање на насилното дејствување и нема морално оправдување, тогаш рејтингот е „низок“. Ако има некакво морално оправдување за насилно дејствување, но нема глорификација, тогаш оцената е во „среден опсег“.

Заштитни фактори

Заштитните фактори се фактори што, доколку се присутни, го ублажуваат ризикот од идно насилство. Заштитните фактори се оценети во однос на нивото или степенот на нивното присуство. Доколку идентификуваните фактори не се присутни, ризикот од насилство е помал и веројатно ублажен. Свеста за присуството или отсуството на овие заштитни фактори е корисна за планирање на програмата за интервенција.

(1) Промена во идеологијата

Ако има поместување на вредностите од претходната екстремистичка идеологија, тогаш рејтингот е „висок“. Оцената е во „среден опсег“ ако е забележано одредено приспособување или промена во идеологијата во ставовите на субјектот или ако промените во вредностите се веродостојни. Ако нема промена во идеологијата и вредностите од претходната екстремистичка идеологија, тогаш рејтингот е „низок“.

(2) Отфрлање на насилството за постигнување цели

Ако субјектот го отфрли верувањето дека насилството што се користи за постигнување цели е морално оправдано и легитимно, тогаш рејтингот е „висок“. Доколку субјектот не ја отфрлил употребата на насилство за постигнување на целите, оцената дадена на оваа ставка е „ниска“. Доколку постои одредено самопреиспитување за вредноста на употребата на насилство, оцената за оваа ставка е во „среден опсег“.

(3) Промена на визијата и концептот на „непријател“

Доколку дојде до промена во перцепцијата за „непријателот“ од (претходната) екстремистичка идеологија, оцената за темата на оваа ставка е „висока“. Ако нема ревизија во идеологијата и непријателскиот референт останува цел, тогаш рејтингот на оваа ставка е „низок“. Ако дошло до извесна модификација во перцепцијата за „непријателот“ и зголемено прифаќање на демократските вредности, тогаш рејтингот е во „среден опсег“.

(4) Интерес за конструктивно политичко вклучување

Ако има интерес за учество во демократските политички процеси, тогаш рејтингот е „висок“. Доколку нема интерес за учество во демократските политички процеси, рејтингот е „низок“. Доколку се забележи некаков интерес за политичкиот процес, а интересот за учество е веродостоен, рејтингот е во „среден опсег“.

(5) Значајна поддршка од заедницата

Ако субјектот има поддршка за дерадикализација од неговото/нејзиното семејство или брачен другар или организација на заедницата, тогаш оцената за оваа ставка е „висока“. Ако во семејството и заедницата нема поддршка за дерадикализација и разграничување, рејтингот е „низок“. Ако има ограничена поддршка, тогаш оцената е во „среден опсег“.

TRAP-18- Terrorist Radicalization Assessment Protocol-18

TRAP-18 е инструмент за ризик што комбинира предупредувачко однесување (патеки, идентификација, фикциска и наративна агресија) и 10 подолгорочни карактеристики (лична тага, идеолошка рамка и психопатологија). Тоа е истражна алатка фокусирана на тероризам извршен од едно лице/поединец.

Фокусот на TRAP-18 е на моделите на однесување, а не на карактеристичните варијабли, т. е. нема намера да предвидува кој ќе изврши или нема да изврши терористички акт; Наместо тоа, алатката може да се користи за да помогне во доделувањето ресурси преку информирање на кои поединци треба да им се посвети приоритетно внимание. Резултатите генерирани од користењето на алатката покажуваат дали случајот бара активно управување (каде што се присутни едно или повеќе предупредувачки однесувања) или следење (каде што постојат само дисталните карактеристики) (Lloyd, 2019).

HCR-20 – Процена на ризикот од насилство

За да им помогнат во расудувањето на оценувачите, многумина користат HCR-20, сметајќи го за многу вредна референтна точка за идно потенцирање на причината и на релевантноста на факторите и формулирањето на случајот, на пример, вклучувајќи теории за личноста, социјалното спознавање, социјалната дезорганизација и одлучување. Врз основа на литература за фактори што водат до насилство, HCR-20 го добила името од три поенти — историска, клиничка (тековна), управување со ризик (иднина) — и од бројот на точки (20) што ги мери. Секоја точка се оценува според структура со рангирање во три нивоа (ниско, средно или високо) (Silva, 2020).

Заклучок

Спречувањето на тероризмот преку справување со радикализацијата и насилниот екстремизам стана глобална карактеристика на националните стратегии, што резултира со развој на многу политики и практики насочени кон спротивставување и спречување на насилниот екстремизам.

Овие пристапи на мека моќ имаат за цел да интервенираат пред да се случи насилство и дадоа повод за нов речник: „спречување насилен екстремизам“, „спротивставување на насилниот екстремизам“ и „спречување радикализација до насилен екстремизам“.

Како што е наведено во овој труд, иако процесите на радикализација, идеологијата на насилниот екстремизам и чинот на тероризам имаат меѓусебно зависни односи, тие се всушност три различни поими што мора јасно да се разберат.

Иако актите на терор не се исклучиво производ на процесот на радикализација, разбирањето на корелацијата е суштествена за успешно спротивставување на насилниот екстремизам.

ГЛАВА II

МРЕЖНО ФУНКЦИОНИРАЊЕ НА ТЕРОРИСТИЧКИТЕ И НА ТРАНСНАЦИОНАЛНИТЕ КРИМИНАЛНИ ОРГАНИЗАЦИИ

Безбедносните предизвици создадени во светот на почетокот на XXI век наметнуваат нов начин на перцепција и изучување на феноменот на тероризмот и на транснационалниот организиран криминал. Соработката на терористичките организации со структурите на организираниот криминал и сè поголемото преклопување на активностите со кои се занимаваат терористите и членовите на организираните криминални групи наведуваат на размислување дека тероризмот и транснационалниот организиран криминал не можат веќе да се анализираат како две целосно различни појави.

Постулат: Како дел од своето дејствување, во пораст е употребата на сојузништво преку мрежни структури помеѓу терористите и криминалците.

Оваа глава укажува на тоа дека транснационалните криминални организации и глобалните терористички организации се многу рационални во своето однесување и се потпираат на мрежните структури при своето дејствување.

Мрежите се последователно глобални и локални. Нивната способност да ја искористат својата интернационална мобилност со огромна брзина, нивната поврзаност со локалните владини структури им даваат огромна предност пред националните и локалните власти што се обидуваат да ги запрат. Нивниот опстанок зависи од способноста на мрежата да се преорганизира со помош на соработка и да ја прекине соработката со леснотија, заземањето нови пазари и тоа што секогаш се чекор понапред (Moises, 2005).

Многу терористи, вклучувајќи го глобалното движење на џихадот, исто така, се потпираат на мрежното функционирање. Едно објаснување на камповите за обука во Авганистан и на други места е тоа дека тие беа и се вежби не само за развивање на терористичките вештини и способности туку и за развивање на врските меѓу поединци што последователно формираат ќелии што ги спроведуваат нападите.

Кога станува збор за примена на теоријата врз терористичките групи, реалистите се стремат да ги игнорираат терористите, а либералите едноставно ги наведуваат во списокот на транснационални актери. Проникливата концепциска анализа посветена на терористичките групи произлезе од теоретичарите на националната безбедност што на војувањето гледаат од аспект на нешто што е наречено мрежна војна. Терминот мрежна војна се однесува на

„еден нов начин на конфликт (и криминал) на општествено ниво, на кој му недостасува традиционалното водење војна и во кој протагонистите користат мрежни форми на организација и доктрини поврзани со нив, стратегии и технологии приспособени на информатичката ера.“

Вмрежување на формите на глобалниот тероризам

Од државно спонзориран тероризам, карактеристичен за времето на Студената војна, кој беше познат и како метод на специјалното војување, еволуирањето на тероризмот отиде во насока на премисите на религијата и на анархијата. Вмрежувањето на религиозно обоените терористички групи, во услови на техничко-технолошки развој и експанзија на глобализацијата, претставува сериозна закана за светскиот мир и безбедност, што во неколку наврати е препознаено и од страна на Советот за безбедност на ООН (UN Security Council Resolution 1368).

Ваквата еволуција на тероризмот отиде во насока на вмрежување на терористичките групи и нивно сè поголемо интернационализирање. На тој начин, искористувајќи ги условите што ги овозможува современиот свет на живеење, а, пред сè, силните интеракциски односи на меѓународен план, подемот на борбата за човекови права и обидот за толкување на правото за самоопределување во духот на сецесијата, глобализацијата и нејзиното влијание врз класичниот пристап на суверени држави, како и промената на рамнотежата на сили во меѓународната политика, започна процес на формирање на современиот тероризам.

Денес, со развојот на најновите научно-технички достигнувања и средствата за комуникација, терористите се приспособиле кон новите околности и создале мрежа на терористички организации, чиишто организациски ќелии егзистираат во сите делови на светот.

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

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

се адаптираат на надворешните влијанија и попродуктивно ги користат информациите за унапредување на процесите за донесување одлуки.

Основни карактеристики на мрежните организации се следниве:

1. Комуникацијата и координацијата не се однапред формално одредени преку вертикални односи на известување, туку се остваруваат според потреба.
2. Внатрешноста на мрежата (пр. делови на мрежна организација во една држава или мрежна организација што е дел од поголема мрежа) најчесто се надополнува со врски со поединци надвор од организацијата (кои често ги преминуваат националните граници). Интерните и екстерните врски се создаваат и згаснуваат во зависност од животниот циклус на проектот, односно задачата.
3. Внатрешните и надворешните врски не дефинираат бирократски правила/заповеди, туку заеднички вредности и норми, како и меѓусебна доверба. Поголемиот дел од активностите ги реализираат „самоуправувачки“ тимови, додека надворешните врски ги сочинуваат организиран збир што вклучуваат комплексна мрежа на групи (Monge, Fulk, 1999).

Може да се заклучи дека латералните координациски механизми го олеснуваат преземањето операции на мрежните терористички организации и се поддржани од напредокот на информацискатa технологија.

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

- Зголемената брзина на комуницирање (со зголемена пропустливост на мрежата и широка вмреженост). Новите технологии ги овозможуваат комуникацијата и координацијата меѓу раздалечените припадници на групите на терористичките организации.
- Намалената цена на комуницирање. Новите технологии значително ги намалија трошоците за комуницирање, овозможувајќи одржливост на мрежниот облик на организација (со оглед на потребата за интензивна комуникација).

4. Интеграцијата на комуникациските и на компјутерските технологии резултирала со зголемен опсег и сложеност на информациите што може да се споделуваат со помош на мрежата (Monge, Fulk, 1999).

Технологиите на информацискатa ера се особено погодни за мрежните облици на организација, чии припадници се географско оддалечени или се задолжени за спроведување различни, но комплементарни активности. Тоа не значи дека традиционалните хиерархиски организирани терористички

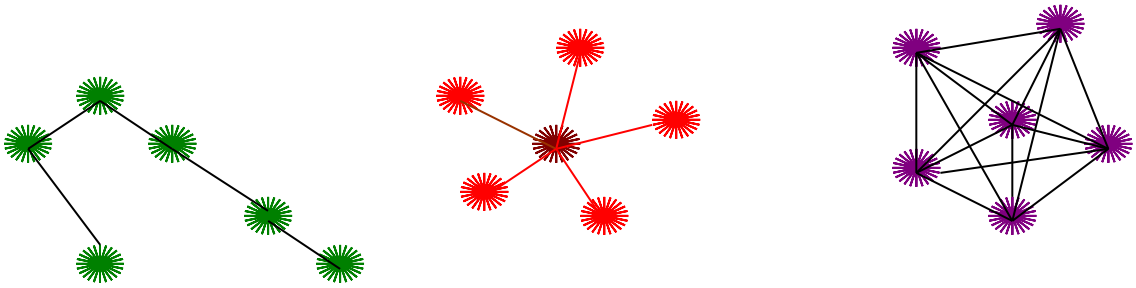
организации нема да ги прифатат или да ги користат информациските технологии за да ги подобрат интерните заповедни, контролни и комуникациски функции. Пример е сектата Аум Шинрикјо, која била организациски високоцентрализирана околу личноста на водичот со кохезиска и строга хиерархиска структура, но истовремено, во голема мера, се служела со информацискатa технологија во внатрешноста на групата.

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

Потенцијалната моќ на Петтата генерација на војување беше демонстрирана во бомбашките напади во Мадрид во 2004 година. Во оваа пригода, серија масовни бомбашки напади на транспортната инфраструктура, која ја предводеа мрежно поврзани терористички групи, во еден единствен ден, и тоа во екот на националните избори, резултираа со вонредна состојба во Владата во Шпанија и влијаеја на моментално повлекување на шпанските воени сили што беа ангажирани во воена кампања против бунтовниците во Ирак.

Бомбашките напади во Мадрид се значајни од причини што терористите, кои стоеја зад нив, беа главни дилери на дрога и дел од наркомрежата што се простираше од Мароко, преку Шпанија и Белгија, до Холандија. Додека почетните процени за цената на бомбите што беа употребени се движеа од околу 50 000 фунти, вкупната заработка откриена во дрога и во готови пари, а која се поврзуваше со овие напади, достигнува вредност од повеќе милиони фунти. При ова, се дојде до сознанија дека групата што ги изврши терористичките напади е дел од транснационална криминална организација. Со ваквото ангажирање, се демонстрира дијалектичката предност на Петтата генерација на војување над веќе познатите методи на војување од Третата и од Четвртата генерација на војување.

Формата на организација на мрежната војна наликува на „ѕвезди“ што имаат некои централизирани елементи или на „синџири“ што се линеарни или на „сеповрзана“ мрежа, во која секој основен контакт комуницира или влегува во интеракција со секој од другите контакти.



Слика – Основни типови и нивоа на мрежи (Arquilla, Ronfeldt, 2001)

1. **Мрежа во форма на „синџири“** - комуникацијата помеѓу краевите на мрежата се одвива преку посредници, односно „ѕвезди“. Оваа форма може подеднакво да ја користат терористичките организации и структурите на транснационалниот организиран криминал преку синџир за криумчарење, во кој луѓето, добрата и информациите патуваат по линија што се состои од одвоени контакти/„ѕвезди“ и каде што комуникацијата од едниот до другиот крај на линијата мора да помине низ сите делови на „синџирот“.

2. **Мрежа во форма на „ѕвезда“** – комуникацијата и координацијата меѓу припадниците на мрежата се одвиваат преку централната „ѕвезда“ или јазол. Овој вид форма на организација е експлоатиран од страна на организацијата на наркокартелот, каде што членовите на криминално-терористичките организации се поврзани со центарот или со главниот организатор, односно преку него мораат да комуницираат и да ги координираат сите свои активности.

3. **Поврзана/канална мрежа** претставува соработничка мрежа на повеќе меѓусебно поврзани помали групи. Мрежата на милитатните групи го применува овој облик на мрежно организирање (Arquilla, Ronfeldt, 2001).

Може да се заклучи дека најтешко се организира и се одржува поврзаната/канална мрежа, која бара честа комуникација, но таа воедно нуди најмногу можности за спроведување заеднички операции, односно таа претставува мрежен облик што најмногу ќе просперира од информатичката револуција (Howard, 2004). Во поврзаната мрежа хиерархијата не е изразена или воопшто не постои, а во внатрешноста на структурата може да фигурираат повеќе лидери и, поради тоа, донесувањето одлуки и, понекогаш, самото дејствување се децентрализирани. Оваа предност им овозможува автономија и ја поттикнува иницијативата на помалите групи. Но, тука се јавува и опасноста дека таквата организација може да остави контрадикторни впечатоци што се движат од анархичност до повеќекратна организираност. Успешното

функционирање на овој мрежен облик треба да се согледа во неговата потреба за постоење заеднички интереси и цели, односно постоење доктрина или идеологија, чии стојалишта ги прифаќаат сите контакти/ѕвезди.

Секоја форма на мрежна организација, според потребата, може да биде приспособена кон различни услови и намена. „Ѕвездата“ или контактот може да биде претставен преку поединец, група и/или институции (или нивни дел) и држава, додека границите на мрежата може да бидат јасно одредени, но може да бидат и недефинирани, односно невидливи и порозни во однос на надворешното опкружување. „Ѕвездите“ на мрежата се, повеќе или помалку, поврзани во одредено членство каде што сите комбинации се можни.

Покрај трите основни мрежни организациски форми, постои можност за комбинирање, кога настануваат хибридните форми.

– Мрежниот актер може да ја организира својата група како поврзана мрежа, а истовремено да ја користи мрежата во форма на „синџири“ и мрежата во форма на „ѕвезда“ за изведување тактички операции.

– Терористичките и организираните криминални организации што се хиерархиски структурирани може да се користат со мрежни организациски форми за спроведување тактички операции.

– Мрежните организирани терористички и организирани криминални организации во облик на поврзана/канална мрежа може да се служат со хиерархиски организирани тимови за реализирање тактички операции (Howard, 2004).

Конкретен пример за хибриден облик на мрежа е терористичката организација ал-Каеда, односно комуникацијата меѓу припадниците на таа мрежа, која се остварува со комбинација на мрежата во форма на „ѕвезда“ (кога контактите, оперативците комуницираат со лидерот и со неговите блиски соработници во Авганистан) и со поврзаната/канална мрежа (кога контактите на мрежата меѓусебно комуницираат без консултирање на лидерот на организацијата) (Simon, Benjamin, 2000).

„Познатите непријатели што ги модифицираат структурите и стратегиите за да ги искористат мрежните дизајни ги вклучуваат транснационалните терористички групи, распространувачи на оружје за масовно уништување на црниот пазар, наркогрупи и други криминални групи, фундаменталистички и етнонационалистички движења, лица што вршат пиратерија и шверцери на имигранти и на бегалци.“ Благодарение на информатичката револуција насекаде низ светот, членовите на мрежите не мораат лично да се среќаваат. Од перспектива на терористите, поради тоа, безбедноста е подигната на повисоко ниво, а една организација може да има поддржувачи низ целиот свет. Овие актери, главно, се состојат од дисперзирани групи, кои се согласуваат да комуницираат и да дејствуваат можеби и без централно лидерство или седиште. Се претпоставува дека хиерархиските организации, какви што се државите,

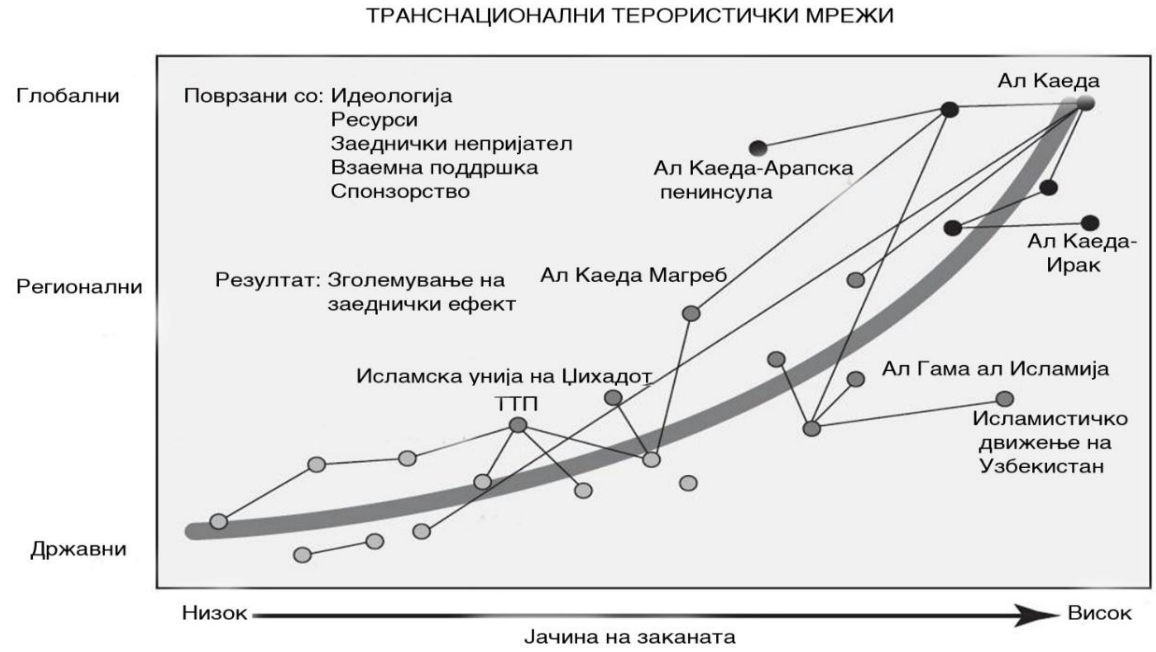
може да бидат несоодветно опремени за да се справат со едни такви организациски иновации (Arquilla, Ronfeldt, 2001).

Меѓународните криминални организации воспоставија софистицирани техники, маркетинг и дистрибуција и потполно се способни да употребат висока технологија за да ги постигнат своите цели. Новитетот од работата во мрежа наречена „лабави фамилии“ им овозможува да се одбранат од применувањето на законот, вешто вршејќи многубројни активности на граница помеѓу дозволеното и недозволеното (Centre for Strategic and International Studies 1994).

Иако транснационалните криминални организации и глобалните терористи имаат креирано внимателно дизајнирани стратегии со кои ќе постигнат одредени цели, целите, сами по себе, се тешки за остварување. Во центарот на овој напор да се дојде до промени е изборот на цели и на оружје. Сепак, терористичките напади е најдобро да се сфатат како финален резултат на повеќе активности што вклучуваат зголемување на фондовите, регрутација, обука, развивање специјални вештини и подготовки пред напад што може да трае со месеци, па дури и со години. Во случајот на криминалните организации, целта е финансиски профит. Со цел да се задржат ваквите добивки, криминалните организации развиваат нелегални бизнис-стратегии. Во исто време, затоа што продуктите и активностите се незаконски и за нив не важат официјалните бизнис-правила, мора да се преземат мерки да се справат со ризикот, без разлика дали е од страна на немилосрдната конкуренција што се бори да го заземе пазарот или од владата и органите на законот што настојуваат да ги оттргнат од бизнисот. Процесот на справување со ризикот се состои од повеќе нивоа и вклучува стратегии за избегнување и за превенција на ризикот, напори да се победи или да се контролира ризикот и олеснувачки стратегии. Избегнувањето на ризикот често се прави преку јурисдиктичка арбитража, во која криминалните организации оперираат од земји каде што државата е слаба и неефикасна за борба со нив. Онаму каде што земјата се соочува со организиран криминал, стратегиите на криминалците за справување со ризикот вклучуваат употреба на корупција и насилство за да го неутрализираат криминалниот правен систем до заобиколување на границите и контрола над имиграцијата и, конечно, да се искористат слабостите на државата и да се задржи безбедноста на територијата. На третото ниво, криминалните организации спроведуваат стратегии за да се намали штетата и да се зголеми издржливоста. Една компонента од оваа стратегија е прифаќање на мрежните структури што се подготвени за групирање и за обнова во случај на уништување некој од деловите на мрежата (Baylis at all, 2022).

Согледувајќи ги предноста и примената на мрежните организациски форми, мора да се земе предвид дека, иако мрежните актери имаат корист од зголемената брзина и намалената цена на комуникациите, како и од широката вмреженост, целосната примена на потребните технологии е проблем за географски широко дистанцирани припадници на мрежите. За мрежното функционирање може да бидат доволни и „старите“ начини на комуникација,

како, на пример, посредник – курир или преку комбинација на „новите“ и на „старите“ начини на комуникација. Потребно е да се забележи дека мрежното војување не претставува интернет-војување, односно тоа не се одвива само во киберпросторот, а начинот на водење и вкупните резултати на мрежната војна зависат од случувањата во реалниот свет.



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

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

- сè поголем број терористички организации ги прифаќаат мрежните форми на организација и притоа сè повеќе ја користат информацискатa технологија;
- терористичките организации (оние што се основани во осумдесеттите и деведесеттите години на 20 век) се подлабоко вмрежени за разлика од терористичките организации со долга традиција;
- помеѓу степенот на активност на терористичките организации и степенот на прифаќање на мрежните форми на организација постои позитивна корелација. Во прилог на ова тврдење се новите и помалку хиерархиски организирани терористички организации, како што се Хамас, Палестинскиот исламски џихад, Хезболах и ал-Каеда, кои воедно станаа и најактивни терористички организации;

- еднаква е веројатноста дека информацискатa технологија ќе се користи како организациска потпора и како средство за напаѓање при војување;
- поголема е веројатноста дека новорегрутираните припадници на терористичките организации се поопособени за користење нови технологии, што имплицира дека во иднина ќе бидат подлабоко вмрежени и повеќе ќе ја користат информатичката технологија.

2.1. Потенцијално преклопување на мрежите на транснационалниот организиран криминал и на тероризмот

Ова поглавје се осврнува на врските помеѓу криминалните групи и терористите и потенцијалното поклопување на нивните мрежи. Анализата за транснационални криминални организации и терористички организации, односно за развојот и организациските мрежи помеѓу и во рамките на овие организации на преклопувањата на мрежите е значајна за импликациите за противтерористички политики и акции.

Тоа што и криминалните организации и терористичките организации заеднички ги користат принципите на мрежи не значи дека терористичките и криминалните мрежи или организации секогаш се преклопуваат. Постоењето работни релации меѓу некои терористички групи резултира во релативно ниско ниво на соработка како безбедни засолништа, патни документи, оружја, информации и слично. Се разбира, важно прашање е дали овие мрежи за делење информации меѓу некои терористички групи се прошируваат на вистинските мрежи на терористички групи со криминални организации и дали оваа соработка подразбира каков било координиран напор кон долгорочни организациски алијанси, здружувања или трансформации.

Генерално, мрежната организација е помалку хиерархиска и, затоа, порамномерна од традиционалната организација. Појавните комуникациски структури (за разлика од формалните врски) се адаптивни и соодветни, комуникациските врски ги надминуваат организациските нивоа и ограничувања и врските избледуваат. Врските се градат и се рушат врз основа на потребите за постигнување на мисијата/задачите на организацијата. Мрежната организација се стреми да биде информациски богата и технолошки софистицирана толку колку што врските се креирани да произведуваат, делат, чуваат и да добиваат различни информации и перспективи. Тоа е помалку стабилен систем дизајниран за средини што исчезнуваат.

Создавањето и распаѓањето на мрежите сугерираат континуирана реконфигурација на организациското структурирање. Мрежните организации често се мешаат со стратегиски алијанси меѓу организациите (Stohl, 2008).

Стратегиските или тактичките алијанси претставуваат намерно и формално поставени односи создадени помеѓу две или повеќе организации и во секоја организација. Комуникациската структура може, но не мора, да биде

хиерархиска и бирократска, механичка и стабилна. Овие алијанси се генерално креирани да следат определени идентификувани дополнителни цели, но се дизајнирани да одржуваат независност од организациите додека се поврзани. Во стратегиски или тактички алијанси секоја организација се стреми да има одредени улоги и ако има простор за појавни врски. Стратегиската алијанса може да се разбие со малку влијание врз внатрешната динамика на секоја организација вон заедничкиот стремеж кон определена цел.

Мрежите може да варираат во големина, облик, членство, кохезија и цел. Мрежите може да бидат мали, локални или глобални, национални или транснационални, кохезивни или дифузни, централно водени или високодецентрализирани, со резултат или без дирекција. Специфичната мрежа може да биде стеснета или цврсто фокусирана на една цел или да е широко ориентирана кон повеќе цели и може да биде или ексклузивна или сеопфатна во своето членство.

Терористичките групи воспоставиле во целиот свет врски и мрежи, обезбедувајќи соработка помеѓу национални и меѓународни терористички организации во форма на финансиска и на техничка поддршка (Stohl, 1983). Централни проблеми во мрежната литература за терористички организации сè уште се појавуваат денес.

Прво, без оглед на инхерентниот механизам и појавната флексибилност вградена во терминот мрежа, јавните креатори на политики ги разгледуваат терористичките мрежи како хиерархиски организирани и централизирани бирократии.

Второ, тајната природа на терористичките мрежи му овозможува на политичкиот опортунизам да наметнува компромис за релијабилноста и за валидитетот на граничните спецификации, извештаи за поврзаност и последователни заклучоци (Stohl, Stohl, M2007).

Робусноста и еластичноста на терористичките мрежи не се основани на многубројни врски што испраќаат или примаат информации, туку на одржуваната можност да мобилизираат и да анимираат, како актуелни така и идни борци, поддржувачи и симпатизери преку овие врски (Hoffman, 2003). Иако истражувачите на тероризмот долго време биле свесни дека терористичките мрежи што издржале низ времето се врзани со етнонационални или борби на заедницата, продолжени конфликти, политички настани или перципирани историски нееднаквости.

Додека оние што го посвојуваат мрежниот јазик честопати нагласуваат дека современите организации не се веќе структури што се поврзани заедно низ познат синџир на наредби и дека мрежите се повеќе хоризонтални отколку вертикални. Кога се дискутира за создавање цели, мотиви и можности, тие честопати паѓаат во неколку хиерархиски претпоставки

(а) мрежните идентитети и улоги се фиксирани и константни,

(б) мрежите оперираат според формални и недвосмислени правила и

(в) овие правила ограничуваат како членовите на мрежата се однесуваат, дефинирајќи и лимитирајќи што е дозволена, а што недозволена акција.

Мрежите треба да се разберат како привремени, динамични, појавни, приспособливи, претприемачки и флексибилни структури. Иако се организирани околу пазарните и хиерархиските принципи, мрежните организации се креирани од комплексни мрежи на размена и зависни врски меѓу многубројни организации (Monge, Contractor, 2003). Во зависност од зоните на нивната соработка, тие може да ги поминат националните ограничувања и така да оперираат во многу различни социјални милеа и на многу различни начини. Постојат, исто така, и некои историски тензии. Утврдените организирани криминални организации се високонационалистички. Криминалните организации Јакуза или Мафија, на пример, може да формираат еднократни краткотрајни или долготрајни алијанси. Колку е поцврсто структурирана утврдената организација, толку е поверојатно таква организациска структура да преовладее.

Со други зборови, за мрежниот пристап да биде корисен, не можеме да размислуваме за мрежната структура дека има јасна команда и контрола со некои врски за давање наредби на другите. Терористичката мрежа е нексусот на повеќе групи и конституенти што се поврзани на значајни, но нехиерархиски начини и може единствено да се разберат во контекст. Се разбира, ова го прави прашањето на дефинирање и на определување мрежни ограничувања многу важно. Како ги определуваме границите кој е во мрежата, а кој не е, има критички значајни политички импликации.

Јасно е дека секогаш кога ќе се занимаваме со тајни организациски мрежи, валидноста на податоците ќе биде во прашање (дури и највнимателните разузнавачки агенции и полициски служби во светот ќе треба да направат претпоставки и да извлечат заклучоци од многу некомпетентни и сомнителни податоци. Исто така, новинарите мораат често да ги пишуваат своите написи од материјал обезбеден од владини службеници или од терористи или симпатизери што обезбедуваат материјали за сопствени цели.).

Решението на дилемата за спецификација на ограничувањата лежи во нашата можност за идентификација на конститутивните карактеристики на организациската комуникација, во смисла на координација, контрола и на интеграција на членство – колаборативен интерфејс, кој резултира во систематичка структура што е значајна и препознатлива. Накратко, нужно е да се биде способен да се разликува помеѓу можноста „да се поврзува мрежно“ од способноста да се мобилизираат, контролираат и да се координираат членовите на специфично планиран акт. Ова значи дека не сите акти на мобилизација се еднакви во своето значење.

Можеби најважните разлики меѓу групите се природата на нивните цели и целта на насилството што го употребуваат.

Некои мрежи се градат врз релации на хомофилност (семејство, пријатели, идентитет). Споредувањето со етнички базираните терористички организации, како што се Хамас, Хезболах и баскиската ЕТА, со мултиетнички терористички групи, како што се ал-Каеда и Аум Шинрикјо, ја истакнува критичката важност на разликување помеѓу глобални и локални мрежи. Хамас и други етнички базирани организации формираат ќелиска структура компонирана примарно од хомофилни врски (пр. клан или група од етнички членови) (Norton, 1998). Конспираторите не формираат многу нови врски вон мрежата и често ја минимизираат активацијата на постојните врски во мрежата. Цврстите врски, кои остануваат често скриени, се фреквентно формирани години претходно во училишта и кампови за обука и ја држат ќелијата поврзана. Многу вакви организации, исто така, ги регрутираат своите членови само од познати отколку од затворени кругови на потенцијални учесници, на пример, од семејство или клан и зависат од роднински врски што им обезбедуваат доверба.

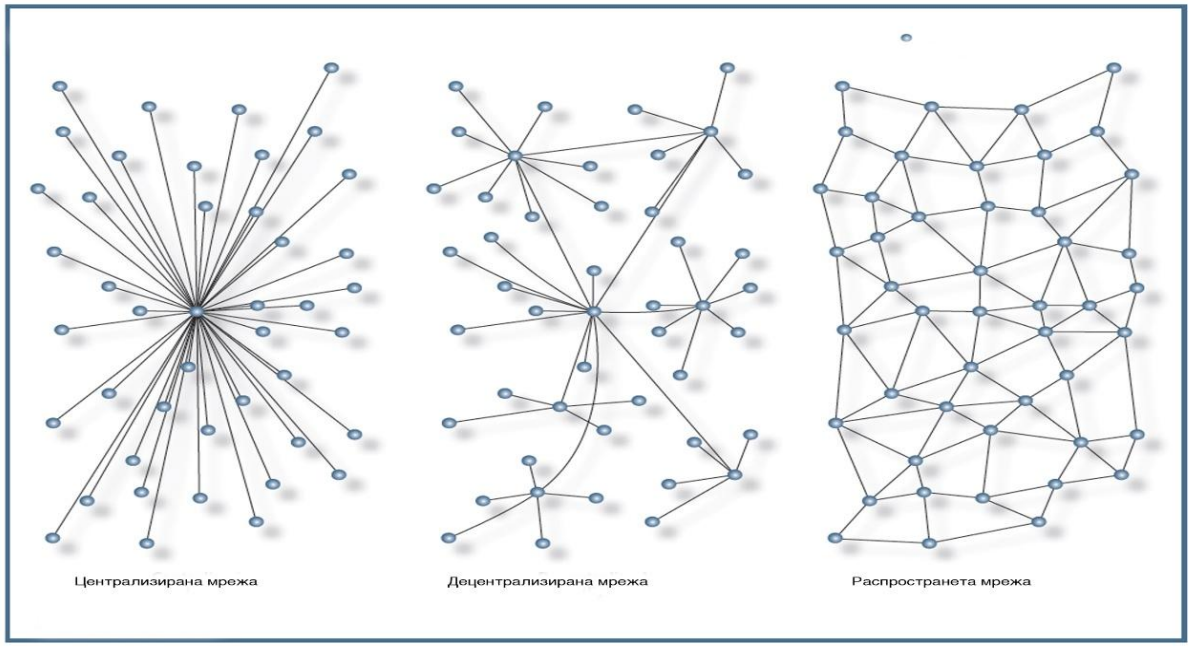
Криминалните мрежи базирани на етницитет се генерално лоцирани во етнички заедници што нудат бази/засолништа и константно снабдување со регрути. Кога овие етнички заедници ќе се прошират вон националните граници, стратегиска алијанса меѓу групите може да се развие. На пример, албанска криминална организација ги користеше сопствените криминални профити да купи оружје и воена опрема за Косовската ослободителна армија – но може да се тврди дека нивната етничка национална религиска идентификација беше нивна мотивација што му асистираше на нивното прекугранично „братство“ (Makarenko, 2004).

Други мрежи се градат врз основа на хомофилноста на определена вредност и „истомисленост“. Ако терористичките и криминалните организации се согласат да соработуваат, тие најверојатно ќе се соочат со разликите во врските што ги имаат доближено заедно во нивните две различни мрежи, вклучувајќи го не само профитот версус политичкиот мотив туку и формите на врски што ги поврзуваат потенцијалните регрути. Кога организациите се конституирани од униплекс идеолошки врски (компарирано со мултиплекс врските и идеолошките линкови), тие може, исто така, да бидат репродуцирани и заменети од многу поголем број потенцијални регрути. Нивните ограничувања се, исто така, многу повеќе попустливи. Исто така, ако членовите се повеќе „идеолошки поврзани“ отколку „идеолошки/идентитетно поврзани“, тие не развиваат структура на мал свет и, како такви, случајната деструкција на ќелијата ги остава овие типови организации повеќе повредливи.

Довербата е хроничен проблем за која било тајна организација, вклучувајќи ги и организираниот криминал и терористичките организации. Така, ваквите организации, во своите напори да избегнат казна и да преживеат, внимателно ќе ги скенираат своите шеми на регрутација, потпирајќи се повеќе

на силни отколку на слаби врски и често бараат тест на лојалност или верност. Постоењето „цврсти врски“, како и трајни односи базирани на високо ниво на доверба, заемна почит и заеднички грижи е карактеристично за алијансите што се формираат помеѓу транснационалните криминални и терористички организации, но, исто така, се повеќе минливи, односи базирани на краткотрајни случајни интереси (Williams, 1999). Тајните мрежи веројатно ќе формираат тактички еднократна или многу краткотрајна конекција отколку поврзаност или чиста алијанса за да ги намалат шансите од пенетрација. Во многу случаи, поврзувањето ќе биде директно поврзано со семејството или со сродството – многу италијански мафијашки групи се сè уште организирани преку семејни врски, додека турската трговија со дрога и криминални организации е сè уште базирана на кланови. Други поврзувачки механизми ги вклучуваат етницитетот и заедничкото искуство во кое учесниците развиваат силно чувство на доверба и заемно потпирање. Членовите на тајните мрежи првенствено се потпираат на претходно формираните мрежи што ја формирале организацијата – основа на која тајното здружение е формирано (силни врски) за да компензираат за ризикот кога се во интеракција со екстерни индивидуи и групи (Morseli at. all, 2007).

Централизираните и децентрализираните мрежи манифестираат висок степен на ранливост, додека распространетата мрежа е флексибилна да опстане во случај некои од компонентите на мрежата (терористички или криминални групи) да бидат откриени, кога веднаш се пронаоѓаат алтернативни патеки, со цел непрекинато функционирање на системот, т. е. криминалната или терористичка организација. Ова е една од причините зошто е толку тешко да се допре до криминална или терористичка мрежа што поседува, односно има карактеристики на распространета архитектура.



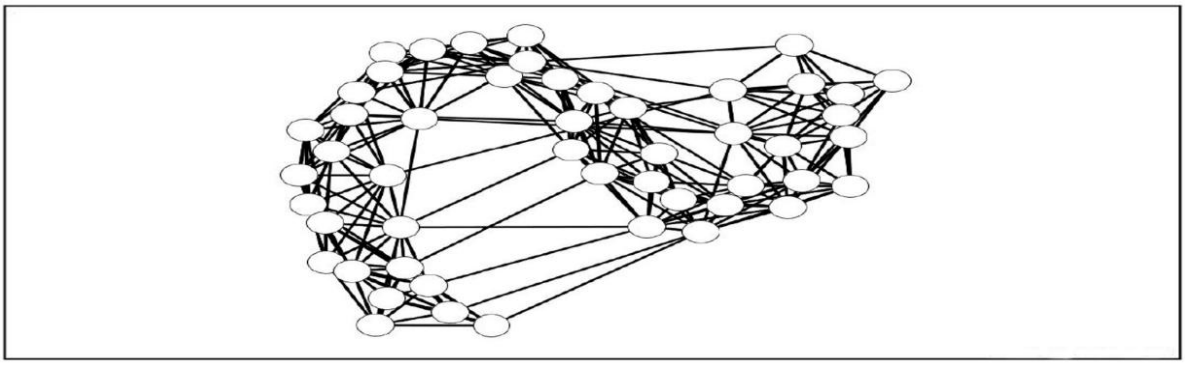
Слика – Видови мрежи

Кога се работи за овој вид мрежа, каде што се очекува вистинско влијание, неопходно е да се нападне постојната група, со најголем број концентрирани врски. Ако не се идентификува вистинската група или не се успее во намерите да се елиминира, мрежата е способна многу брзо да се реконфигурира, како, на пример, мрежата на ал-Каеда, која себеси се реконструира на различни нивоа и во различни региони (Badia, Dalmases, 2010)

Комплексноста на овие мрежи се согледува преку лесното еволуирање во други понапредни форми што се многу ефикасни во размена на информации и се тешки за откривање, додека нивната топологија е способна да се адаптира на променливите околности и да ги разреши препреките со цел да ги реализира зацртаните планови.

Солидно организираните криминални и терористички компоненти на овие мрежи јасно ги демонстрираат овие предности. Комуникацијата е можна на хоризонтално ниво меѓу повеќекратните контакти, овозможувајќи им локално решавање на проблемот без да го пријават на командниот центар, и со тоа ги надминуваат вертикалните линии на комуникација. Оваа флексибилност и локална иницијатива на распространетите мрежи го покажуваат контрастот со ригидноста на хиерархиите, кои не се доволно приспособени, туку најмногу се способни за реализирање контрола (Sageman, 2004)

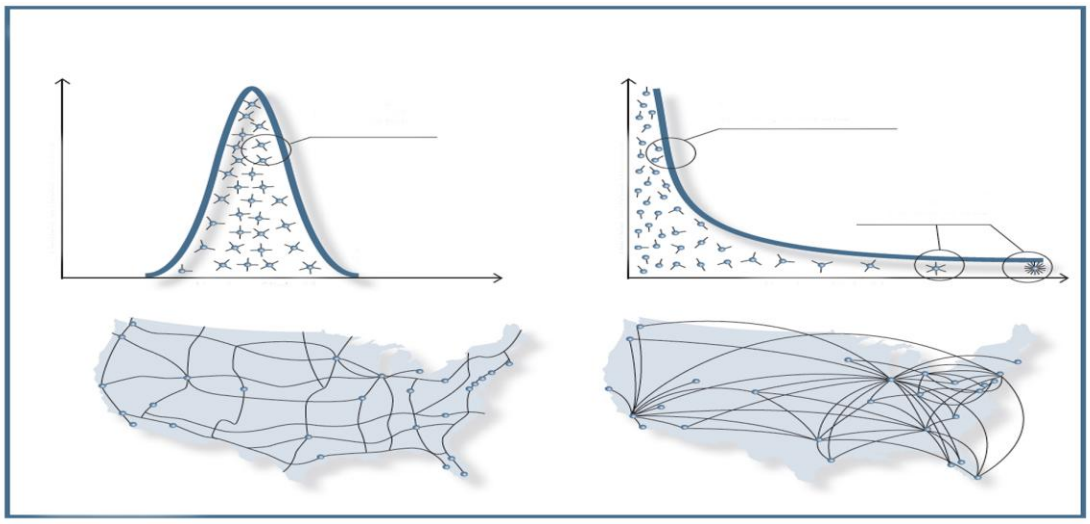
Првата категорија на мрежи е тесно поврзана мрежа (small-world network), која се карактеризира со кратка должина на патеките меѓу компонентите на мрежата што се нарекува дијаметар д. Тоа е генерално прифатен математички модел, конструиран со поврзување на секоја група во мрежата. Поради случајните врски во оваа мрежа, дури и многу голема мрежа може да има мал дијаметар (Watts, Strogatz, 1998). Анализата на оваа категорија на мрежи е комплицирана поради многубројноста на врските што се воспоставуваат. Најкратката патека во мрежата не е таа што математички се обработува со помош на алгоритми бидејќи индивидуата типично во дадена општествена мрежа има целосно разбирање на сопствената локална мрежа, но има ограничено знаење за глобалната мрежа (Dodds at.all, 2003)



Слика – Тесно поврзана мрежа (small-world network)

Разбирањето на мрежните динамики може да помогне за напаѓање на многубројноста на терористичките ќелии. Терористичките мрежи се многу повеќе од едноставни општествени мрежи; тие вклучуваат знаење за мрежи, задачи на мрежи и извори на мрежи (Carley, 2002). Ова ја надминува, односно ја проширува науката за контратероризам подалеку од анализирање на општествените мрежни врски, овозможувајќи комплексна слика на целата мрежа што вклучува финансиски и експертски мрежи.

Мрежата на теорија еволуирала од 1990, преку опишување на мрежите како статички феномени до разгледување како системи што постојано растат, од случајни мрежи до мрежи во кои се дистрибуира моќта.



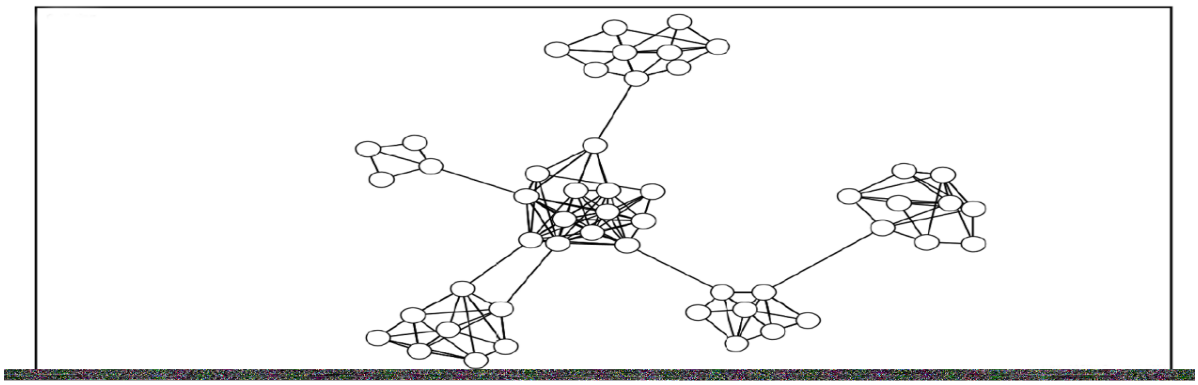
Слика – Случајни и слободни мрежи

На Сликата се прикажува дистрибуцијата на случајна мрежа, која ја следи кривата што демонстрира дека повеќе контакти на мрежата имаат ист број врски, додека групи со голем број врски не постојат (Barabási, 2003). Спротивно, слободната мрежа го почитува законот на моќта, каде што мал број контакти го поседуваат мноштвото на врски/линкови во системот[3]. Најпрво, нови линкови може да се појават, односно да се формираат меѓу постојните членови на мрежата. Оваа појава имплицира дека криминалците или терористите што претходно не биле поврзани може да се поврзат во иднина (Xu, Chen, 2008) Поради контактите што имаат висок степен на поврзаност, слободните мрежи, исто така, може да бидат перципирани како поткатегорија на тесно поврзаните мрежи (small-world networks) (Mitchell, 2007). Корисноста на слободните мрежи, каде што се почитува децентрализацијата на моќта, се согледува во способноста да презентира опис на реалните светски мрежи, што е, исто така, признавање дека најголем број на вистинските мрежи се отворени системи што континуирано растат и привлекуваат сè поголем број контакти (Réka, Barabási, 2002). Слободниот мрежен модел може да поднесе висок степен на случајно

[3] Овој закон на моќта е сличен на Парето Принципот или 80/20 правило, каде помалку од 20% на поединци контролираат 80% од претпоставената област.

отстранети контакти, додека целата мрежа брзо се деградира кога најмногу контакти (поединци, групи) се отстранети/ елиминирани. Овие анализи се неопходни за истражување на мрежите бидејќи сугерираат дека случајното елиминирање терористички или криминални индивидуи или групи може да продолжи бесконечно, сè додека најповрзаните единки преживеале. Ова ни покажува како терористичките мрежи закрепнуваат по одредени напади, поради фактот дека тие сè уште имаат способност да привлечат нови регрути/приврзаници/следбеници и можат да одржат трансактивна меморија, како што претставуваат прирачниците за обучување терористи или одредени датабази (Tsvetovat, Carley, 2003).

Третиот модел – ќелискиот е составен од мали кластери на центри, понекогаш нарекувани ќелии[4], кои се поврзани меѓусебно на лабав начин или се поврзани со централниот контролен кластер или центар. Секој кластер е поврзан со секоја индивидуа/група во внатрешноста на кластерот. Како мрежен модел, ќелиската мрежа може, исто така, да покажува карактеристики на мрежа small-world бидејќи секој контакт на мрежата може да биде достигнат со релативно мал број линкови.



Слика – Ќелиски мрежен модел

Како организациски модел, ќелискиот дизајн е најсоодветен за прикриените групи (криминални и терористички), во споредба со претходните два модела, поради потребата за максимизирање на безбедноста. Пет карактеристики се апликативни за ќелиските организации:

1. целата мрежа претставува поврзана компонента;
2. мрежата е редунтантна на секое ниво;
3. мрежата е мала и динамична на локално ниво;
4. мрежата не се раководи преку контрола, туку преку лидерство засновано на намери и
5. организациската структура не е слободна одлука, туку неопходен одговор заснован според безбедносните ограничувања (Tsvetovat, Carley, 2007).

[4] Забелешка: Ќелијата претставува најмала независна функционална единица (индивидуа или група).

Со цел да ги реализираат нападите, терористичките ќелии имаат потреба од ресурси, информации за целите, експертиза за оружје и набљудување, локации на кои ќе се засолнуваат, како и луѓе што ќе ја извршуваат мисијата. Како резултат на тоа, аналитичарите мораат, исто така, да ги анализираат и да ги определат дополнителните мрежи, со цел да развијат покомплетно разбирање за тоа како тече работата низ мрежата. За среќа, овој концепт на „тек на работа“ се заклучува од социјалните мрежи ако е обезбеден дополнителен контекст (Moon at all, 2008).

Ова води кон наведување метамрежа, која е мрежа од мрежи. Оваа метамрежа има две дефинирачки карактеристики, кои се дека е мултиконтактна, со неколку различни суштински класи како агенти, акции, локации и така натаму, како и мултиплекс, со неколку различни типови конекции како финансиски и директива (Carley, 2006). Тие се исто познати како бипаритни мрежи, каде што контактите од иста класа не се поврзани едни со други, туку, наместо тоа, се поврзани со контакти од различна класа,-.

Една тешкотија во додавање на метамрежите на глобалното терористичко движење е тоа дека мрежите не постојат изолирано од општествата што ги населуваат. Иако тие може да бараат да ја максимизираат безбедноста, не сите терористи може да се кријат во пустина додека да одлучат да изведат напад на друга држава или цел. Поради тоа што определен терорист може да припаѓа на повеќе од еден социјален круг, тие може да имаат повеќе од една припадност, што, исто така, значи дека терористичките групи се вградени во определен степен во општеството од кое потекнуваат. Ова се должи на пресекот на нивните различни припадносни мрежи базирани на нивната способност да припаѓаат на повеќе од една група (Duncan, 2003).

Поврзување на системот е тешко во вакви околности. Од друга страна, пак, релативно е лесно да се додаде метамрежна анализа во релативно изолирана племенска заедница. Племенската заедница има комплексни, но релативно самостојни социјални, економски, воени и разузнавачки мрежи. Ваков самостоен метамрежа опис на племенските заедници може да помогне во објаснувањето зошто овие групи може брзо да се адаптираат за воени акции (Reed, 2007). За жал, овој факт на динамични мрежи го компликува разбирањето на мрежите како прво бидејќи тие може да се променат од минута во минута (Strogatz, 2001).

Истражувањата посочуваат два типа динамики, кои имаат цел целосно да разберат како мрежите еволуираат во текот на времето. Видот на динамиките што најмногу се употребуваат во социјалните мрежни анализи се тие што се занимаваат со природата на интеракциите меѓу контактите, како последица од мрежната структура што е наречена динамика на мрежата (Duncan, 2003).

Оваа категорија раководи со тоа како контактите реагираат еден со друг базирани на целокупната структура на мрежата. Вториот вид мрежна динамика, динамики на мрежата, раководи со промените на мрежната структура и со

еволуцијата на таа структура. За терористичките мрежи, динамиката на и во мрежите се примарно раководени од регрутирање агенти. Како што контратерористичките сили ги извлекуваат терористите од мрежата, динамиката на мрежата диктира како луѓето ќе дејствуваат меѓусебно во новата намалена структура. Ако безбедносните структури убијат важен член на терористичката ќелија, другите агенти мораат да ги користат другите постојни врски за да продолжат да комуницираат и да водат операции. Многу од постојните истражувања, кои може да се аплицираат на динамиката на терористичките мрежи, се базирани на информациските мрежи, како интернет, кои рутински се соочуваат со критични контакти.

Мрежна (networked) природа – клучни карактеристики

1. **Децентрализација и модуларност**
    - Организациите работат како мрежи од автономни ќелии/јазли што можат самостојно да дејствуваат, но и да се координираат кога е потребно. Ова ги прави потешко ранливи на „удари“ против единични лидери.
2. **Хибридизација (слевање на функции)**
    - Терористички групи преземаат криминални практики (трговија со дрога, криумчарење, изнуди), додека криминални мрежи користат политички/идеолошки покритие за свои операции.
3. **Фацилитаторски мрежи**
    - Мрежи на посредници: корумпирани службеници, фиктивни бизниси, логистички оператори и криминални посредници (smugglers, money mules).
4. **Технолошка зависност и изборни алатки**
    - Енкриптирани апликации, darknet платформи, криптовалути, GenAI за автоматизација/пропаганда.
5. **Паралелни легални и нелегални економии**
    - „Преминувување“ на нелегални приходи низ легални бизниси за перење пари и финансирање активности.
6. **Транзитивна и дијаспорска логистика**
    - Дијаспори и мигрантски мрежи што се искористуваат за финансирање, логистика и прикривање на движења.

ГЛАВА III

КОНЦЕПТОТ НА ТЕРОРИСТИ ВОЛЦИ САМОТНИЦИ

Природата на тероризмот значително се промени во текот на последната деценија. Во последниве години, феноменот на таканаречениот тероризам волци самотници се зголеми со сѐ повеќе и повеќе напади извршени од страна на поединечни актери. Промената на природата на тероризмот предизвика дебата за тоа како точно да ги опишат поединците што дејствуваат независно од синџирот на команда на терористичката организација. Концептот на осамениот волк треба да се преиспита и приспособи на променетите околности. Целта на оваа Глава ќе биде фокусирана на една од најнепредвидливите форми на терористички акти – оние што ги извршил еден поединец, т.н. „волк самотник“. Политички, концептот осамен волк се користи за да се увери јавноста и да се каже дека опасноста веќе не е иманентна. Најтешкиот дел во откривањето на волк самотник е дека нивните напади се случуваат во контекст на повеќе идеолошки рамки и не се ограничени само на една група или систем на верување. Во моментов, има повеќе прашања отколку одговори за содржината и валидноста на концептот на волци самотници, но треба да бидеме свесни дека надворешните услови се променија, а старите одговори можеби веќе не се соодветни на денешниот тероризам реализиран од еден поединец.

Неодамнешните настани доведоа до зголемено внимание на релативно ретката форма на тероризам: терористи волци самотници што планираат и спроведуваат напад без помош од други. Тие се гледаат себеси како претставници на некоја поголема група или кауза и може да имаат некое искуство во група, организација или општествено движење поврзано со оваа причина.

Тероризмот „волци самотници“ се перципира како сериозна закана по јавната безбедност во последните неколку години, со оглед на фактот дека оваа појава се интензивира со алармантна брзина.

Концептот на терористи „волци самотници“ е сѐ позачестен привлекувајќи внимание од страна на медиумите како „нова“ и „опасна“ закана. Тој претставува растечки феномен, додека истражувањата на оваа тема се со одредени недостатоци, бидејќи овој вид насилство е еден од најмистериозните и непредвидливи облици/форми на тероризам.

Дефинирање на концептот

Терористите волци самотници ги ризикуваат сопствениот живот и слобода за својата кауза. Зошто некој поединец ќе го преземе овој ризик? Генерално, зошто кој било поединец ќе одлучи да се жртвува за некоја причина?

Одговорот на овие прашања бара, пред сè, длабинско, базирано на докази разбирање на еволуцијата на тероризмот волк самотник, радикализацијата на осамените волци и општествено-политичките контексти во кои се наоѓа феноменот. Овој труд има за цел да обезбеди таков увид. Притоа, трудот се обидува да понуди значајни чекори кон превенција преку обезбедување нови начини на размислување и одговор на тероризмот волк самотник. Ова бара јасна дефиниција на феноменот, односно како се разликува овој вид тероризам од другите видови тероризам.

Прецизна дефиниција на терорист волк самотник е императив, особено затоа што терминот често се злоупотребува или се користи непрецизно. Во овој труд поимот „терористи волци самотници“ се однесува на терористички акции извршени од лице поединец, наспроти оние извршени од страна на терористички организации или државноспонзориран тероризам. Елементот на тероризмот што е истакнат во оваа разлика – имено, субјектот што извршува терористичко насилство (поединец) – следува во традицијата на истражувачите што го дефинираат осамениот волк како „личност што дејствува сама по себе без наредби или врски со одредена организација“ (Burton, Stewart, 2008).

Според оваа формулација, осамен волк не е оној што прави конспирација со други во обид да изврши тероризам. Осамениот волк е осамен по природа и претпочита да дејствува сосема сам, иако неговата или нејзината радикализација кон акција може да биде поттикната од насилни медиумски слики, книги што поттикнуваат на насилство, манифести и фатви.

Во овој труд радикализацијата е дефинирана како процес со кој поединците усвојуваат екстремни ставови, вклучувајќи верувања дека треба да се преземат насилни мерки за политички или верски цели. Додека дејствува независно, волкот самотник е сепак политичко суштество што не извршува чисто егоцентрични цели (Hoffman, 2006).

Не постои професионален консензус за дефинирањето на терористите волци самотници, а некои научници целосно го отфрлаат овој термин. На пример, Џонатан Вајт (2003) тврди дека терминот има мала практична вредност. Тој забележува дека „некои волци самотници подобро е да се перципираат како вистински екстремисти што веруваат дека одат надвор од ограничувањата“, односно „терминот ги слави нивните постапки и не треба да се користи.“ Вајт не е сам во својата критика. Истражувачот за тероризам Брајан Џенкинс (2011), исто така, тврди дека „терористот волк самотник“ е „романтичен термин што наведува на зајадлив и смртоносен сторител“, и кога тоа не е секогаш случај. За да се избегне оваа претпоставена глорификација, истражувачите честопати се осврнуваат на овој феномен со такви псевдонаучни зборови како „тероризам со еден актер“, „тероризам соло актер“, „тероризам со еден актер“, „изолиран тероризам“, „самостоен тероризам“, „идиосинкратичен тероризам“, „осамен одмазднички тероризам“ или „терор на осаменик актер“.

Некои експерти користат широка дефиниција на терорист волк самотник во однос на мотивите и бројот на сторителите што се вклучени. Џефри Симон (2013) го дефинира како кривично дело со употреба на насилство врз

владата, општеството, бизнисот или војската од страна на индивидуално дејствување или со минимална поддршка од еден или двајца други луѓе за остварување политички, социјални или финансиски цели. Оваа дефиниција го вклучува она што Симон го нарекува „криминален волк самотник“ или „оние што го извршуваат нивното насилство за чисто лична или финансиска добивка.“

Додека идеолошката мотивација на волкот самотник делумно објаснува зошто овој феномен добил хиперболичко внимание во академските кругови, токму самиот статус на „осаменик“ го прави овој терорист уникатен, слабо разбран и, што е најважно, непредвидлив во неговиот или нејзиниот избор на цели за насилство. Поради недостатокот на терористички тренинг и логистичка поддршка, волците самотници обично ги избегнуваат тешките цели (како што се добро зајакнати владини згради) во корист на поедноставни напади врз делумно обезбедени меки цели (како што се јавни собири). Овие карактеристики го разликуваат тероризмот извршен од неповрзани поединци од оние што се направени од поширок радикални движења. Далеку повеќе од фигура на говорот, тогаш концептот на „терорист волк самотник“ е епистемолошко препознавање на методите, валидноста и обемот на оваа посебна форма на политичко насилство.

Пол Гил (2015) идентификува три категории:

1. индивидуални терористи што тренираат сами и ги избираат сопствените цели;
2. лица што добиле обука од терористички организации и им биле дадени цели за напад;
3. и парови што можеби се радикализираат едни со други, но што не добиле надворешна насока.

Слично на тоа, други експерти, како Кристофер Хјуит (2003), ја дефинира терористичката група како група што се состои од најмалку четири лица, додека ако се состои од помалку се смета за операција на волк самотник. Во оваа дефиниција, двојките и тријата се сметаат како волци самотници.

Веројатно, ако две или три лица извршуваат акт на тероризам, тогаш тоа веќе не е „осамен“ чин што го извршил „неповрзан“ поединец, бидејќи имало повеќе сторители што биле барем поврзани меѓусебно. Другото прашање се однесува на насилната радикализација. Во случаи на терористи волци самотници, поединецот обично станува радикализиран во рамките на неговите или нејзините сопствени достигнувања, како, на пример, преку насилни медиумски слики, онлајн проповеди и политички сведоштва или лично почитување на терористите што претходно реализирале напади (Spaaij, 2012). Малите терористички групи (вклучувајќи двојки или трија) имаат поинаков вид динамика, при што радикализацијата се случува со конспиративна помош на другите членови на групата (Hamm, 2002).

Без оглед на тоа колку мали ќелии може да бидат двојки, трија штом две или повеќе индивидуи комуницираат едни со други со цел да извршат терористички напад, динамиката на мали групи влегува во игра (Pantucci, 2011).

Напади од волци самотници и пропаганда

Терорист волк самотник е вообичаено некој што дејствува од силно идеолошко или верско уверување, што внимателно ги планира своите постапки и успешно ги крие своите намери од другите.

Полицискиот комесар Бил Братон им изјавил на новинарите дека, во споредба со нападите на ал-Каеда, „ИСИС ќе биде многу повеќе инспирација на терористите волци самотници... Тие се многу софистицирани во своите способности преку своите видеа, преку своите социјални медиуми, преку своите списанија“ (NYPD, 2014).

Првиот напад на волк самотник во Америка, кој беше инспириран од Исламската Држава, се случи на 26 септември 2014 година, кога триесетгодишниот Алтон Нолен го уби соработникот во фабрика за преработка на храна во Оклахома. Тој претходно во затвор ја сменил својата вера, чии дигитални отпечатоци вклучуваат пропаганда на ИСИС (Schuurman et al, 2017).

Експлицитниот повик на ИСИС за поддржувачите од западните земји да извршат терористички напади од типот на „волк самотник“ во своите матични земји стана суштински дел од пропагандата на групата во текот на следните две години.

Истражувачите велат дека терористичкиот напад врз двете џамии во Нов Зеланд бил извршен од еден сторител. Но, повикувајќи се на него како на „волк самотник“ се затскрива екстремно десничарскиот терор.

Како прототип на волк самотник важи норвешкиот терорист Андрес Брејвик, кој на 22 јули 2011 година уби 77 луѓе (Berntzen, Sandberg, 2014). „Европа сè повеќе се навикнува на напади на терористи екстремисти, но делото на Брејвик од него направи најсмртоносен од сите т.н. волци самотници во историјата на континентот“ (Seierstad, 2016). „Замислата дека терористите оперираат сами ни дозволува апстрахирање на врската меѓу насилниот чин и идеолошката заднина“ (Burke, 2017). Теоријата за волци самотници ја јакне посакуваната човечка перцепција „дека одговорноста за насилен екстремизам на поединци ја сноси исклучиво поединецот.“

Терористите на модерната доба не сакаат во секој случај да припаѓаат на една терористичка група со јасен наслов како ал-Каеда или Исламската Држава или т.н. НСУ (Националсоцијалистичко подземје). Сепак, нивната радикализација се случува во општествената клима во која живеат. Интернетот и социјалните мрежи им овозможуваат на денешните терористи досега невидено вмрежување и ширење, дури и пренос во живо на својот чин на „Фејсбук“, како што беше последниот случај во 2019 година во Нов Зеланд.

Многу експерти се согласуваат дека терористите се производ на своето време. Во претходните години се етаблираше општествен тренд, како, на пример, пораст на интолеранција, распламтена од политиката со растечки знаци на популизам. Токму тој копнеж по едноставни одговори поларизира – неистомислениците се странци и непријатели. Етаблирањето на екстремизмот во општеството се зајакнува и со дигитализацијата на човечкиот живот.

Реалните врски се заменуваат со виртуелни, но и виртуелните контакти имаат реални последици. Давид Сонболи, кој на 22 јули 2016 година во трговски центар во Минхен уби девет луѓе, интензивно се движел во виртуелниот свет на мрежата на ксенофоби. Сонболи свесно за датум на нападот ја избрал петгодишнината од терористичкиот напад на Андерс Брејвик, напад што во виртуелниот свет доби пофалби од истомислениците. Дури и џихадистичките атентатори, кои во Европа извршија напади како поединци можни членови на Исламската Држава, пред атентатите имале непосредни контакти со членови на ИСИС во Сирија и Ирак.

Ако Австралиецот Терант е автор на манифестот од 74 страници, тогаш тој изрично се повикува на Андерс Брејвик и на Американецот Дилан Руф, кој во црква во Чарлстон уби девет Афроамериканци. Докажани се контактите на Брејвик и Тернат со други десничарски екстремисти, како во земјата така и во странство. На својот во меѓувреме избришан профил на „Фејсбук“, Терант ги споделувал десничарските идеи и написи за десничарски екстремизам, меѓу кои и најмалку еден текст за десничарски екстремизам меѓу војниците на Бундесверот, кои очигледно за него се браќа според дух.

Брејвик и Терант себеси се гледаат како модерни крстоносци во борба за зачувување на чистата, и веројатно загрозена бела, европска раса. Тие двајцата во муслиманите гледаат наводни „освојувачи“ што стремат кон инвазија во светот.

Концептите членство во групи и дејствувањето самостојно сè потешко може да се применат во свет каде што терористичките организации сè повеќе се организираат преку социјалните медиуми.

Ова докажува дека општествените врски играат клучна улога во текот на процесот што води од идеолошка радикализација до планирањето и подготовката на терористичките напади.

3.1. Појаснување на улогата на мотивацијата за тероризмот волк самотник

Исламофобијата, расизмот и белиот национализам се веќе одамна присутни во парламентите на западните демократии, САД, Австралија, Европа. Во таа смисла е студијата за 119 терористи („волци самотници“), која е објавена во февруари од Меѓународниот центар за терористички студии на Државниот универзитет „Пенсилванија“. Според студијата, големо мнозинство на терористи поединци, чие однесување е истражувано во неа, „редовно се движело во препознатлив и видлив спектар што вклучува однесување и активности на поширока интересна група, општествено движење или терористичка организација“ (International Center for Terrorism Studies, 2013).

Студијата доаѓа до драматичен заклучок. Кај околу две третини од испитуваните случаи, членови на семејството, пријатели или познајници се потврдува дека знаеле за одредена екстремистичка идеологија следена од

извршителите. Во 64 случаи, семејството и пријателите знаеле за намерата на поединец да учествува во некој терористички акт, зашто тоа и усно им го кажал (International Center for Terrorism Studies, 2013).

Волците самотници не се гледаат себеси како осамени волци; токму спротивното е точно. Волците самотници често се сметаат себеси за дел од херојската авангарда што се обидува да заштити поголема група луѓе. Важно е да се разбере дека осамениот волк е етикета прикачена на поединец од екстерни сили, а не од самиот актер. Може да се тврди дека тоа само по себе не ги прави гореспоменатите критериуми неважечки, бидејќи објективно индивидуата дејствувала сама, без оглед на тоа дали тој или таа верува дека припаѓа на една организација или презема дејства во име на група или не. Норвешкиот терорист Андерс Брејвик, кој во 2011 година уби седумдесет и седум лица, и „Unabomber" Тед Качински, кој убил три лица и повредил дваесет и три лица во текот на седумнаесет години, често се користат како типични примери за заканата со еден актер. И двајцата беа поединци што се покажаа способни за планирање и извршување смртоносни терористички напади (Hemmingby, Bjørgo, 2016).

Импликациите од овие наоди за спречување и нарушување на екстремизмот поставен од единствениот актер може да се илустрираат со тоа што ќе се проучуваат радикализацијата на еден актер и однесувањето пред нападот.

Во овој труд, радикализацијата на еден актер се изучува од релациска перспектива. Ова ни овозможи да ги идентификуваме различните степени и видовите „осаменост" во однос на радикалните милеа и групите во поставките за онлајн и офлајн. Нивната осаменост е, во неколку случаи, засилена со претерана смисла на самобитноста, комбинирана со презир за ефикасноста и посветеноста на причината за потенцијалните козаговорници. Некои се едноставно сами, како резултат на значајни промени во нивната социјална средина (Malthaner at all, 2017).

Слично на тоа, лондонскиот бомбардер Дејвид Коупленд, кој започна со солобомбардирање во 1999 година, во кое загинаа три лица, а 140 се повредени, можеби се обиде да формира неонацистичка терористичка ќелија пред да одлучи да нападне сам (McLagan, Lowles, 2000).

На пример, Мохамед Буери, кој го убил контроверзниот холандски режисер Тео ван Гог во 2004 година, бил централна фигура во џихадистичката „Hofstadgroup" (Schuurman et al, 2015).

Нивното актуелно или минато учество во радикалните милеа ги изложува на авторитетни личности и лидери што можат да обезбедат оправдување за употребата на насилство или да обезбедат „модели на улоги" чија вмешаност во тероризам може да ги инспирира сопствените напади на самите актери. За повеќето поединци, повредите или убивањето на други лица бараат надминување на внатрешните морални бариери за употреба на сила (Bandura, 1990). Изложеноста на екстремистички идеологии и авторитетни фигури може да игра клучна улога во овој процес и истражувањата покажале дека 78 проценти од осамените актери биле изложени на надворешни извори на охрабрување или оправдување за употреба на насилство (Schuurman et al, 2017).

Поголемиот дел од терористичките напади на Запад не се изведуваат од добро организирани меѓународни групи. Наместо тоа, терористичката закана на Западот во голема мера доаѓа од волците самотници што се поединци или мал број лица што извршуваат напад за поддршка на група, движење или идеологија без материјална помош или наредби од таква група (Simon, 2013). Овие видови напади сочинуваат 70 проценти од сите смртни случаи на Запад од 2006 до 2014 година.

Ова несовпаѓање нагласува дека терористот волк самотник опфаќа широк спектар на актери со различни мотиви, цели и цели.

Она што покажуваат податоците е дека некои земји имаат многу повисоки нивоа на терор од волци самотници од другите. Податоците, исто така, покажуваат дека нападите на терористи волци самотници во западните земји не се ексклузивно инспирирани од повикот за меѓународен џихад од страна на ал-Каеда и ИСИС (Spaaij, 2012).

Од 2006 до 2019 година, петте најголеми напади на волци самотници на Запад се случиле во четири различни земји. Најголемата категорија напади реализирани од волци самотници на Запад биле политички напади – 37, кои предизвикаа 110 смртни случаи и 135 повреди.

Првиот пример е масакрот во Соединетите Американски Држави, кога еден војник убил 13 лица во воена база во Тексас во 2009 година. Холандија, исто така, имаше кој акт на тероризам од еден напаѓач во 2009 година, кога поединец со својот автомобил се втурнал во толпата за да се обиде да го оштети автобусот во кој било холандското кралско семејство убивајќи седум, а повредени биле 12 лица.

Најголемиот политички терористички напад од волк самотник се случил во Норвешка (Borchgrevink, 2012) во 2011 година кога екстремно десничарскиот терорист Андерс Брејвик спроведе два напади во еден ден убивајќи 77 луѓе, вклучувајќи и деца што присуствуваа на младински камп воден од политичка партија (Global Terrorism Index, 2015).

Вториот најголем напад на волк самотник во САД се случи во Орландо, Флорида, на 12 јуни 2016 година, кога дваесет и деветгодишниот Омар Матејн упаднал во геј ноќен клуб, користејќи пушка и пиштол, и го извршил најсмртоносниот терористички напад од 11 септември, при што загинале четириесет и девет лица и повредил уште педесет и три лица. Пред да биде убиен во полициска престрелка, Матејн викнал на своите жртви: „Време е да се стави крај на бомбардирањето во Сирија“, а потоа ја повикал 911 да ја прогласи верноста кон Исламската Држава (Alvarez, Perez-Pena, 2016).

Последната терористичка акција е извршена од австралискиот Брентон Х. Тарант, кој е обвинет за извршување на масакрот во џамиите „Ал Нуор“ и „Линвуд“ – напад делумно емитуван во живо на „Фејсбук“. Тарант се соочува со 51 обвинение за убиство и 39 обвинениja за обид за убиство (Graham-Mc Lay, 2019).

Екстремистичките политички гледишта, исто така, беа распространети и за нападите во САД од волци самотници мотивирани од желбата да се дојде до

политичка револуција, анархизам и антивладини чувства, опозиција на противниците на хомосексуалните бракови и противење на поборниците на абортусот.

Значајни терористички напади на волци самотници извршени на Запад исто така ги вклучуваат:

- ✓ Anders Behring Breivik (Норвешка, 2011) – напад со експлозив во Осло и масакр на островот Утоја; над 70 жртви. Мотивација: екстремна десничарска, антимуслиманска и антиимигрантска идеологија; напишал долг манифест.
- ✓ Во 2012 година, во Брисел, имам на шиитска џамија бил убиен од бомба поставена од волк самотник.
- ✓ Во мај 2014 година повторно во Белгија, четири лица биле убиени во престрелка во Еврејскиот музеј во Брисел од страна на поранешен член на ИСИС.
- ✓ На 7 јануари 2016 година во Париз, човек со лажен експлозивен појас нападнал полициски безбедносни сили.
- ✓ Omar Mateen (САД, Orlando nightclub, 2016) – масакр во ноќен клуб; дејствуваше сам на самото место. Мотивација: сложена – мешавина од екстремистички симпатии и лични фактори; поврзан со радикализација преку интернет.
- ✓ На 14 јули 2016 година, терорист волк самотник возел товарен камион во толпата што го прославувала Денот на Бастилја во Ница, при што загинаа 85 лица (Global Terrorism Index, 2016).
- ✓ САД, El Paso, 2019 – масакр насочен кон имигранти/латинска популација; расноекстремистички мотив. Посебност: публикуван манифест на интернет во кој ги опишува мотивите.Brenton Tarrant (Нов Зеланд, Christchurch, 2019) – напад врз џамии; директен видеострим и манифест[5]; екстремно десничарско насилство. Посебност: користење livestream.

[5] Терминот **„манифест“** (лат. *manifestum* — јасно, отворено изразено) во контекст на тероризмот се однесува на документ, текст или видео во кое напаѓачот или група го објаснуваат своето идеолошко уверување, целите и мотивацијата за насилното дејствување. Кај „волците самотници“, манифестите имаат централна улога во процесот на само-радикализација, бидејќи служат како: идеолошки водич, оправдување за насилство, средство за ширење на омраза, и начин да се обезбеди „постхумна слава“ и медиумско влијание. **„The Great Replacement“-**Овој 74-страници долг манифест е напишан од **Брентон Тарант**, кој изврши терористички напад врз две џамии во Крајстчрч (Нова Зеландија), убивајќи 51 човек. Насловот се повикува на теоријата на заговор „Големата замена“, според која муслиманските и неевропските имигранти ќе ги „заменат“ домородните Европјани. Манифестот содржи идеолошка комбинација од расизам, антимигрантски ставови и повици на насилство, како и „патокази“ за тоа како да се изврши напад за да се постигне максимален медиумски ефект. Тарант го објавил документот онлајн непосредно пред нападот.

КАТЕГОРИЈА	СУБ-КАТЕГОРИЈА	ДЕФИНИЦИЈА
Расни и религиозни супремацисти	Антиисламизам	Цел избрана поради нивната поврзаност со исламот. Ова вклучува напади врз џамии и напади од одмазда.
	Антисемитизам	Мотивирани од предрасуда против Евреите.
	Бела супремација/ надмоќ	Мотивирани од расистички поглед на светот и може да вклучуваат идентификација со ставовите на нацистите и ККК (Кју Клукс Клан).
Индивидуални прашања	Индивидуални прашања	Нападот се должи на прашања специфични за поединецот. Ова може да вклучува желба да се привлече внимание, одредена догма или дејства поврзани со одредени заблуди што произлегуваат од влијание на дрога или ментална болест.
	Инспирирани од ал-Каеда	Под влијание на ал-Каеда, но и преземање напад без вклученост на ал-Каеда за понатамошно ширење на идеологијата.
Исламски фундаментализам	Инспирирани од ИСИС	Под влијание на ИСИС и преземање напад без вмешаност на ИСИС за да се прошири идеологијата на групата.
	Џихадизам	Инспириран од исламскиот фундаментализам за да се вклучи во насилство. Напаѓачот може да биде инспириран од одредена исламистичка група, но повеќе се фокусира на насилниот џихадизам.
	Антиамериканизам	Напад преземен за да се изрази противење на специфични надворешни политики или други активности од страна на САД и нејзините сојузници.
Политички	Контравладини	Антиавторитарни мотиви за нивниот напад вклучувајќи и отпор кон полицијата, даночната служба, поштата или други инструменти на власта. Анархистите се вклучени во оваа категорија.
	Националистички	Напаѓач инспириран од национализмот – ги вклучува и сепаратистите.
	Политички екстремизам	Акција преземена за да се промовира одредена политичка гледна точка. Ова може да вклучува ставови за имиграција, абортус, ЛГБТ права или кој било друг поглед – екстремистички по дефиниција поради насилството кое е вклучено.

Табела 1. Мотивација на напади реализирани од волци самотници

Заеднички карактеристики и мотиви

- **Идеолошка инспирација:** десничарски екстремизам, религиозен екстремизам, антидржавни/антитехнолошки позиции, расизам.
- **Онлајн радикализација:** честа улога на форуми, социјални медиуми, манифести и видеа во процесот на радикализација.
- **Психолошки фактори:** осаменост, лична изолација, ментални нарушувања или сензација на лична неправда (не значи секогаш болест).
- **Самостојно планирање:** често користат достапни средства и компромитирани знаења; подолгорочно собирање информации.
- **Симболична цел:** сакаат видливост и да предизвикаат јавна реакција; често се обидуваат да останат „во историјата“.

Многу „самотници“ не се целосно изолирани – тие може да имаат индиректна поддршка или пребегнување комуникации, материјална помош или идеолошки врвни влијанија.

Заклучок

Денес, една од најпредизвикувачките и непредвидливи форми на тероризам се насилни терористички дејства извршени од страна на поединци, честопати наречени терористи волци самотници. Еден од главните проблеми во откривање на евентуалните волци самотници е тоа што не постои конзистентен или типичен профил на волк самотник.

Меѓутоа, честата неможност на волците самотници за регрутирање или приклучување кон други лица за терористички цели не значи дека тие ја напуштаат целата општествена интеракција или дека нивната социјална средина нема да учествува во нивното наведување. Волците самотници вообичаено се радикализираат и онлајн и офлајн преку „радикалните милеа“. Преку таквата интеракција, тие развиваат слаби или придружни социјални врски со радикалните актери, дури и ако нивната интеграција и социјализација во овие милеа честопати се делумни, периферни и дисконтинуирани.

Во суштина, нападите од волк самотник претставуваат недефинирана закана за националната безбедност, бидејќи тие се навидум невозможни за предвидување или за собирање разузнавачки информации.

Тероризмот како логика не разликува религии и културни идентитети. Масовниот убиец од Нов Зеланд превиде одлучувачка работа, односно дека тероризмот може да ги дели луѓето, но и да разбуди солидарност.

Терористите волци самотници претставуваат сериозна и комплексна закана поради нивната автономија, онлајн инспирација и тешкотијата проактивно да се детектираат. Најефикасниот одговор е мултисекторски – комбинирање на превенција (заедниците и образованието), процена (службите и експертите) и одговор (правосудство и поддршка), секогаш почитувајќи ги човековите права и етичките стандарди.

ГЛАВА IV

СОВРЕМЕНИ ПРЕДИЗВИЦИ НА КИБЕРБЕЗБЕДНОСТА: ТЕРОРИЗАМ И НАПАДИ ВРЗ КРИТИЧНИ ИНФОРМАЦИСКИ МРЕЖИ

Новиот тероризам се одликува со воен карактер, екстремна бруталност, односно нов стил на дејствување, кој ќе биде поразорен и поубиствен во споредба со традиционалниот тероризам. Новите терористички организации постојано го усогласуваат своето дејствување со современите процеси, достигнување во науката и со техниката, особено со примената на комуникациските технологии и употреба на интернет за потребите на пропаганда, регрутирање, индоктринација, собирање средства и водење психолошка војна. Во економски зависен систем, новиот тероризам ги менува целите и стратегијата на сопственото дејствување. Неговата цел сè повеќе се поместува од едноставен психолошки ефект за креирање страв и несигурност кон цели за масовно разорување делови од светските економски, финансиски или технолошки мрежи (Милошевска, 2016).

Во основа, ако војувањето со информации претставува начин за војување во иднината, тогаш и иднината на тероризмот ќе биде суштински детерминирана со појавата на кибертероризмот. Терористите ги искористуваат придобивките на информатичката технологија, односно од поврзаноста на тероризмот и интернетот произлегува и една нова форма на тероризам – кибертероризмот (Бакрески, Милошевска, 2021).

Кибертероризмот е значаен потсистем на кибервојувањето, и е многу потежок за откривање и спротивставување, бидејќи е скоро неможно да се одреди политичката припадност или спонзорите на неговите извршители. Кога се зборува за поимот кибертероризам, според Федералното истражно биро – ФБИ овој феномен се дефинира како: „предумислени, политички мотивирани напади против информации, компјутерските системи, компјутерските програми и податоци што резултираат со насилство против цели кои не се воени од страна на субнационалните групи или тајни агенти“ (Hower, 2011). За разлика од кибертероризмот, кибервојувањето е насочено спрема информациите и информативните системи што даваат поддршка на цивилните и на воените структури на противникот. Тоа навлегува во сфера што е многу посуптилна од физичките напади и уништувања, односно дејствува врз протокот на информациите во мрежите и манипулира со нив (прекинува, видоизменува, додава и слично). Неговите активности се насочени првенствено кон информациите што се пресудни за функционирање на цивилните и воените системи, како и контролата на авиосообраќајот, стоковите берзи, меѓународните финансиски трансакции, логистичките потреби и цели.

Дефиницијата што ја применува и Сојузниот криминалистички завод го опишува кибертероризмот како „користење киберкапацитети за изведување овластувачки, попречувачки или разорувачки милитантни операции и за инструментализирање на стравот преку насилство или закана со насилство, за да се предизвика политичка промена.“

За Мишевски, кибертероризмот е и насилен акт извршен со користење интернет, преку кражба на доверливи и лични податоци со цел тие да бидат искористени за заплашување или принуда/присила поради остварување одредени политички или општествени цели. Како акт на кибертероризам се сметаат и активностите преку кои намерно се уништуваат голем број компјутерски мрежи, како и персонални компјутери поврзани на интернет, преку користење алатки/програми како компјутерски вируси. Односно, кибертероризмот уште може да се дефинира и како меѓународно користење компјутер, мрежа или јавен интернет за да се предизвика уништување или штета на персонални компјутери (Мишевски, 2017).

Според Петровиќ, кибертероризмот е конвергенцијата помеѓу киберпросторот и терористичките активности, на пример, политички мотивирано хакирање, кое има за цел да предизвика сериозна штета како загуба на човечки животи и/или сериозни економски последици. Основните карактеристики на хакирањето се: насилен планиран пристап, бидејќи станува збор за пробивање на заштитата на системот; неовластеното навлегување („упад“) во системот, кое се базира на високо професионално знаење; местото на „упадот“ е по правило оддалечено од местото каде што се наоѓа напаѓачот; при самото хакирање, напаѓачот истовремено врши и други дела: измами, кражба на идентитет, саботажа, дистрибуција на вируси и сл.; неовластени навлегувања можат да вршат поединци или групи, физички или правни лица (Петровиќ, 2007).

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

Нападот на самонаречениот „киберкалифат“ врз француската телевизија „TV5 Monde“ претставува вовед во ново ниво на кибертероризмот. Акцијата во секој случај беше кибернапад кога истовремено беше прекината програмата на сите 11 канали на таа телевизија и беше преземена контролата врз профилите на „Фејсбук“ и „Твитер“, со импликации за техниката за производство на телевизиска програма. Со часови по нападот телевизијата можеше да емитува само претходно подготвени прилози (Lichfield, 2015). Инцидентот не дојде ненадејно. Сојузниот криминалистички завод уште во 2014 година во една интерна анализа предупреди на терористичките закани од киберпросторот. И

европската полициска агенција Европол во една анализа на ризиците во септември 2014 година укажа на опасностите од кибертероризмот.

Кибертероризмот претставува една од главните глобални закани на современата безбедност. Системи за заштита од ваков вид напади поседуваат меѓународните организации како НАТО и ЕУ и развиените држави како што се САД, Кина, Русија, Велика Британија и други. НАТО е единствената организација што на систематски и стручен начин се занимава со заштита од овој вид тероризам и поседува развиен систем на киберодбрана. За да останат во тек со рапидно променливите облици на закана и за да одржат силен ниво на киберодбрана, НАТО усвои нова и напредна политика и акциски план што го поддржаа сојузниците на Самитот во Велс во септември 2014 година. НАТО силите за одговор на компјутерски инциденти (The NATO Computer Incident Response Capability (NCIRC) ја штитат сопствената мрежа нудејќи 24-часовна поддршка во киберодбраната на разни сајтови на НАТО. НАТО Кооперативниот центар за киберодбрана (The NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE)) во Талин во Естонија е најистакната од страна на НАТО акредитирана институција за истражување и обука, која се занимава со образование, консултации, размена на лекции и развој во врска со киберодбраната (Калач, 2017). Целокупниот овој систем е токму фокусиран и лоциран во Естонија, кога во април 2007 година, се извршени напади врз информациско-комуникациските системи на естонскиот Парламент, во банките, во владата, во медиумите, всушност, во сите значајни државни институции при што предизвикале дестабилизација на државната безбедност, кои од страна на мноштво експерти беа карактеризирани како класичен пример за кибертероризам. Ваквиот вид напад сепак не претставува напад со огромни последици и загуби, голема материјална штета или човечки жртви, но тоа беше првиот напад од такви размери за да се блокираат сите витални институции на државата, со што целиот систем и државата одат во насока на колапс. Многу пострашен исход би имал нападот што би се состоел од навлегување во естонските компјутери и бази на податоци на здравствени или на криминални евиденции, исчезнување на банкарски сметки и сл. (Lewis, 2007)

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

4.1 Ранливост на критичната инфраструктура од терористички напади преку интернет

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

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

- Критичката инфраструктура е ранлива на сите видови напади и сè повеќе напади се извршени преку интернет и сé повеќе е јасно дека ништо на интернет не е безбедно. (World Economic Forum, 2016).
- ИСИЛ веројатно нема да може да изврши спектакуларни напади преку интернет, како што е таргетирање критична инфраструктура, сепак, активно се обидува да регрутира лица способни за извршување напади преку интернет и најверојатно ќе може да го стори тоа. (STRATFOR, 2015).
- Постои зголемена загриженост дека терористичките групи евентуално можат да развијат капацитети за користење интернет и поширок интернет-простор за да спроведат деструктивни напади против критичната инфраструктура, со потенцијал да предизвикаат значителна штета. (ICT4PEACE Foundation, 2016).
- Капацитетот за извршување напади преку интернет не мора да доаѓа од ИСИЛ. Достапноста на алатки и услуги на компјутерскиот криминал на подземните криминални пазари веројатно ќе им овозможи на ИСИЛ и на други терористички организации уште повеќе да ги зајакнат постојните способности. ИСИЛ се обидува да регрутира квалификувани лица способни да реализираат сложени напади преку интернет, Растот на црните пазари на ИКТ им отвора простор на „хакерите за изнајмување“ (STRATFOR, 2015).
- Очекуваниот раст на милијарди уреди преку интернет (индустриски „интернет на нештата“) ќе донесе значителни безбедносни предизвици, вклучувајќи и употреба на IoT од страна на терористите за извршување напади против критична инфраструктура (World Economic Forum, 2016).
- Cloud computing и криптирање ја зголемуваат комплексноста на предизвикот (Council of Europe, 2016).

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

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

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

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

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

5. Комплексности на екосистемите: Денешните софтверски и хардверски опкружувања се повеќе сложени екосистеми населени со мрежа на интерактивни уреди, мрежи, луѓе и организации. Ова значи дека решенијата за компјутерска безбедност честопати бараат доброволно ангажирање, соработка и инвестирање на многу независни субјекти, и покрај тоа што стимулациите и механизмите за преземање вакви активности се дистрибуираат неконзистентно низ екосистемот (World Economic Forum, 2016).

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

- ✓ донесување најдобри практики и киберхигиена;
- ✓ подобрување на системите за автентикација; и
- ✓ подготовка за напади (на пр., со подобрување на форензички способности, развој на планови за континуитет на деловните активности) (Cyber security white paper).

Во делот на компјутерската безбедност значајно место му припаѓа на киберпросторот. Киберпросторот претставува глобален домен во областа на информациите и се состои од независна мрежа на информациски системи и

инфраструктура, вклучувајќи интернет, телекомуникациски и компјутерски мрежи (Kissel, 2011). Со зголемување на зависноста од информатичката технологија, сите државни витални инфраструктури се ранливи на некој вид надворешен напад. Дури и ако експертите не се согласуваат за степенот и за природата на заканата, државите, сепак, треба да усвојат мерки за зајакнување на заштитата на информациските системи. Подигањето на свеста и поттикнувањето на обуката во областа на безбедноста на информациите и заштитата на инфраструктурата ќе бидат исклучително корисни. Тоа треба да вклучува тесна соработка изразена преку изведување заеднички вежби преку кои ќе се врши симулација и моделирање на способност за да се разбере влијанието на можен напад врз меѓусебно поврзаната и меѓусебно зависната информациска инфраструктура. Тоа ќе придонесе за развој на нови можности за детекција и идентификација на можните негативни импликации врз информацискатa инфраструктура.

Киберзакани врз индустриските контролни системи и критичната инфраструктура

Критичната инфраструктура претходно се сметаше за нешто стабилно и конкретно, било да се работи за физички или за информациски и комуникациски системи, но денес е актуелна холистичката перцепција на критичната инфраструктура што претставува збир на мрежи и системи што се од витално значење за општеството како целина. Разликите во концептуализацијата и во дефинирањето на критичната инфраструктура во различни земји се резултат на различната перцепција на заканите и безбедносните ризици и разлики во географските и историските услови, но влијаат и социополитичките фактори (Pursiainen, 2009).

Следејќи ги глобалните трендови, постои реална можност во наредниот период јавниот и приватниот сектор да се соочат со зголемен број кибернапади, вклучувајќи и индустриска кибершпионажа, кибервандализам и идентификација на ранливости кај енергетскиот сектор, финансискиот сектор, здравствениот сектор, транспортните системи и други делови од критичната информациска инфраструктура и важни информациски системи. Притоа, може да се очекува различен пристап, од предизвикување непосредни прекини во функционирањето на делови од критичната инфраструктура до целосно блокирање. Нефункционалноста на гореспоменатите системи може да има фатални последици, а, поради висока хетерогеност на техничките решенија, подоцнежната техничка анализа е значително отежната (Национална стратегија за сајбер безбедност на Република Македонија (2018-2022)).

За да се постигнат безбедна и отпорна мрежна и информациска инфраструктура и заштита на податоци, потребно е редовно спроведување безбедносни мерки, со фокус на превенција, откривање и одговор на инциденти,

развивање нови безбедносни решенија, зајакнување на координацијата и соодветно приспособување на законските обврски (Стратегија за сајбер безбедност (2025-2028))

Информациските системи сè повеќе се соочуваат со закани и со изложеност на ризици од разни извори, вклучувајќи измами со помош на компјутер, шпионажа, хакерски упади или, пак, од т.н. малициозни програмски кодови, односно вируси, кои се сè покомплексни и пософистицирани.

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

- *Кибершпионажа*. Претставува акт или практика на здобивање тајни (осетливи, сопствени или класифицирани информации) од индивидуалци, конкуренти, ривали, влади и непријатели за стекнување воена, политичка или економска предност користејќи нелегални методи за искористување на интернетот, мрежите, софтверот и/или компјутерите.
- *Веб-вандализам*. Напади што ги обезличуваат веб-страниците, или напади со одбивање услуга.
- *Пропаганда*. При овој вид напад можно е да се испраќаат политички пораки кон секој што има пристап до интернет.
- *Собирање информации*. Овој напад се користи со цел информациите што не се чуваат безбедно да се пресретнуваат, па дури и да се модифицираат, овозможувајќи вршење шпионажа од кој било дел од светот.
- *Напади со дистрибуирано одбивање услуга*. Овој напад се карактеризира со можност за искористување голем број компјутери во една или повеќе држави за лансирање напад врз системите на државата од каде што воопшто и не се лансира нападот.
- *Нарушување на функционирањето на опремата*. Жртви на овој напад се воените активности во кои за координација се искористени компјутери и сателити. Користејќи го овој напад, злонамерниците можат да ги пресретнат или да ги изменат наредбите и комуникациите, со што војниците би се ставиле во ризична ситуација.
- *Напаѓање на критичната инфраструктура*. Со помош на овој напад, злонамерниците можат да навлезат во системите за контрола на електрична енергија, водата, горивото, комуникациите, транспортот и слични клучни инфраструктурни елементи и да се обезбеди контрола врз нив со основна цел уценување, кражби, изнудувања, измама и слично.
- *Компромитиран фалсификуван хардвер*. Овој напад се однесува на заедничкиот хардвер искористен во компјутерите и мрежите што имаат злонамерен софтвер скриен во софтверот, firmware-от или дури и во микропроцесорите (Nickolov, 2008).

Нема дилема дека ако може да се каже дека компјутерските мрежи станаа нешто налик на „нервен систем“ на инфраструктурите на цивилниот и на воениот сектор, и онеспособувањето на овој „нервен систем“ ќе значи и парализа на целокупниот систем, на целата земја. Кибернападите може лесно да бидат извршени од страна на криминалци, но може да бидат подготвени од терористички ќелии и меѓународно распространети групации. Ако еден насилен напад над државните инфраструктури го сметаме за акт на војна, тогаш зголемениот број на релевантни актери значи и дека војната не е веќе базирана единствено на политичката рационалност. Цел на нападите може да бидат мали или големи системи, и може да се мотивирани од обичен вандализам, финансиски и политички придобивки, па сè до начин на докажување и заработување, но и престиж во очите на другите „кибервојници“. Географската оддалеченост и границите се исто така неважни, бидејќи една цел може да биде погодена од спротивната страна на светот за само неколку секунди (Johnson, 2015).

Како прв комбиниран напад на кибернапад и воена офанзива се бележи нападот врз Грузија. DDoS – напад од мали размери (напади со дистрибуиран прекин на услугите) врз грузиската интернет-инфраструктура, биле регистрирани во јуни 2008 година, речиси два месеци пред петдневната војна помеѓу Русија и Грузија, по прашањето за Јужна Осетија. На 20 јули 2008 година, фондацијата Shadowserver регистрирала група чувари на интернет што забележале повеќе DDoS напади насочени кон официјалната веб-страница на грузискиот претседател Михаил Сакашвили, кои резултирале со пад на веб-страницата повеќе од 24 часа. Утврдено било дека нападот бил координиран преку американски сервери, факт што ја нагласува транснационалната природа на оваа закана. Според „New York Times“, нападите врз грузиската комуникациска мрежа кулминирале на 8 август 2008 година, првиот ден од војувањето, кога биле регистрирани напади на веб-страниците на владата и медиумите. Како се заострувал конфликтот така ескалирале и on-line нападите што руските хактивисти ги вршеле над веб-страниците на претседателот, Парламентот, Министерството за одбрана, Министерството за надворешни работи, грузиската Народна банка и новинарски агенции. Грузија од кибернападите претрпела мала штета бидејќи грузиската економија и виталната инфраструктура сè уште не биле интегрирани во е-општество. Сеедно, кампањата водена од страна на националистичките хактивисти, поттикнати на акција со помош на рускиот on-line хакерски форум, ефикасно ја нарушила дистрибуцијата на информации на Владата на Грузија, во клучните моменти на нападот.

Овие кибернапади имаа три целни групи:

1. серверите задолжени за интернет-инфраструктурата на државата;
2. веб-страниците на владините институции и важни политичари во земјата и

3. провајдерите на приватниот сектор во земјата (банките, медиумите итн.).

Критичната инфраструктура како цел на кибернападите

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

Нападите насочени кон критичната инфраструктура, без разлика дали зад нив стојат политички, верски, сепаратистички или други видови организации или станува збор за тероризам, индустриска шпионажа, хакерски напади, претставуваат едни од најопасните глобални закани што ја придружуваат денешницата. Новите облици на загрозување што произлегуваат од сè посложените меѓународни односи и новите облици на невоените закани, кои се во согласност со променетиот концепт на безбедност, ги менуваат и концептите на меѓународната, а особено и националната безбедност. Комплексноста и сложеноста на проблематиката што ја третира безбедноста на критичната инфраструктура директно се врзуваат со стратегиите на националната безбедност на голем број држави каде што се добива поширока витална димензија, вклучувајќи економски, стопански, политички и еколошки прашања. Националната безбедност веќе не подразбира исклучиво воени стратегии, туку сè почесто се настојува да се елиминираат невоените загрозувања со воочување на реалната опасност и ефикасна елиминација на истата. Често тоа претставува создавање стратегии на национална безбедност, низ еден деликатен и сеопфатен процес вклучувајќи ја и безбедноста на критичната инфраструктура како составен дел на безбедносниот концепт на секоја држава (Правна рамка за обезбедување на критичната инфраструктура, 2016).

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

Информациското војување (приватни корисници – хакери или, пак, одредени држави можат од различни причини да ги нападнат информациските системи во различни земји и да доведат до големи проблеми не само во

функционирање на информатичката инфраструктура туку и во многу други сектори, со оглед на фактот дека многу се потпираат на информациските системи. Голем дел од оваа инфраструктура е контролиран од индустриски контролни системи – ИКС, кои, исто така, се познати како „Надзорна контрола и стекнување со податоци“ (Supervisory Control and Data Acquisition – SCADA) (Loukas, 2015), програми што се ранливи на хакирање или DDoS напади. Ако заканата не може да предизвика хакирање во системот, тогаш секогаш е можно да се пробие заштитата поради човечки фактор, т. е. корисничка грешка. Многу е полесно да се напаѓаат корисниците (се мисли персоналот) отколку самата опрема. Кога нападот е успешен, опциите за извршување на посакуваниот удар се многубројни. Важно е да се напомне дека повеќето инфраструктурни системи имаат слични проблеми: исти оперативни системи, недостаток на средина во која би можело да се тестира моменталната кибер безбедносна состојба, локален менаџмент и нема присуство на надзор. Програмите се направени за специфични системи што оригинално се поставени во затворени мрежи, па се направени со земање предвид на можноста за високи побарувања, но без заштита на доверливоста или интегрирана заштита (Amoroso, 2011). Сопствениците на овие системи веруваат дека тие ќе бидат заштитени со тоа што се непознати за јавноста и никој нема да хакира во нивните системи. Исто така, тие се чувствуваат недопирливо, тргнувајќи од тоа дека нивните програми во кои целиот систем работи се специјално напишани само за нив, односно се уникатни со конкретни исполнувања што ги бара специфичниот дизајн на хардверот. Повеќето од овие системи користат исти протоколи што се развиени/напишани во истите програмски јазици како и сите други програми на пазарот денес, што пак е релативно лесно да се најдат ранливости во нив. Нападите против SCADA системите се дуплираа во 2014 година на повеќе од 160 000 напади (Dell's, 2015).

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

Инцидент	Што се случи	Клучни лекции / ризици
Collins Aerospace / vMUSE (Европа, септември 2025)	Атака на IT провајдер на аеродромите преку софтверот vMUSE што се користи за чекирање и управување со бординг. Привремени застои на летови, редови, проблеми со логистика на аеродромите.	● Слабости поради зависност од надворешни IT/софтверски провајдери. ● Важност од резервни опции (manual check-in, back-up). ● Потреба од подобро заштитување на софтверската верзија, VPN, интерфејси што се изложени.
JLR (Jaguar Land Rover) напад (В. Британија / глобално, 2025)	Хакери навлегле долго време пред нападот, потоа преку софтверски/цеп-lan управувани системи, кражба на информации и прекин на производство. Производството било стопирано, сериозни пречки за веригата на снабдување.	● Предизвик: откривање и лесно прикривање на напади во софистицирани ИТ/производствени мрежи. ● Значајност на криптографија, сегментација на мрежи, и превентивно тестирање. ● Неопходно е осигурување (cyber insurance) и стратегија за лесно погодно враќање на нормални операции.
Volt Typhoon (САД, U.S. критична инфраструктура, 2023 – 2025)	Група поврзана со државни актери се обидела да воспостави долгорочен, скриен пристап во оперативната технологија на јавните комунални служби, системи за вода и струја. Делумно успеале, но некои од активностите биле спречени/откриени (www.techradar.com)	● Дури и кога нападите не се целосно успешни, потенцијалната штета е голема ● Ризик од поголема зависност од дигитални управувачки системи без соодветна контрола. ● Значајноста на јавно-приватни партнерства за одбрана, и вклучување на менаџментот на CI

Инцидент	Што се случи	Клучни лекции / ризици
		операторите во раната детекција и одговор.
Bremanger Dam Sabotage (Норвешка, април 2025)	Хакери (претпоставено) преку напад ја презеле контролата на брана, отвориле брана со испуштање вода за неколку часа, што е потенцијална хидрокатастрофа. Немаше сериозна флуидна штета бидејќи водостојот бил низок, но практично показател за можноста на физичка и дигитална саботажа (Guardian, 2025).	● Критична инфраструктура што комбинира физички и дигитален контролен систем е подвласна на мешани (hybrid) закани. ● Потребата од мониторинг, строг пристап/контрола на системите со отворен код или надворешен пристап. ● Важноста на вежби за справување со саботажа и сценарија на природни катастрофи + кибер напад комбинирано.

Табела: Светски примери на киберинциденти

Земја	Инцидент / случај	Засегната инфраструктура / јавен сектор	Последици / значајни лекции
Северна Македонија	Напад врз **Министерството за економија и труд** (септември 2024)	Владин сектор / е-услуги / државна администрација	✓ Прекини на интернет и службени имејлови; ✓ можно ransomware; ✓ важност од брза реакција и транспарентност кон јавноста.
Северна Македонија	Кибернапад врз **MEPSO** (оператор на преносен систем на електрична енергија) – март 2024 (Mia, 2024)	Енергетска инфраструктура / критична инфраструктура	✓ Иако не беше загрозено снабдувањето, инцидентот покажува дека и енергетскиот сектор е под ризик;

Земја	Инцидент / случај	Засегната инфраструктура / јавен сектор	Последици / значајни лекции
			✓ потреба од мониторинг и превентивни мерки во енергетските оператори.
Србија	Напад врз **Elektroprivreda Srbije (EPS)** / кибер криминални групи (Qilin) декември 2023 (Kaspersky, 2024)	Енергетска инфраструктура / оператор на снабдување со електрична енергија	✓ Публикацијата на голем обем податоци, ризик за приватност; ✓ иако производството и дистрибуцијата не биле директно прекинати, покажано е дека информациите се ранливи.
Албанија	49 кибер инциденти на критичната инфраструктура во 2023 година	Разни сектори: јавни услуги, IT системи, Можеби енергетски и социјални услуги	✓ Од нив 12 се високо влијателни; ✓ важност од анализа на ризици и развој на техничка и методолошка поддршка за инциденти; ✓ подигнување на капацитетите.
Косово	Напади и DDoS активности кон државни институции, медиумски тела, и друг јавен сектор (спроти политичка и геополитичка мотивација)	Влада / институции / јавен сектор (киберпростор)	✓ Блокирање на веб-страници; зголемен ризик при криза; ✓ потреба од подготвеност, капацитет за реагирање и отпорност на јавните платформи.

Табела: Примери на кибер инциденти во регионот на Западен Балкан

Опасноста од кибернападите во контекст на националната и глобалната безбедност

Во современиот дигитализиран свет, кибернападите се наметнуваат како клучна глобална безбедносна закана, споредлива по сериозност со традиционалните воени и терористички активности. Тие веќе не се ограничени само на кражба на податоци или финансиски злоупотреби, туку директно ја засегаат функционалноста на државните институции, приватниот сектор и критичната инфраструктура, како што се енергетските мрежи, транспортните системи, болниците и банкарскиот сектор.

1. Национална безбедност

Кибернападите можат да ја поткопаат државната сувереност, да ја нарушат довербата на граѓаните во институциите и да предизвикаат дестабилизација на виталните системи. Преку киберпросторот, државни и недржавни актери можат:

- да соберат чувствителни информации (кибершпионажа);
- да блокираат владини комуникации;
- да манипулираат со јавните податоци и дезинформации;
- да саботираат изборни процеси или јавни услуги.

Во такви случаи, националната безбедност е директно загрозена, бидејќи без физичка војна може да се парализира цела држава.

2. Глобална безбедност

На глобално ниво, кибернападите се транснационални по природа – не познаваат граници и не бараат физичко присуство. Поради тоа, тие го поткопуваат класичниот концепт на безбедност базиран на територијалност. Организирани криминални групи и државни актери често дејствуваат преку киберпрокси-мрежи, при што нивните активности може да предизвикаат:

- прекин на меѓународни финансиски системи (SWIFT, банкарски трансакции);
- нарушување на глобалните синџири на снабдување;
- хаос во меѓународниот транспорт и комуникации;
- влијание врз јавниот ред и меѓународните односи.

Овие феномени ја прават кибербезбедноста централна компонента на глобалната безбедност, рамноправна со борбата против тероризмот, климатските промени и нуклеарната закана.

3. Кибернападите како глобални безбедносни закани

Во документите на Обединетите нации (ООН), Европската Унија, како и во стратегиските документи на НАТО, кибернападите се препознаваат како „асиметрични закани“, односно закани што со минимални ресурси можат да предизвикаат огромни штети. Примери како нападот WannaCry (2017), кој погоди болници, енергетски компании и државни системи во над 150 земји, покажаа дека една единствена линија код може да создаде глобална криза.

4. Поврзаност со организиран криминал и тероризам

Современите кибернапади сè почесто се изведуваат или поддржуваат од организирани криминални групи, кои користат технологија за перење пари, шпионажа и финансирање на терористички активности. Киберкриминалот станува главен инструмент за хибридни закани, каде што се преклопуваат криминал, политика, економија и дезинформации.

5. Потреба од отпорност и заедничка одбрана

Справувањето со овие закани бара изградба на национална и меѓународна киберотпорност (cyber resilience), која опфаќа:

- развивање правна рамка за заштита на критичната инфраструктура;
- воспоставување национални компјутерски тимови за инциденти (CERT);
- меѓународна соработка во следење, истраги и санкции;
- подигнување на јавната свест и дигиталната едукација.

Заклучок

Кибернападите денес претставуваат една од најголемите глобални безбедносни закани, која ја редефинира традиционалната концепција на национална и меѓународна безбедност. Тие бараат нови форми на одбрана, мултисекторска соработка и високо ниво на отпорност. За држави како Северна Македонија, изградбата на киберкапацитети и заштита на критичната инфраструктура не е само технолошки туку и стратегиски безбедносен приоритет.

ГЛАВА V

ГЕНЕРАТИВНА ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА И ПОТЕНЦИЈАЛОТ ЗА РАДИКАЛИЗАЦИЈА И НАСИЛСТВО: РИЗИЦИ И ПРЕДИЗВИЦИ ЗА БЕЗБЕДНОСТА

Оваа глава ќе анализира како и до кој степен терористите и насилните екстремисти досега комуницирале преку генеративна вештачка интелигенција и ќе ги идентификува потенцијалните начини на кои би можело да ја злоупотребат генеративната вештачка интелигенција во иднина. Затоа е неопходно да се преиспитаат претпоставките дека терористичките и насилните екстремистички актери брзо ќе ја усвојат генеративната вештачка интелигенција само врз основа на проценатa на способностите што таа може да ги понуди. Иако истражувањата покажаа дека технолошката способност и достапноста се клучни двигатели на терористичките иновации, терористичките и насилните екстремистички актери исто така ја проценуваат секоја нова технологија за нејзината компатибилност (и со нивниот начин на работа и со идеологија), релативната сложеност, трошоците и контекстот во кој тие работат. Разбирањето на овие фактори, и изолирано и во однос еден со друг, ќе биде клучен аспект во следењето на степенот до кој терористите и насилните екстремисти усвојуваат генеративни алатки за вештачка интелигенција.

Со доаѓањето и брзото усвојување софистицирани модели за длабоко учење како што е ChatGPT, постои зголемена загриженост дека терористите и насилните екстремисти би можеле да ги користат овие алатки за да ги подобрат своите операции на интернет и во реалниот свет. Големите јазични модели имаат потенцијал да им овозможат на терористите да учат, планираат и да ги пропагираат своите активности со поголема ефикасност, точност и влијание од кога било досега. Како таква, постои значителна потреба да се истражат безбедносните импликации на овие модели за длабоко учење. Наодите од ова истражување ќе се насочат како составен дел на развојот на ефективни контрамерки за спречување и откривање злоупотреба на овие платформи од страна на терористи и насилни екстремисти. Поточно, се анализираат потенцијалните импликации на командите што може да се внесат во овие системи што ефективно го „нарушуваат“ моделот, овозможувајќи му да отстрани многу од неговите стандарди и политики што го спречуваат основниот модел да обезбедува екстремистичка, нелегална или неетичка содржина. Користејќи повеќе сметки, трудот ги истражуваше различните начини на кои екстремистите потенцијално би можеле да користат различни големи јазични модели за да ги поддржат нивните напори во обуката, спроведувањето оперативно планирање и развивањето пропаганда. Оваа глава ги разгледува потенцијалните импликации и предлага препораки за креаторите на политиките за решавање на овие прашања.

Терминологија

Генеративната вештачка интелигенција (GenAI) е тип на вештачка интелигенција (ВИ) што може да создаде широк спектар на податоци, како што се слики, видеа, аудио, текст и 3Д модели (generativeai.net). Тоа го прави со учење на обрасци од постојните податоци, а потоа го користи ова знаење за да генерира нови и уникатни резултати: „GenAI може да произведе високореална и сложена содржина што ја имитира човечката креативност, што ја прави вредна алатка за многу индустрии како што се игри, забава и дизајн на производ“ (Goaltide, 2023).

Индустријата GenAI се развива брзо, а моделите за основање (како што се моделите на опсежни јазични модели или LLM) се усвојуваат во речиси сите индустрии. Генерирањето текст вклучува користење генеративни модели за учење со вештачка интелигенција за генерирање нов текст врз основа на обрасци научени од постојните текстуални податоци. Една од овие нови апликации е ChatGPT што претставува четбот за генерирање текст, развиен од OpenAI и објавен во ноември 2022 година. Оваа извонредна апликација може да се користи и за злонамерни цели, на пример, од терористи и насилни екстремисти.

Метаверзумот претставува слевање на физичкиот и виртуелниот свет во дигиталната сфера, користејќи 3D технологии и уреди за онлајн комуникација како компјутери и паметни телефони, овозможувајќи им на луѓето да имаат интеракции и искуства во реално време на долги растојанија.

Фразата **насилен екстремизам** се користи во контексти кога екстремистичките погледи на светот се придружени со оправдување и употреба на екстремно насилство (како што се злосторствата) против оние што не го делат истото верување или идеологија. Насилниот екстремизам може да се изрази од поединци или групи преку говори или објави во медиумите, со извршување изолирани акти на насилство во име на екстремистички идеологии или со физичко приклучување кон насилни групи (Aroua, 2018).

Дефинициите за **тероризам** варираат во различни национални јурисдикции и не постои универзално прифатена дефиниција за тероризам. За целите на овој труд, избрано е да се користи скратената верзија на дефиницијата од академски консензус на Шмид (2011), каде што тероризмот е дефиниран како:

„1.Тероризмот се однесува, од една страна, на доктрина за претпоставената ефективност на посебна форма или тактика на генерирање страв, принудно политичко насилство и, од друга страна, на конспиративна практика на пресметано, демонстративно, директно насилно дејствување без законски или морални ограничувања, насочени главно кон цивили и неборци, извршени поради неговите пропагандистички и психолошки ефекти врз различни публика и конфликтни страни;

2. Тероризмот како тактика се користи во три главни контексти:

(i) нелегална државна репресија;

(ii) пропагандистичка агитација од недржавни актери во време на мир или надвор од зоните на конфликт; и

(iii) како недозволена тактика на нередовно војување употребена од државни и недржавни актери.“

Потенцијална злоупотреба на генеративни платформи за вештачка интелигенција

Потенцијалната експлоатација на генеративната вештачка интелигенција од страна на терористите и насилните екстремисти привлече дел од предупредувања, вклучително и дека четботите може да се користат за подведување или радикализирање на младите луѓе (Taher, 2023) или зголемување на ризикот од биотероризам (Sandbrink, 2023).

Веќе во 2020 година, Kris McGuffie и Alex Newhouse (2020) го истакнаа потенцијалот за злоупотреба на генеративните јазични модели со оценување на GPT-3. Експериментирајќи со инструкции што претставуваат различни видови екстремистички содржини, тие откриja значителен ризик за радикализација и регрутирање на интернет од големи размери. Во април 2023 година, Лабораторијата за иновации на ЕУРОПОЛ издаде извештај во кој се претставени некои од начините на кои LLM како што е ChatGPT може да се користат за извршување или олеснување на криминалот, вклучувајќи имитирање, напади од социјален инженеринг и производство на злонамерен код што може да се користи во компјутерски криминал. LLM како ChatGPT имаат потенцијал значително да ги подобрат перформансите на четботови, оддалечувајќи ги од однапред напишаните одговори засновани на правила и зголемувајќи ги нивните квалитети слични на луѓето. Ова доведе до дискусија во врска со потенцијалот за создавање „терористички GPT“, приспособен четбот што може да ги охрабри поединците на патот кон радикализација.

Владините тела, исто така, изразија загриженост за потенцијалните злоупотреби на генеративните платформи за вештачка интелигенција, при што во извештајот на австралискиот комесар за безбедност на интернет што беше објавен во август 2023 година беа забележани многуте начини на кои терористите или другите насилни екстремисти би можеле да ја искористат оваа технологија (eSafety Commissioner, 2023). Во тој извештај, тие изразија загриженост дека терористите „потенцијално би можеле да ги користат овие модели за финансирање тероризам и за извршување измами и киберкриминал;“ дополнително, овие модели би можеле да им овозможат на „екстремистите да создаваат насочена пропаганда, да радикализираат и да таргетираат одредени поединци за регрутирање и да поттикнуваат насилство“ (eSafety Commissioner, 2023).

На почетокот на ноември 2023 година, извештајот на Техниката против тероризмот, иницијатива поддржана од Извршниот директорат на Комитетот за борба против тероризмот на Обединетите нации, заклучи дека сè уште има релативно малку докази за генеративната вештачка интелигенција која е систематски искористена од терористи и насилни екстремисти, дефинирајќи дека нивниот ангажман со технологијата е „во нејзината експериментална фаза“. И покрај прилично малиот сет на податоци, примерите во извештајот се илустративни за најочигледната употреба на генеративната вештачка интелигенција за терористите и насилните екстремисти – производството на

пропаганда. Тие вклучуваат постери генерирани од вештачката интелигенција произведени од медиумски ентитет усогласен со ал-Каеда, слики и мемиња генерирани од вештачка интелигенција на екстремно десничарски канал на „Телеграм“, и транскрипција на пропагандна порака на Исламската Држава од арапски говор на арапски, индонезиски и англиски текст од поддржувач на ИСИС.

Терористите и насилните екстремисти се покажаа како неверојатно приспособливи во користењето на онлајн платформите за да ги унапредат своите цели (Weimann, 2005, 2015). Од појавата на екстремистичките веб-страници во доцните 1990-ти, до новите платформи за социјални медиуми како што се „Фејсбук“, „Јутјуб“, „Твитер“, „Инстаграм“ и „ТикТок“, овие групи брзо ги усвоија и ги искористија новите случувања во киберпросторот. Во поново време, тие исто така почнаа да прифаќаат шифрирани апликации за пораки, како што се „Telegram“, „TikTok“ и „TamTam“. Тие користат анонимни платформи за складирање облак, па дури и Dark Net, нагласувајќи ги нивните континуирани обиди да ги искористат најновите достигнувања и еволуции во дигиталниот свет. „Од своја страна, многу терористи го променија начинот на дејствување, усвојувајќи ги овие нови технологии и спроведувајќи различни оперативни безбедносни мерки дизајнирани да ги избегнат или поразат софистицираните операции за собирање разузнавачки информации“ (Wagner, 2007). За терористите, овие технологии нудат можност за комуникација и координирање на операциите низ целиот свет со разумни очекувања за приватност и безбедност. Вештачката интелигенција можеше да ги искористи новите технологии за поединци и групи, правејќи ја заканата од кибернапади и шпионажа поприсутна од кога било досега (Esmailzadeh, 2023). Таа има потенцијал да биде и алатка и закана во контекст на терористички и екстремистички групи.

Поимот за вештачка интелигенција и тероризам најмногу се фокусираше на потенцијалните употреби на вештачката интелигенција за контратероризам или спротивставување на насилен екстремизам (McKendrick, 2019). Во 2021 година, Канцеларијата за борба против тероризмот на Обединетите нации (2021) објави специјален извештај во кој се разгледуваат можностите понудени од вештачката интелигенција за борба против тероризмот на интернет. Навистина, неколку студии се фокусираа на употребата на вештачка интелигенција во контратероризмот (Verhelst, at all, 2020). Сепак, малку внимание е посветено на истражување на другата страна: како терористите и насилните екстремисти можат да ги користат технологиите базирани на вештачка интелигенција за да шират омраза, пропаганда и да влијаат на ранливите поединци кон нивните идеологии. Неодамна, Глобалниот интернет-форум за борба против тероризмот објави извештај за заканите од екстремистичката/терористичката употреба на GenAI (GIFCT Red Team Working Group, 2023). Потенцијалните употреби на вештачката интелигенција од страна на екстремистичките групи вклучуваат:

- ✓ Пропаганда: Вештачката интелигенција може да се користи за генерирање и дистрибуција на пропагандна содржина побрзо и поефикасно од кога било досега. Ова може да се користи за регрутирање или за ширење говор на омраза и радикални идеологии. Ботови со вештачка интелигенција, исто така, можат да ја засилат оваа содржина, што ги отежнува откривањето и реагирањето.
- ✓ Интерактивно регрутирање: четботови напојувани со вештачка интелигенција можат да комуницираат со потенцијалните регрути обезбедувајќи им приспособени информации засновани на нивните интереси и верувања, со што пораките на екстремистичката група ќе изгледаат порелевантно за нив.
- ✓ Автоматски напади: Терористите може да користат вештачка интелигенција за поефикасно и поефективно извршување напади – на пример, со користење дронови или други автономни возила.
- ✓ Експлоатација на социјалните медиуми: Вештачката интелигенција може да се користи и за манипулирање со социјалните медиуми и други дигитални платформи за ширење пропаганда и регрутирање следбеници.
- ✓ Кибернапади: Вештачката интелигенција може да ја користат екстремистичките групи за да ја подобрат својата способност да лансираат кибернапади врз цели, потенцијално предизвикувајќи значителна штета.

Потенцијални примери

1. **Пропаганда и дезинформација**
    - Екстремистичките групи користат GenAI за креирање слика и визуелни материјали (memes, плакати, видеа) што ги туркаат своите приказни, манипулации и митови (Tech Against Terrorism, 2025).
    - Deepfake видео или аудиозаписи за да се прикажат јавни личности како извршуваат злосторства или изјавуваат нешто што никогаш не го рекле, со цел да се создаде страв или раздор (Nelu, 2024).
2. **Радикализација и врбување (Recruitment)**
    - Користење четботови или AI-генерирани виртуелни личности за комуникација со ранливи лица, кои се изложени на екстремистички влијанија, со цел да ги привлечат, убедат или радикализираат.
    - Генерирање преводи, субтитли и алтернативни верзии на екстремистички пораки за да се прошират нивниот обем и влијание преку различни јазици и платформи.
3. **Психолошка војна и манипулација**
    - Се шират погрешни/измамнички визуелни или текстуални прикази (deepfake, false flag), за да се предизвика паника, хаос или губење доверба кон институции (International Centre for Counter-Terrorism, 2025).

- Користење AI за создавање „токсични“ содржини што ги поттикнуваат омразата, разидувањето, дискриминацијата.

4. **Проблеми со откривање и модерирање**
   - Експерименти покажаа дека GenAI дејствува така што може да заобиколи hash-базирани методи на откривање, кои често се користат за филтрирање екстремистички или забранет материјал. (Tech Against Terrorism, 2025).
   - Автоматизирани алатки за превод, препишување и трансформација на пораки, што им овозможува на овие групи да избегнуваат блокади или цензура.
5. **Поддршка за операции и логистика**
   - Користење AI за креирање упатства, чекори за подготовка на напади, идентификација на ранливи точки или планирање локации преку анализа на достапни податоци.
   - Користење AI-асистенти за шифрување на комуникации, прикривање идентитет, балансирање на социјалната мрежа со нови виртуелни профили.

Индоктринација и регрутирање

Регрутирањето и ангажирањето преку интернет се заштитен знак на современиот екстремизам. Метаверзумот ризикува да ја прошири оваа способност така што ќе им олесни на поединците да се социјализираат и да се поврзуваат (Elson at all, 2022).

Голем дел од досегашната анализа се фокусираше на тоа како генеративната вештачка интелигенција може да помогне во создавањето и ширењето терористичка и насилна екстремистичка пропаганда. Најзначајно, генеративната вештачка интелигенција овозможува создавање нови слики или адаптација на постојните на размер и со брзина што претходно не беше можна. Слично на тоа, актерите сега можат да користат такви алатки за да генерираат синтетичко видео и аудио, вклучувајќи монтирани фалсификати на познати или значајни поединци. Иако доверливоста и квалитетот на видеопродукцијата вообичаено се неконзистентни, лансирањето на OpenAI’s Sora во февруари 2024 година, кое може да генерира видеа врз основа на текстуални инструкции, укажува на брзата брзина со која се развива оваа технологија (Montgomery, 2024).

Конечно, различни LLM што постојано се подобруваат можат да креираат текст користејќи различни стилови, формати и, што е најважно, јазици. Претходно, терористичките групи мораа да се потпираат на мануелни и често релативно слаби преводи на пропаганден материјал, а овој процес во голема мера се потпираше на вештините на неколку поединци. Генеративната вештачка интелигенција теоретски може да се користи за создавање и транскрипција на видео и аудиопропаганда, или генерирање пропаганда базирана на текст, речиси моментално и на повеќе јазици.

Во комбинација, овие случувања создаваат потенцијал за зголемување на обемот и квалитетот на терористичкиот или насилен екстремистички пропаганден материјал.

Во моментов, технолошките компании можат да го споделат „дигиталниот отпечаток од прст“ или „хаш“ на терористичката содржина меѓу себе, овозможувајќи нејзино навремено отстранување и/или спречување да се постави на изворот (GIFCT's Hash-Sharing Database, 2023). Употребата на генеративна вештачка интелигенција за манипулирање со слики може да го промени овој дигитален хаш без суштинска промена на датотеката, ефикасно „уништувајќи го споделувањето хаш како решение“ (Gilbert, 2023). Иако главните платформи можат да идентификуваат и отстранат терористичка содржина на други начини – вклучително и употреба на обработка на природен јазик за да се идентификуваат нови содржини што се слични, но не и идентични со постојната терористичка содржина (United Nations Office of Counter-Terrorism and United Nations Interregional Crime and Justice Research Institute, 2021) – споделувањето хаш е суштинско во напорите на меѓуплатформските напори за спротивставување на терористичката содржина од 2016 година (Meta, 2016). Нејзиното потенцијално деградирање како решение е опишано како „голем ризик“ (Gilbert, 2023).

Важно е да се нагласи дека создавањето терористичка содржина е само првиот дел од процесот. Терористичките актери, исто така, треба да најдат начин со сигурност да складираат и да споделуваат содржина на интернет. Благодарение на комбинација од регулатива, иновативни акции и јавно-приватно партнерство, ова во моментов е тешко да се направи на повеќето големи платформи, со терористички актери наместо да се потпираат на помали, помалку регулирани опции (Wells, 2022). Сепак, клучно е што генеративната вештачка интелигенција им нуди на терористичките актери потенцијална способност да го оптимизираат нивното избегнување на главните контрамерки на платформата, особено употребата на т.н. hash-sharing.

Како може метаверзумот да биде искористен од насилни екстремисти и насилни екстремистички организации?

Метаверзумот може да стане нова територија за терористичка активност, перспективна платформа за подобрување и унапредување на нивните онлајн активности, вклучувајќи радикализација, регрутирање, обука, собирање средства и координација на нападите (Debuire, 2022).

Комбинирањето на вештачката интелигенција со зголемената реалност во метаверзумот ќе им овозможи на екстремистичките лидери да се состанат и да се сретнат со своите поддржувачи, да развиваат и одржуваат виртуелни идеалистички општества и да ги зголемат нивните сфери на влијание. Поради екстремната емоционална средина овозможена од метаверзумот, можеби е предизвик за некои поединци да направат разлика помеѓу реалниот живот и виртуелната реалност (Council of the European Union, 2022). Некои корисници

можеби сметаат дека она што се случува во метаверзумот не е фактичко дури и ако има реални последици по нивните животи. Со спојување на вештачката интелигенција и проширената реалност во метаверзумот, онлајн регрутерите за терористички или насилни екстремистички групи ќе може да се сретнат во виртуелна просторија со потенцијалните следбеници и да ги примамат со визии за иднината.

Прво, метаверзумот ќе им обезбеди на екстремистите уникатна средина за регрутирање нови членови бидејќи тие можат да создадат свои приватни сервери, да допрат до поширока публика и да симулираат мрежи за регрутирање лично. Овие сервери ќе бидат тешки до умерени, а сегашните регулаторни упатства и технолошки механизми не го спречуваат доволно производството на малициозна содржина и однесувања. Како резултат на тоа, метаверзумот ќе послужи како идеален инкубатор за регрутирање екстремисти.

Второ, метаверзумот ќе ги поедностави собирањето средства и киберкриминалот за насилните екстремисти. Преку употреба на криптовалути, компјутерски криминал и перење пари, метаверзумот ќе обезбеди дополнителни слоеви на анонимност и ќе спречи потенцијално откривање од органите за спроведување на законот и од финансиските институции.

Трето, метаверзумот им овозможува на екстремистите способност да го направат поголемиот дел од нивното планирање пред нападот и виртуелно собирање разузнавачки информации. Со ограничување на бројот на пати кога мора да посетат потенцијална цел и минимизирање на времето поминато на интернет за спроведување разузнавачки информации со отворен код, насилните екстремисти ќе можат да дејствуваат дискретно, сепак да одржуваат високо ниво на ефикасност. Дополнително, доколку добијат пристап до серверите што ги користат органите за спроведување на законот за да спроведуваат сопствени виртуелни обуки, насилните екстремисти ќе имаат можност да развијат поефикасни планови за напади и вонредни ситуации.

Конечно, како што технологијата на метаверзумот станува пореална, екстремистите можат да вежбаат создавање и ракување со експлозиви, оружје и спроведување симулации на напади со различни потенцијални нарушувања или променливи промени и да воспостават методи на најдобра практика за да ги постигнат своите клучни цели (Levin, 2024).

Виртуелен тренинг-планирање пред напад

Еден аспект за кој насилниот екстремист може да го искористи метаверзумот е проширување на нивните способности за планирање на напад. Според традиционално разбирање на активностите пред нападот, поединците што планираат да извршат акти на насилен екстремизам развиваат разновидни различни однесувања за да ги планираат своите напади. Во извештајот објавен од Канцеларијата на директорот на заедничкиот тим за антитеристичка процена на националното разузнавање, нивните истражувачи идентификуваа циклус на планирање напади што се повторуваат. Според извештајот, насилните

екстремисти генерално планираат напади во фази што може да се набљудуваат, иако конкретните детали, редоследот и времето може многу да се разликуваат и да се менуваат со текот на времето. Покрај тоа, тие забележаа дека одредени активности полесно се забележуваат од другите. Надзорот пред нападот, обуката и пробите често се набљудуваат и можат да понудат можности за идентификување заговори и спречување напади (ODNI, 2020). Сепак, една голема грижа за метаверзумот е тоа што може да ја отстрани потребата насилните екстремисти лично да го спроведат најголемиот дел од нивното собирање разузнавачки информации пред нападот. На пример, доколку насилните екстремисти станат способни да ја комбинираат метаверзната технологија со други модерни технологии како видеонадзор, лични камери, објави на социјалните мрежи и други можности за пренос во живо, тие можеби никогаш нема да мораат да излезат во јавноста за да соберат разузнавачки информации што им се потребни за извршување на нападите на одредени цели или локации.

Друга област на загриженост во врска со планирањето напад од насилните екстремистички групи е нивната способност да користат метаверзни игри и алатки за обука што се веќе достапни за спроведување на законот и вооружените сили за да се спротивстават на потенцијалните проблеми за време на нивните напади.

Пример за алатките што се веќе достапни и би можело да се менуваат за незаконски цели е AUGGMED (Автоматски генератор на сценарија за сериозни игри за обука за мешана реалност). Целта на AUGGMED беше да развие сериозна платформа за игри за да овозможи обука на крајните корисници базирана на еден и тим со различни нивоа на експертиза од различни организации што реагираат на закани од тероризам и организиран криминал. Платформата автоматски генерира нелинеарни сценарија приспособени да одговараат на потребите на индивидуалните учесници со резултати од учењето што ги подобруваат стекнувањето емоционално управување, аналитичкото размислување, решавањето проблеми и вештините за донесување одлуки. Сценарија на игра вклучуваат напредни симулации на оперативни средини, агенти, телекомуникациски и закани и може да се испорачаат преку виртуелна реалност и средини со мешана реалност преку мултимодални интерфејси. Покрај тоа, платформата AUGGMED ќе вклучува алатки за обучувачите што ќе им овозможат да постават цели за учење, да дефинираат сценарија, да ги следат сесиите за обука, да ги менуваат сценаријата и да даваат повратни информации во реално време, како и да ја оценуваат работата на практикантите и да поставуваат наставни програми за обука за поединечен персонал во фаза по сесијата за обука (European Commission, 2022). Дополнително, штом овие виртуелни сценарија беа креирани и функционираат без никакви технички проблеми, трошоците за реплицирање и споделување на софтверот со други агенции се минимални. Ова овозможува повторна употреба и повторување по ниска цена (Herath & Jarnecki, 2022).

Екстремистите или се приклучуваат на службата со цел да добијат борбена и логистичка обука, или се регрутираат откако нивната служба ќе заврши од радикални групи што се засноваат на комбинацијата од траума, губење на целта и заедницата што често ги погодува ветераните (Ware, 2023). Накратко, пристапот до поранешните органи за спроведување на законот, персоналот на вооружените сили и нивните информации за протоколот за одговор ќе го подигнат успехот на насилното екстремистичко планирање пред нападот во метаверзумот и нивните оперативни способности.

Последната област на загриженост кога станува збор за насилните екстремисти што го користат метаверзумот за планирање напад веќе може да се демонстрира со онлајн игрите како што се „Minecraft“, „Roblox“ и „Sandbox“. Врз основа на јавно достапни планови и распореди, онлајн информации, слики и други технологии за мапирање, корисниците можеа да создадат плејада на виртуелни рекреации на реалната инфраструктура во рамките на овие платформи. Како резултат на тоа, насилните екстремисти веројатно ќе имаат способност да соберат разузнавачки информации едноставно со создавање, преземање или интеракција со овие виртуелни рекреации за да снимаат белешки и да ги идентификуваат сите точки на ранливост што би можело да ги искористат за време на напад. Ова ќе биде особено загрижувачко за владините згради, критичната енергетска инфраструктура, јавните места, универзитетските кампуси, спортските стадиони и сите други локации што може да станат потенцијални цели за насилен екстремизам.

5.1 Симулација на напад

Последната активност што е алармантна и бара итно внимание е зголемената способност на насилните екстремисти да симулираат напади. Како што споменавме погоре, војската со децении ги користи моќите на симулацијата на виртуелна и проширена реалност. Иако технолошките можности на висококвалитетната метаверзна графика сè уште се во развој, софтверските компании се обидуваат да создадат програми што се сметаат за толку реални, што ќе го прекинат неверувањето дека тоа е симулација и ќе ги измамат нивните умови да мислат дека физички се на друго место. Ова ќе се преведе во софтверски програми што ќе им овозможат на корисниците да манипулираат со сложеноста на животот, како што се различни фреквенции на цивили, различни модели на инфраструктура и сообраќај, промена на теренот и различни временски услови. Пример за тоа како ова веќе се манифестира во американските вооружени сили е синтетичката средина за обука, која беше развиена од софтверската компанија „Bohemia Interactive Simulations“, која создава симулации со висока верност за војниците да тренираат насекаде во светот. Оваа верзија на метаверзумот се нарекува One World Terrain и софтверот комбинира тридимензионални податоци собрани од сателити, сензори или скенери и ги комбинира со

дополнителни информации за да направи симулации на терен со висока верност. Понатаму, со дигиталниот свет може да се манипулира со вештачка интелигенција и машинско учење за да се постигнат специфични вежби и резултати за обука (Easley, 2022).

Доколку насилните екстремисти може да добијат пристап до овие софтверски програми, постои бесконечна количина веродостојни сценарија во кои тие ќе манипулираат со алгоритмите до точните спецификации на претстојниот напад и ќе ги симулираат своите активности под големи слоеви на анонимност.

Втората клучна компонента на симулацијата на напад во рамките на метаверзумот што претставува зголемена закана за јавната безбедност е нивната способност да вежбаат со виртуелно оружје и експлозиви. Сега се појавува алтернативна опција каде што корисниците би имале пристап до слични нивоа на анонимност, само што сега ќе биде многу поимпресивна од мрежата Tor. Во рамките на метаверзните сервери, организираниот криминал, како што е трговијата со оружје, може да се одвива релативно лесно под тековниот недостаток на технолошко разбирање, регулација или надзор (INTERPOL, 2022). Што се однесува на конкретно тестирање и купување огнено оружје, постојат компании што веќе имаат изградено контролери за емулирање на огнено оружје што се спаруваат со слушалки за виртуелна реалност што се шокантно реални. Со оваа технологија, корисниците на метаверзумот и насилните екстремисти ќе можат да симулираат употреба на кој било број различни огнени оружја, да ја тестираат нивната ефикасност во голем број симулирани ситуации и да донесат одлука во која преферираат да користат во реалниот живот.

Последната активност и критично важна област на загриженост е како метаверзумот ќе им овозможи на насилните екстремисти да ги вежбаат своите напади. Откако ќе го завршат планирањето пред нападот, ќе ги соберат сите потребни материјали, следниот чекор во циклусот на планирање напад е пробата. Насилните екстремисти често го вежбаат сценариото за напад за да ги потврдат претпоставките за планирање, да ги подобрат тактиките и да ги практикуваат патиштата за бегство. Тие, исто така, може да предизвикаат инцидент на целната локација за да ги тестираат реакцијата на безбедносниот персонал и првите лица што реагираат. Додека ја проценуваат ефикасноста на нивните планови пред нападот, насилните екстремисти, исто така, се обидуваат да ги утврдат условите што фаворизираат највисока стапка на успех и најмал ризик. Факторите што тие вообичаено ги разгледуваат вклучуваат елемент на изненадување, избор на време и место, употреба на тактики за пренасочување и начини да се попречат мерките за одговор. Освен ако насилниот екстремист не планира самоубиствен напад, патеките за бегство и плановите за вонредни состојби се исто така внимателно планирани (ODNI, 2020). До неодамна овие активности најчесто се извршуваа лично. Сепак, со додавање метаверзум технологија, насилните екстремисти би можеле да имаат неспоредливи можности за вежбање (Elson et al., 2022). На пример, насилните екстремисти можат да симулираат различни потенцијални нарушувања или симулирани

ситуации и да воспостават методи на најдобра практика за сепак да ги постигнат своите клучни цели. Ова ќе им овозможи на насилните екстремисти да ги реплицираат силите за спроведување на законот и цивилните одговори, да научат остварливи и ефикасни патеки, да ги координираат алтернативните рути доколку некои од нив се блокираат и да воспостават повеќе планови за вонредни ситуации доколку дојде до прекини.

Заклучок

- **Широка пристапност**: Генеративните AI-алатки се поевтини и се достапни на многу луѓе, што значи дека и „малите актери“ (аспиративни екстремисти) може да ги користат.
- **Брзина и скала**: Со AI, пораките, материјалите, deepfake и текстовите може да се создаваат, преведуваат и шират многу побрзо отколку порано.
- **Тешкотија при откривање**: Deepfakes и синтетичките материјали може да изгледаат реално и да го заобиколат филтрирањето на податоци.
- **Влијание врз јавната перцепција**: Кога јавноста не може лесно да ја препознае лажната содржина, тоа ја поткопува довербата во медиумите, институциите и лидерите.
- **Интеграција со други закани**: Генеративниот AI не е самостоен; се комбинира со кибернапад, социјален инженеринг, финансирање, разузнавање. Тоа ја прави заканата мултисекторска.

Терористичките и насилните екстремистички групи и поединци покажаа дека можат многу добро да се приспособат и значително да еволуираат во текот на деценииите. Тие покажаа потенцијал за иновација, на пример, во нивната организациска структура, станувајќи децентрализирани, франшизирани и глобални.

Импликациите покажуваат дека метаверзумот наликува на Пандорината кутија; технологијата што се појавува е многу посложена отколку што можат да се справат нашите сегашни системи, а последиците би можело да бидат поразителни. Треба да се следи еволуцијата на усвојувањето на вештачката интелигенција од страна на терористички групи и поединци.

Зголемената соработка помеѓу приватниот и јавниот сектор, меѓу академската заедница, високата технологија и безбедносната заедница, би ја зголемила свеста за потенцијалната злоупотреба на платформите засновани на вештачка интелигенција од страна на насилните екстремисти, поттикнувајќи го развојот на пософистицирана заштита и контрамерки. Треба да се истражи употребата на вештачка интелигенција и поврзаните нови технологии за спротивставување на терористичките закани овозможени со вештачка интелигенција, особено за да се спротивставиме на терористичката радикализација и да се шират позитивни наративи.

ГЛАВА VI

КРИПТОВАЛУТИ И ГЛОБАЛЕН ТЕРОРИЗАМ – НОВИ БЕЗБЕДНОСНИ ПРЕДИЗВИЦИ

Виртуелните валути, вклучувајќи криптовалути како што е Bitcoin, добија значителна популарност во текот на изминатите неколку години. Целта на трудот е да се согледа дали терористичките организации и терористичките групи во моментов користат криптовалути за финансирање на своите активности и, ако не, зошто не ги експлоатираат ваквите валути. Криптовалутите се лесни за употреба, безбедни и, доколку се користат правилно, можат да го сокријат идентитетот. Последните истражувања тврдат дека терористите ги користат дигиталните криптовалути за финансирање на своите активности. Дали е точно тоа тврдење, и, ако е така, до кој степен? И, има ли реални примери што може да се потенцираат? Особено, факторите што имаат тенденција да ја обесхрабрат употребата содржат континуирана непредвидливост во општествата за криптовалути, соработка меѓу меѓународните полициски служби и разузнавачката заедница и развојот на регулативата и спроведувањето. Прашањето дали терористичките организации ќе ги користат овие системи зависи од достапната технологија, како и од потребите и способностите на овие групи.

Постои голема потреба да се разбере целосниот потенцијал за терористичка употреба на криптовалути, вклучувајќи опции за идентификување и следење на нивната употреба, софистицираност и технолошка способност на терористички групи и потенцијал за такво користење да се зголеми во иднина, со оглед на очекуваниот технолошки развој (Dion-Schwarz at all., 2019).

Сепак, предизвикот поставен од криптовалути се протега надвор од опсегот на биткоинот. Многу нови криптовалути се појавија во изминатите неколку години, вклучително и такви алтернативни валути (altcoins) како што се Omni Layer (MasterCoin), BlackCoin и Monero, кои се промовираат како поприватни и побезбедни од Bitcoin. Zcash е друга криптовалута што нуди повисок степен на приватност и обезбедува потенцијална можност за користење и трансфер на валута офлајн, што може да го отежни спроведувањето на Законот за откривање незаконски трансакции. Другите криптовалути, вклучувајќи го и Хок, можат да овозможат целосно приватни договори и трансакции на блок-синџирот Ethereum. Како и биткоин, блок-синџирот Ethereum е дистрибуирана компјутерска платформа и оперативен систем (Dion-Schwarz at all., 2019).

Терминологија

Криптовалута означува дигитална валута произведена од јавна мрежа, наместо од која било влада, што користи криптографија за да се осигури дека исплатите се испраќаат и примаат безбедно (Cambridge Dictionary).

Дигиталниот дел се однесува на користење електронски систем што користи бинарен број за снимање звук или зачувување информации и што дава висококвалитетни резултати (Oxford Learner Dictionary, 2008).

Тероризмот е употреба на насилство за политичка цел. Тероризмот е употреба на насилство врз случајни цивилни цели со цел да се заплашат или да се создаде генерализиран сеприсутен страв заради постигнување политички цели (Yonah, 1976). Дефиницијата за тероризам еволуираше со текот на времето, но неговите политички, религиозни и идеолошки цели практично никогаш не се променија (Sloan, 2006).

Денес, тероризмот се промени единствено во однос на својата димензија, актери, платформа и активности. Тероризмот вклучува акти на киберхакерство, трговија со дрога, киднапирања, тортура, атентати, пропаганда, саботажа, вандализам, воздушни бомбардирања, киднапирања, самоубиствени напади што вклучуваат чин на насилство кон општеството (Jackson at all, 2011).

Оваа публикација ја користи организациската теорија за тероризам иницирана од Марта Креншоу (2008). Организациската теорија најмногу ги дискутира целите, дејствата и внатрешната динамика на терористичката организација. Оваа теорија ја нагласува главната цел на терористичката организација, а тоа е опстанокот што може да се илустрира како државна институција или комерцијално претпријатие. Како одговор на надворешните притисоци, терористичката организација ќе ги менува, односно адаптира своите намери преку иновација (Ozdamar, 2008).

6.1. Можности на криптовалутите за олеснување на финансирањето на терористичките операции

На терористите им се неопходни значителни финансиски средства за извршување напади и други активности. Доколку терористичките групи се подобро финансирани во целина, може да има почести, поуспешни и поголеми напади (Acharya, 2009). Постојат неколку причини што ја поддржуваат оваа хипотеза.

Прво, повеќе средства за операции веројатно ќе доведат до зголемено финансирање на структурите што ги овозможуваат овие напади, кои вклучуваат регрутирање и обука на напаѓачи и инспирирање потенцијални осамени волци.

Второ, групите што се соочуваат со помал монетарен притисок (т. е. оние што се подобро финансирани) исто така може да бидат поподготвени да ризикуваат, како што се поголеми или поризични напади (Shapiro, 2012).

И на крај, а можеби и повеќе спорно, зголемените средства може да се користат директно за дополнителни и поголеми напади. Можеби е тешко директно да се поврзат зголемените средства со терористички напади, иако во специфични документирани случаи „литературата често опишува недостиг на готовина како проблем за терористички операции“ (Oftedal, 2015).

Дали и како терористичките организации би користеле систем на криптовалута зависи од достапната технологија и нејзините својства, како и од потребите и можностите на организацијата. Поновите криптовалути може да се појават со својства што терористичките организации ги сметаат за попривлечни од оние на моментално достапните криптовалути. На пример, ако идната криптовалута обезбедува подобра анонимност од биткоин за големи трансакции и е пошироко усвоена од Zcash, тогаш терористичките организации би можело да бидат подготвени да ја користат таа валута за специфични активности. Затоа, важно е да се разгледаат одделни терористички групи за да се анализира што би им требало од криптовалутите и да се споредат тие потреби со својствата на достапните криптовалути.

Биткоинот постојано го користат купувачите и потрошувачите на недозволени добра и услуги на темната мрежа. Во извештајот под наслов „Терористичка употреба на виртуелни валути: содржана потенцијална закана“ се наведува дека терористичките организации ги користеле криптовалутите за да го поддржат опстанокот на своите организации. На пример, терористичката организација во појасот Газа ги искористи криптовалутите за финансирање на нивните операции, како и членовите и приврзаниците на Исламската Држава во Ирак и Сирија (ИСИС), кои особено ги користеа криптовалутите евидентирани во Индонезија и САД. Забележувајќи понатаму дека значителното и ненадејно губење на нивната физичка територија, како и ширењето на опсегот на воените операции може да го ограничат нивниот пристап и да ги отежнат преместувањата на нивните финансии преку географските области и границите или традиционалната финансиска трансакција наречена хавала што се однесува на физичката финансиска трансакција со користење локален брокер за трансфер на пари помеѓу локации (Ward, 2018). Така, овој феномен потенцијално ги охрабрува терористичките организации да ја истражуваат новата технологија што може да ја поддржи нивната способност да ги движат средствата преку криптовалути преку низа примери: конкретно, ал-Каеда и придружните организации, Исламската Држава во Ирак и Сирија (ИСИС), Хезболах, наркотерористички организации и терористи волци самотници. Иако овие групи се разликуваат во нивните цели, нивната потреба за анонимни, безбедни и подготвени насоки на финансирање ги прави криптовалутите со потенцијална вредност за нив. За овие групи, се испитани пет финансиски активности (прибирање финансиски средства, нелегална трговија со дрога и оружје, дознаки и трансфер на средства, финансирање напади и оперативно финансирање) и се

процени важноста на криптовалутните својства во олеснувањето на овие активности (Dion-Schwarz at all., 2019).

Постојат различни начини на кои може да се користат виртуелните криптовалути од страна на терористичките групи. Организациите можат да ја користат темната мрежа за добивање оружје, вклучувајќи традиционално огнено оружје, експлозиви, хемиски или биолошки токсини, плаќајќи ги со виртуелни криптовалути. Виртуелните криптовалути исто така може да олеснат други активности за недозволени приходи од терористички групи; имало, на пример, виртуелни барања за криптовалути за време на киднапирање за откуп, а киднапирањето за откуп е популарен извор на приход исто така и за терористички организации. Слично на тоа, ако терористичките организации се насочат кон повеќе дигитални напади или кибертероризам, виртуелните криптовалути може да станат покорисни за овие организации бидејќи дозволуваат набавка на „дигитално оружје“, како што е малициозен софтвер. Очигледно, виртуелните криптовалути не се клучни за ниту една од овие активности, но тие можат да ги направат овие трансакции полесни од традиционалните плаќања со картички или банкарските трансфери (Entermann and Berg, 2018).

Дополнителен аспект што може да го забрза усвојувањето виртуелни криптовалути од страна на терористичките групи е конвергенцијата на терористичките и криминалните организации. Терористичките групи веќе долго време користат организирани криминални средства, како што е шверц на тутун, за финансирање на своите активности и има многубројни примери за соработка помеѓу двата типа на групи. Овие се движат од односот на ЕТА со колумбиските наркокартели и олеснувањето на шверцот со кокаин во Европа, до соработката на ПИРА со источноевропските шверцери со луѓе и соработката на Хезболах со мексиканските наркобосови. Во поново време, има зголемен акцент на таканаречената поврзаност криминал – терор, на пример преку движење на лица со криминално минато во терористички мрежи. Најмалку две третини од лицата со оперативна врска со Исламската Држава што извршија напади во Европа и Америка во изминатите неколку години имаа криминално минато (Basra, Neumann, 2017). Постојат докази дека криминалните „вештини“, како што се пристапот до фалсификувани документи и оружје, лесно се користат во нивните нови екстремистички средини. Со оглед на овие случувања, може да биде само прашање на време додека не се извезат виртуелните алатки и тактики на криптовалути што ги користат криминалните синдикати во терористички групи; или дека соработката и трансакциите меѓу терористички и организирани криминалци може да вклучуваат виртуелни криптовалути (Entermann and Berg, 2018).

Овие дигитални криптовалути поседуваат својства како анонимност, употребливост, безбедност, прифаќање, сигурност и волумен. Под анонимност мислиме на можноста да се скрие и заштити идентитетот на корисникот. Употребливоста се однесува на леснотијата со која корисникот може да спроведува трансакции и да управува со сопствената валута. Безбедноста се

однесува на степенот до кој инфраструктурата на криптовалутата обезбедува доверливост, интегритет и точност на трансакциите и корисничките сметки. Под прифаќање мислиме на степенот до кој валутата е прифатена од корисничката заедница, како и големината на заедницата на корисници. Сигурноста се однесува на брзината и достапноста на трансакциите, како што гледаат корисниците. Конечно, волуменот се однесува на просечната временска збирка на трансакции во инфраструктурата на криптовалутата.

Моментални и идни потреби на терористичките организации за криптовалути

Прашањето дали и како терористичките организации би користеле систем на криптовалута зависи од достапната технологија и нејзините својства, како и од потребите и можностите на групите. Поновите криптовалути може да се појават со својства што терористичките организации ги сметаат за попривлечни од оние на моментално достапните криптовалути. На пример, ако идната криптовалута обезбедува подобра анонимност од биткоинот за големи трансакции и е пошироко усвоена од Zcash, тогаш терористичките организации би можело да бидат подготвени да ја експлоатираат таа валута за специфични активности. Затоа, важно е да се разгледаат одделни терористички групи за да се анализира што им е потребно од криптовалутите и да се споредат тие потреби со својствата на достапните криптовалути (Dion-Schwarz at all., 2019).

Сепак, особено со подобрена употребливост, криптовалутите, како што е биткоин, може да бидат привлечни за употреба при прибирање средства, а се појавуваат некои докази дека терористичките организации може да користат криптовалути за оваа намена (Stalinsky, 2018).

Современите криптовалути се потенцијално многу пофлексибилни, а тоа може да создаде предизвици во финансиското сметководство, особено за оние што се вклучени во спречување компјутерски упади. Областа на криптовалутите е помалку сигурна, многу подинамична каде што иновациите може да им овозможат на терористичките групи да го заобиколат мониторингот. Од друга страна, тоа е поле каде што софистицираноста е важна; перењето пари може да биде потешко да се открие кога го спроведуваат софистицирани актери, но техничките способности на многу терористички групи во моментот не се соодветни за овој вид активност (Dion-Schwarz at all., 2019).

Зголемената употреба на криптовалути на комплементарни и соседни пазари може да укаже на нивната зголемена одржливост меѓу терористичките организации. Некои операции за фалсификување започнаа да користат темни мрежи и постои значителна трговија со украдени кредитни картички и идентитети на овие пазари (Aliens, 2012).

Улога во поширок контекст	Специфични случаи	Опис
Овозможување анонимни финансиски трансакции	Употреба на биткоин преку Tor за анонимност	Додадено ниво на анонимност и претпазливост (DiPiero, 2017)
	Перење пари на криптовалути преку Tumbling услуги	Специфични услуги за перење пари, на пр., преку конвертирање во биткоини (Dalins et al., 2017)

Постојат неколку недозволени цели на искористување на криптовалутите од терористички организации, како што се набавка на дрога, продажба на наркотици, оружје и дозволување недозволени услуги во темната мрежа. Покрај тоа, терористичките организации започнаа, односно промовираа сопствени донации преку криптовалутите. Може да се заклучи дека криптовалутите може да се претворат во исплата на откуп. Покрај тоа, постојат неколку карактеристики на криптовалути што обезбедуваат предности за корисниците, односно се подобри од готовина или кредит, разменливи за стоки и услуги, конвертибилност и стабилност на вредноста (нестабилност на цената на билансот) (Everette, 2017).

Документирани примери за терористичко стекнување криптовалута

Терористичките мрежи се приспособија на технологијата, вршејќи сложени финансиски трансакции во дигиталниот свет, вклучително и преку криптовалути (The US Department of Justice, 2020).

Врз основа на студијата спроведена од RAND Европа насловена „Зад завесата: недозволена трговија со огнено оружје, распрскувачки материи и муниција на Мрачната мрежа“, постои директна врска помеѓу терористичките напади во Париз и Минхен, како и со оружјето што било набавено преку темната мрежа со криптовалути. Студијата покажува дека имало дваесет и четири пазари на француски и британски криптовалути на темната мрежа во текот на септември 2016 година, каде што 75 проценти од трансакциите докажале дека реализираат незаконска трговија со оружје (Everette, 2017). Оружјето што го користеле напаѓачите може да биде поврзано со пропагандата на ИСИС што повикувала на ширење поедноставни напади со употреба на возила, огнено оружје, оружје, хемиско оружје и ножеви. Покрај тоа, организацијата поврзана со ал-Каеда, имено al-Sadagah, користела „Фејсбук“ и „Телеграм“ за да ја започне својата финансиска кампања преку биткоин (Malik, 2018).

Во текот на изминатата година, терористичките групи се свртеа кон стекнување и складирање богатство во виртуелни валути како биткоини. Во

август 2020 година, Министерството за правда на САД ја објави најголемата заплена до денес на криптоактиви поврзани со терористички групи. Министерството за правда на САД објави дека запленило еквивалент на милиони долари преку повеќе од 300 сметки на криптовалути поврзани со три назначени странски терористички организации во САД, имено Хамас, ал-Каеда и т.н. Исламска Држава. Во 2019 година, военото крило на Хамас започнало кампања за собирање средства на криптовалути преку интернет со помош на алатки за социјални медиуми за поттикнување анонимни донации. Спротивно на популарното верување, анонимноста често поврзана со криптовалути е погрешна именка. Шемата на Хамас последователно се расплетува, со запленети 150 сметки на криптовалути.

Ал-Каеда, исто така, се разграничи со користење алатки за социјални медиуми за да генерира интерес од донатори со цел да ги поддржи своите активности во Сирија преку криптовалута. Во случајот на ал-Каеда, Министерството за правда на САД заплени повеќе од 100 сметки на криптовалути. Интересот на Хамас и ал-Каеда за криптовалута, соодветно, претходеше на објавата на Министерството за правда на САД, но овој прилив на финансии привлече многу помалку внимание во однос на другите извори на финансирање (IntrelBrief, 2020).

Како и Хамас и ал-Каеда, ИСИС беше вмешан во соопштението на Министерството за правда во август 2020 година. Слично како на Хамас така и на ал-Каеда, лицата поврзани со ИСИС вклучени во шеми на криптовалути не се нови. Во 2017 година, Зообија Шахназ обезбеди 85 000 УСД на ИСИС со тоа што ги зголеми кредитните картички за да купи биткоин, а потоа го претвори биткоинот во готовина за да ги замагли нелегалните активности. Две години пред шемата на Шахназ, Али Шукри Амин се изјасни за виновен за обезбедување материјална поддршка на ИСИС, покажувајќи им на луѓето како да стекнат и испратат биткоин до групата. Последните напори за криптовалута беа спроведени од Мурат Цакар, хакер на ИСИС (и поврзан со Шахназ), кој создаде веб-страница со наводна продажба на опрема за лична заштита, вклучително и маски за лице N95, заради профит. Со оглед на епидемијата на КОВИД-19 и тешкотиите поврзани со лични финансиски потфати, случаите во август 2020 година може да претставуваат стожер на организирани терористички групи кон стекнување виртуелни средства. Особено ИСИС веројатно ќе продолжи со напорите за собирање богатство преку операции овозможени преку интернет, од кои некои може да вклучуваат криптовалута (Soufan Center, 2020). На почетокот на 2019 година, бригадите ал-Касам објавија повик на својата страница на социјалните мрежи за донации на биткоин за да ја финансираат својата терористичка кампања. Бригадите ал-Касам потоа го пренесоа ова барање на своите официјални веб-страници, alqassam.net, alqassam.ps и qassam.ps. но ваквите донации не беа анонимни. Работејќи заедно, агентите на IRS, HSI и FBI ги следеа и запленија сите 150 сметки на криптовалути што пореле средства од и од сметките на бригадите ал-Касам.

Во 2020 година, Работната група за финансиска акција (FATF), меѓувладино тело, го потенцираше можното зголемување на терористичкиот интерес за криптовалутата, особено за време на пандемијата КОВИД-19. Во мај, FATF објави извештај во кој се тврди дека пандемијата на коронавирус може да доведе до „зголемување на злоупотребата на онлајн финансиски услуги и виртуелни средства за преместување и прикривање недозволени средства.“ Помалку од еден месец по објавувањето на Министерството за правда на САД, FATF објави друг извештај за индикатори со црвен аларм, истакнувајќи дека виртуелните средства може да се користат од финансиери на тероризам и перачи на пари. Индикаторите се движат од уникатни модели на трансакции до профили на географски ризик што може да укажуваат на злоупотреба на виртуелните средства. За единиците за финансиско разузнавање, давателите на услуги за виртуелни средства и финансиските институции, овие индикатори обезбедуваат корисни упатства за спротивставување на употребата на криптовалута од низа недозволени актери. И покрај упатствата на FATF и потегот од август 2020 година на Соединетите Американски Држави за запленување и барање одземање на финансиските средства на Хамас, ал-Каеда и ИСИС, терористите сè повеќе користат криптовалута за да собираат и складираат богатство. Овој пат е особено веројатен поради веројатното континуирано потпирање на „виртуелно“ деловно работење дури и откако ќе се дистрибуираат вакцините КОВИД-19 во текот на 2021 година. Бидејќи повеќе секојдневни потрошувачи користат криптовалути, можностите за терористите ќе се зголемуваат, бидејќи тие бараат покривање и прикривање на зголемениот обем на вкупните трансакции (Soufan Center, 2020).

Терористите користат виртуелни валути за да избегнат откривање и прибирање финансиски средства. Терористите, како криминалци, користат криптовалути бидејќи тоа обезбедува иста форма на анонимност во финансискиот амбиент како што е криптирањето за комуникациските системи (Weimann, 2016). Генерално, употребата на криптовалути треба да се гледа како дел од општата промена кон тероризмот преку интернет (Casadei Bernardi, 2019).

Оваа Глава покажува дека, доколку се појави криптовалута што обезбедува широка имплементација, подобра анонимност, засилена безбедност и што подлежи на несигурна регулација, тогаш можната корисност на оваа криптовалута, како и потенцијалот за нејзино користење од страна на терористичките организации ќе се зголемат.

Злоупотреби што создаваат најголема загриженост (трендови)

- **Брзо повикување за донации по поголеми настани/конфликти:** во кратки временски прозорци, кампањи повикани од групи или симпатизери можат да соберат значителни криптоволумени. (thesoufancenter.org, 2024)
- **AI и автоматизација во ширење повици и „phishing“ за донации:** автоматизирани ботови и платформи можат да помагаат во агитација, а

криптовалутите го олеснуваат брзото примање средства (www.fatf-gafi.org/)

- **Крипто како дел од хибридни финансиски мрежи:** комбинација од крипто, даркнет/OTC услуги и традиционални сметки — што го комплицира следењето (www.fbi.gov).

Заклучок

Загриженоста за употребата на криптовалута за да се дозволат терористички активности допрва треба да биде очигледна, но идниот развој на технологиите за криптовалута веројатно ќе има значителна долгорочна последица врз финансирањето на тероризмот. Брзината со која се прифаќаат овие технологии и деталите за тоа кои технологии се користат и како се организирани се критични несигурности што имаат важни оперативни влијанија. Овој труд предлага регулирање на криптовалутите, заедно со меѓународната соработка меѓу спроведувањето на законот и разузнавачките служби, да бидат императив чекори за да се спречат терористичките организации да користат криптовалути за финансирање на своите активности.

Безбедноста во опкружувањето на криптовалутите е од умерена до висока позиција за терористичките организации, бидејќи постојните криптовалути се изложени на разновидност на кибернапади.

Сè уште новите врзани валути за кои се претпоставува дека ја унапредуваат безбедноста се предмет на значителен надзор бидејќи со текот на времето се откриваат нови слабости на безбедноста. Кога ги анализираме заемно сите аспекти, вклучително и други значајни фактори како што се конзистентноста и капацитетот на пазарот на криптовалути, ќе откриеме дека ниту една постојна криптовалута не може да ги реши сите финансиски потреби на терористичките организации.

Не постои „едно решение“ – потребен е мултидимензионален одговор: законодавство, технолошки контрамерки, финансиска верификација и меѓународна операционална координација, додека околу етичкиот/правен контекст важно е да се одржи баланс помеѓу приватноста на корисниците и националната/глобалната безбедност – мерките мора да бидат правно основани и транспарентни.

ГЛАВА VII

ВЛИЈАНИЕТО НА КОВИД-19 ВРЗ ГЛОБАЛНИОТ ПОЛИЦИСКИ ОДГОВОР ВО ОДНОС НА ОНЛАЈН СЕКСУАЛНА ЕКСПЛОАТАЦИЈА И ЗЛОУПОТРЕБА НА ДЕЦА

Во оваа глава се обрнува внимание кон значителни зголемувања во активноста поврзана со сексуална злоупотреба и експлоатација на деца и на површинската и на темната мрежа за време на периодот на рестрикциите КОВИД-19. Целта на овој труд е анализа за тоа како пандемијата КОВИД-19 ги модифицираше трендовите и заканите за сексуална експлоатација и злоупотреба на деца, кои веќе беа на високо ниво и пред пандемијата. Оваа статија ги истакнува трендовите и заканите во тековниот контекст на КОВИД-19 во споредба со мерките пред пандемијата, какво влијание имаат тие на краток рок и со какви промени резултираа кога мерките за КОВИД-19 се намалија или целосно се укинаа. Трудот придонесува за разбирање на просторот на темната мрежа за време на пандемијата преку манифестација на тековниот организиран бизнис-модел што еволуирал како што се шири технологијата и нивото на закана што го претставува за децата. Целта е да се споделат овие трендови низ глобалната заедница за спроведување на законот и науката со цел да се подобрат мониторингот и откривањето на сексуалната експлоатација и злоупотреба на деца на интернет, понатамошни истраги и глобален полициски одговор.

Пандемијата на КОВИД-19 и мерките преземени од многу влади за ограничување на нејзиното ширење веројатно имаа влијание врз трендовите, заканите и престапите поврзани со онлајн сексуална експлоатација и злоупотреба на деца во светот.

Агенциите за спроведување на законот, владините и невладините организации (НВО) на глобално ниво изразија загриженост во врска со влијанието што може да го имаат мерките за изолација на КОВИД-19 врз злосторствата врз децата (ECPAT, 2020 година). Со затворањето на училиштата и другите услуги за поддршка, веројатното зголемување на времето на интернет и затворањето дома (UNICEF, 2020) се претполага дека децата може да бидат изложени на зголемен ризик од сексуална експлоатација и онлајн и офлајн.

Онлајн сексуалната експлоатација и злоупотреба на деца[6] се однесува на сексуална злоупотреба и експлоатација на деца преку интернет. Со оглед на тоа што сексуалната злоупотреба или експлоатација многу често се случува во физичкиот свет, последователното споделување слики и видеа што ја прикажуваат оваа злоупотреба значително го влошува влијанието на ова

[6] Терминитe сексуална злоупотреба на деца и материјал за сексуална злоупотреба на деца вклучуваат материјал за сексуална злоупотреба на деца и материјал што може да се произведе преку експлоатација на дете во замена за некаква материјална добивка. Тој се користи во овој труд во согласност со Терминолошките упатства за заштита на децата од сексуална експлоатација и сексуална злоупотреба, достапни на http://luxembourgguidelines.org/

кривично дело врз жртвите. Количината на комерцијална онлајн сексуална злоупотреба на деца беше запрепастувачка и продолжи да се зголемува за време на пандемијата со статистика што укажува дека количината на материјал брзо се зголеми во некои земји. Додека бројот на мали деца што пристапуваат на интернет значително порасна во последните години, свеста за потенцијалните ризици останува ниска, а случаите на сексуална злоупотреба и експлоатација на интернет значително се зголемија (Европол, 2020).

Следниве промени во околинските, социјалните и економските фактори се особено земени предвид во овој труд:

• затворање на училиштата и последователно движење во виртуелни средини за учење;

• зголеменото време што децата го поминуваат онлајн за забава, социјални и едукативни цели;

• ограничување на меѓународните патувања и репатријација на странски државјани;

• мерки за затворање што водат до зголемено време поминато дома;

• ограничен пристап до услугите за поддршка на заедницата, детската грижа и образовниот персонал што често игра клучна улога во откривањето и пријавувањето случаи на сексуална експлоатација на деца.

Терминологија

Сексуалната злоупотреба и експлоатација на деца преку интернет се користи во овој труд за да се разгледаат сите видови престапи. Онлајн комерцијалната сексуална експлоатација на деца може да има голем број различни форми што вклучуваат:

Онлајн подведување – Чин на развивање врска со дете за да се овозможи негова злоупотреба и експлоатација и онлајн и офлајн. Онлајн платформите, како што се социјалните медиуми, пораките и преносот во живо, може да се користат за да се олесни оваа навреда.

Пренос во живо – Услугите за пренос во живо може да ги користат сексуални престапници на деца за да ги поттикнат жртвите да извршат или гледаат сексуални дејства преку веб-камера. Престапниците, исто така, пренесуваат или гледаат во живо сексуална злоупотреба од контакт или непристојни слики на деца со други престапници. Во некои случаи, грабливците ќе им платат на олеснувачите да пренесуваат злоупотреба на контакти во живо, при што сторителот ќе насочи какви сексуални дејства се извршени против жртвата.

Онлајн принуда и уцена – Присилување или уцена на дете со технолошки средства, со користење сексуални слики и/или видеа што го прикажуваат тоа дете, за целите на сексуална добивка (на пр. да се добие нов експлицитен материјал или да се доведе до сексуална средба), финансиска добивка или друга лична корист.

Поседување, производство и споделување непристојни и забранети слики на деца – Може да користат онлајн платформи за складирање и споделување експлицитен материјал и забранети слики. Онлајн платформите, исто така, може да се користат за да се олесни производството на материјал, на пример, снимање на екранот / извршен преку пренос во живо.

Непристојни слики на деца се слики на дете или што прикажуваат дете или дел од дете за кои се оценува дека ги прекршуваат признатите стандарди за пристојност. Примери за слики што се сметаат за непристојни се оние што прикажуваат дете што учествува во сексуална активност или на сексуален начин, преку позирање, акции, облека итн. Во непристоен материјал се вклучени и фотографии, видеа, псевдофотографии и траги.

Забранети слики на деца се нефотографски слики, на пример, цртани филмови итн., кои прикажуваат дете што е вклучено во сексуална активност, сексуален чин што се изведува во присуство на дете или се фокусира на гениталниот или аналниот регион на детето (National Crime Agency, 2023).

Еволуција на криминалните трендови и закани поради КОВИД-19

Мерките за рестрикција за време на пандемијата КОВИД го зголемија времето што децата и возрасните го поминуваат онлајн за образовни, професионални, забавни и социјални цели и создаваат ненамерен ризик од сексуална експлоатација од страна на грабливци што работат на интернет (FBI, 2020). Информациите од повеќе извори, вклучително и земјите членки на ИНТЕРПОЛ, укажуваат на значително зголемување на споделувањето комерцијален материјал со сексуална злоупотреба на деца преку користење peer-to-peer мрежи за време на пандемијата КОВИД-19.

Виралната содржина не мора да има корелација со бројот на престапници активни на интернет или со бројот на самогенериран материјал што се дистрибуира. Сепак, континуираната повторна виктимизација на жртвата и зголемениот ризик невините членови на јавноста да бидат ненамерно изложени на материјал со сексуална злоупотреба на деца значат дека ефикасното управување со вирусната содржина на ваков материјал на површинската мрежа е важен фактор.

Покрај значителното зголемување на мрежната контрола, неколку земји објавија некои забележителни зголемувања и трендови во дистрибуцијата на материјал за сексуална експлоатација и злоупотреба на деца (МСЕЗД) на површинската мрежа:

• Зголемување на корисници на јасни мрежни апликации што разговараат и споделуваат материјали за злоупотреба на деца;

• Зголемување на дистрибуцијата на самогенериран материјал (Interpol, 2020).

Податоците од INSAFE, глобална мрежа на линии за помош против материјал за сексуална експлоатација и злоупотреба на деца и негативни онлајн однесувања, покажуваат дека контактите направени на линиите за помош во

првиот квартал од 2020 година забележале нагло зголемување во споредба со претходните периоди, што резултирало со најголем број контакти во еден квартал во последните четири години (Europol, 2020a). Зголемувањето на контактите може да ги одрази бројките наведени во претходните документи и анализи (Europol (2020a) и другите извештаи (ECPAT, 2020) за зголемената ранливост и изолација на многу деца во овој период.

Технолошки потпомогнатата онлајн сексуална злоупотреба на деца обично започнува со вид психолошка манипулација (воспоставување врска со малолетна жртва), потоа „секстинг“ (создавање и/или споделување сексуално сугестивни слики од жртвата), сексуална уцена „онлајн“ (уценување на детето жртва со неговите слики за да се изнуди сексуална услуга или пари) или сексуална злоупотреба во живо (принудување дете на сексуални активности) и сексуализирани материјали што прикажуваат деца (Bird at all, 2020).

Слика: Фази и елементи на комерцијална онлајн сексуална експлоатација и злоупотреба на деца (ECPAT, 2017)

Дигиталните и мрежни технологии сега може да се најдат во секоја фаза од процесот на комерцијална онлајн сексуална експлоатација и злоупотреба на деца:

1) Наводно, трговците со луѓе користат веб-форуми на dark web што се само за членови и апликации за шифрирана комуникација како што се „ShadowCrew“ и „WhatsApp“ за безбедно и анонимно комуницирање и планирање на своите криминални активности;
2) Откриено е дека децата се манипулираат преку „Instagram“, „Facebook“, „Snapchat“ и „KIK“ (BBC News, 2019);

3) Малолетниците се присилени на онлајн сексуална злоупотреба преку „Skype“, онлајн игри и виртуелни светови како „Second Life“ и „VRChat“ (Stop it Now, 2021);
4) Таквите незаконски активности потоа се пренесуваат во живо, се снимаат и складираат на апликации базирани на облак, како, на пример, Dropbox, Google Drive и OneDrive, а потоа се пренесуваат преку peer-to-peer мрежи или на форуми до кои се пристапува само со покана, и тоа и на интернет и на темната мрежа;
5) Трговците со луѓе, наводно, ги „рекламираат“ своите жртви на веб-локации како што се Backpage и Craigslist (Malik, 2018);
6) Незаконските средства и трансакции потоа анонимно се дистрибуираат и циркулираат помеѓу „купувачите“ на комерцијална онлајн сексуална злоупотреба на деца, трговците со луѓе и криминалните мрежи; и, на крај, овој технолошки подобрен циклус на криминални активности повторно почнува под (1) или во фазата на планирање на криминалното дело (Wagner at all, 2021).

7.1. Начин на дејствување „modus operandi“

Природата на прекршоците извршени за време на пандемијата КОВИД-19 во врска со онлајн комерцијална сексуална експлоатација и злоупотреба на деца не е променета во однос на познатиот начин на работа, но прекршителите ги искористуваат мерките за рестрикција со цел да продолжат со злоупотреби и да ги таргетираат децата на интернет.

Низата услови поврзани со промените во социјалната и физичката средина на жртвите и престапниците за време на КОВИД-19 резултираа со тоа што тие поминуваат зголемено време на интернет. Овие средби на потенцијални жртви и престапници на интернет се еден од клучните фактори што доведува до зголемена перцепција за заканите за децата и покрај тоа што нема забележителни промени во начинот на извршување (modus operandi).

Површинска мрежа

Огромниот волумен на онлајн материјал за сексуална злоупотреба на деца е откриен на веб-страници за хостирање слики што се достапни од површинскиот веб и на P2P мрежите (Europol, IOCTA, 2019). Престапниците продолжуваат да користат голем број начини за прикривање, што го прави покомплициран пристапот за органите на прогонот да откријат слики и видеа со злоупотреба на деца. Иако онлајн дистрибуцијата на комерцијална онлајн сексуална злоупотреба на деца продолжува да се одвива преку различни платформи, споделувањето на P2P мрежата останува меѓу најпопуларните начини за споделување меѓу сторителите. Дистрибуцијата и споделувањето еден на еден меѓу поголемите групи рутински се одвиваат на платформите за социјално вмрежување. Ова штетно споделување и повторно споделување

содржини што ги виктимизира децата е постојано забележано на рекордно ниво за време на пандемијата КОВИД-19 во Европа. Националниот центар за исчезнати и експлоатирани деца (NCMEC) изјави дека има зголемување од 106 % во таквата активност низ целиот свет (Forbes, 2020).

Таквиот материјал се создава со помош на низа средства. Еден од најштетните е сексуалната злоупотреба на деца со директен контакт од страна на престапниците. Сепак, способноста на прекршителите да измамат, присилуваат и сексуално да ги изнудуваат децата да произведуваат материјал со специфична содржина без воопшто да се сретнат со нив на интернет исто така видно се појави во неодамнешните случаи (Independent, 2020). Ефектите забележани од жртвите во вакви случаи се исто така исклучително штетни.

Темна мрежа

Посветените огласни табли на темната мрежа беа популарни меѓу прекршителите како канал за дистрибуција на комерцијален материјал за онлајн сексуална експлоатација и злоупотреба на деца во овој период. Набљудувањето на овие страници од страна на Европол потврди дека има зголемување на активноста од март до мај 2020 година на истата темна веб-страница, особено во однос на објавите за видеата снимени преку веб-камера. Овие видеа се движат од деца што се принудени или изнудени од сторителот да произведуваат материјал за злоупотреба до други видеа од сексуална природа произведени од деца за врсници или за внимание на социјалните мрежи и вклучуваат видеа што се снимени без нивно знаење. Категориите под кои се наведени материјалите за злоупотреба на деца вклучуваат „шпионски камери“, „веб-камери“ и „пренос во живо“.

Во друг мрачен веб-форум, делот специјално за оние што ја снимаат оваа снимка од пренос во живо, познат како „cappers“, забележа дека бројот на пораки и нишки се зголемил повеќе од тројно, од 500 пораки од декември 2019 до февруари 2020 година на 1 500 од март до мај 2020. Ова ја зајакнува загриженоста претходно изразена од Европол / IOCTA (2019) и други (IWF, 2018) за количината материјал што изгледа дека е самопроизведен од самите деца. Некоја од овие активности може да се однесува на годишни „натпревари“ организирани во рамките на форуми за собирање и промовирање видеоснимки со материјал за сексуална експлоатација и злоупотреба на деца.

Севкупно, вкупниот број датотеки ставени на располагање од престапниците на неколку од истакнатите темни веб-форуми значително се зголеми во периодот од март до мај 2020 година. Во еден случај, бројот на достапни датотеки се зголеми за речиси 50 %, а во друг случај, речиси се удвои.

Како одговор на операциите за спроведување на законот насочени кон овие темни веб-заедници и поради потребата да се изберат учесници и да се осигури дека размената на информации е строго поврзана со сексуална злоупотреба на деца, некои престапници создадоа нови форуми. Овие форуми делуваат како места за средби каде што учеството е структурирано слично на

криминалните организации, со правила за припадност, кодекси на однесување, поделба на задачите и строги хиерархии. Целта на структурата е да ги спроведе правилата и да промовира поединци врз основа на нивниот придонес во заедницата, што тие го прават со евидентирање и објавување на нивната злоупотреба на деца, охрабрување на другите на злоупотреба и обезбедување истомисленици, како и техничка и практична поддршка еден на друг (Europol, 2020c).

Постојаното следење на овие заедници покажа дека активностите на престапниците на сексуална злоупотреба на деца на темната мрежа биле помалку погодени од ограничувањата за време на пандемијата отколку оние на површинската мрежа. Како што претходно беше објавено од Европол, имаше многубројни дискусии за КОВИД-19 на мрачните веб-форуми посветени на сексуалната експлоатација на децата, вклучително и ентузијастички пораки за создадените можности кога децата ќе бидат онлајн повеќе од порано (Europol, 2020b).

Апликации за социјални медиуми и шифрирани пораки

Апликациите за пораки продолжуваат да се користат од прекршителите за време на пандемијата КОВИД-19 за пристап до деца и дистрибуција на комерцијален материјал за сексуална експлоатација и злоупотреба на деца. Како и кај платформите за социјални медиуми, забележано е зголемување на циркулацијата на вакви вирални видеа преку апликации за пораки (Interpol, 2020).

Комерцијален материјал за сексуална експлоатација и злоупотреба на деца сè повеќе се дистрибуира преку апликациите на социјалните медиуми. Функцијата за самоуништување на некои од овие апликации ги прави истрагите особено комплицирани. Во некои случаи, ова е резултат на самогенерираниот материјал што се споделува со врсниците, по што дополнително се дистрибуира преку социјалните медиуми и на крајот завршува на платформите за злоупотреба на деца. Има и случаи кога се креираат лажни сметки на социјалните мрежи со цел да се шират приватни слики и видеа на малолетни жртви заедно со нивните лични податоци. Иако таквите сметки често брзо се бришат, на сторителите им е лесно и едноставно да создадат нова сметка. Шифрираните пораки може да се користат и од оние што разменуваат материјали за злоупотреба на деца, дури и дозволувајќи им да формираат заедници и групи за да го сторат тоа (Europol, 2019).

Според експертите за безбедност на децата и органите за спроведување на законот, „дистрибутерите на слики од сексуална злоупотреба на деца тргуваат со линкови до материјали на површинската мрежа, односно на платформи што ги вклучуваат 'YouTube', 'Facebook', 'Twitter' и 'Instagram' користејќи кодиран јазик за да ги избегнат алатките за откривање на компаниите“ (Solon, 2021).

Платформите за игри продолжуваат да се користат за дистрибуција на комерцијален материјал за сексуална експлоатација и злоупотреба на деца и

како средство на престапниците, односно грабливците да воспостават контакт со деца.

Влијание врз полициската активност

Земјите пријавија зголемени пречки за жртвите да пријават прекршоци и да бараат медицински третман и други форми на поддршка. Ова резултираше со недоволно пријавување одредени видови прекршоци за време на пандемијата КОВИД-19. Одложување на пријавувањето траеше додека не се отворија училиштата и/или пристапот до социјалните услуги не се врати во нормала. Постои загриженост дека некои повреди можеби никогаш нема да бидат пријавени ако доцнењето во пристапот до услугите е предолго.

Земјите, исто така, пријавија тешкотии во контактирањето со жртвите преку конвенционални средства во овој период, што го отежнува продолжувањето на постојните истраги.

Персоналот за спроведување на законот што работи на онлајн сексуална експлоатација на деца беше погоден од воведувањето на политиките за работа од дома во светот. Ова, заедно со промената на приоритетите поради обврските поради КОВИД-19, имаше влијание врз користењето на базата на податоци за меѓународна сексуална експлоатација на деца на ИНТЕРПОЛ. Шеесет (60) проценти од земјите членки што редовно ја користат оваа база на податоци или не пристапиле до базата на податоци забележале значително намалување на нивните активности за време на пандемијата КОВИД-19. Државите, исто така, пријавија одредено влијание врз техничките ресурси поради политиките за работа од дома, како што е неможноста за далечинско поврзување со полициските мрежи.

Препораките вклучуваат стекнување безбедни VPN конекции за далечинско работење и користење алтернативни работни места што може да бидат слободни поради некритични операции (Interpol, 2020).

Светската здравствена организација (СЗО) ги повика технолошките компании и давателите на телекомуникациски услуги да направат сè што можат за да ги задржат децата безбедни на интернет, со оглед на зголемените ризици од онлајн повреди. „Тие мора да направат повеќе за откривање и запирање на штетната активност против децата на интернет, вклучително и заштита од подведување и создавање и дистрибуција на слики и видеа од сексуална злоупотреба на деца.“ Овие напори ќе бидат попречени бидејќи провајдерите на социјалните медиуми („Јутјуб“, „Фејсбук“ и „Твитер“) предупредија дека сè повеќе се потпираат на вештачката интелигенција и автоматизираните алатки за откривање нелегална содржина на нивните платформи поради тоа што персоналот се соочува со ограничувања додека работи од дома. Таквиот софтвер има ограничувања и можеби нема да биде толку прецизен како прегледот од луѓе.

CyberTipline е телефонска линија што прима извештаи за повеќе форми на онлајн сексуална експлоатација на деца, управувана од Американскиот

центар за исчезнати и експлоатирани деца. Во 2020 година, вкупниот број примени извештаи од CyberTipline се зголеми за 28 % од 2019 година, со 21,7 милиони извештаи (NCMEC CyberTipline, 2021). Сепак, само во март 2020 година, Центарот забележа зголемување од 106 % во CyberTipline извештаите за сомнителна сексуална експлоатација на деца – што се зголеми од 983 734 пријави во март 2019 година, а подоцна и над 2 милиони (Solon, 2021). Бројот на извештаи беше уште поголем во април 2020 година (4,2 милиони извештаи според соопштенијата за печатот) (Alfonso, 2021). Поголемиот дел од извештаите примени во 2020 година генерално (99,6 %) се поврзани со сомнителни CSAM и вклучија 65,4 милиони слики, видеа и други датотеки, вклучително и 33,6 милиони слики, од кои 10,4 милиони беа единствени, и 31,6 милиони видеа, од кои 3,7 милиони беа единствени (NCMEC CyberTipline, 2021).

Влијанието на КОВИД-19 врз полициското работење варира во зависност од земја, но некои клучни проблеми што се идентификувани вклучуваат:

- Намалување или доцнење во пријавувањето прекршоци во доменот на комерцијална онлајн сексуална злоупотреба на деца бидејќи се засегнати нормалните канали за известување;
- Намалување на користењето на базата на податоци на Интерпол од страна на земјите членки;
- намалување на достапноста на специјализирани човечки ресурси за Спроведување на законот што ги поддржуваат истрагите на комерцијална онлајн сексуална злоупотреба на деца;
- Промени во процесите и ефикасноста поради техничките ограничувања на работењето од дома што влијаеше и на органите за спроведување на законот и на давателите на електронски услуги што известуваат до органите за спроведување на законот;
- Одложувања или затворања на судовите што доведе до одложување на процесирањето на предметите;
- Зголемување на онлајн активноста на комерцијална сексуална злоупотреба на деца и на темната и на површинската мрежа;
- Значајно зголемување на споделувањето материјал за комерцијална онлајн сексуална злоупотреба на деца преку користење peer-to-peer мрежи;
- Значително зголемување на виралните содржини споделени и преку платформите за социјални медиуми и преку апликациите за пораки што резултира со повторна виктимизација на жртвите и изложување на невини случајни „минувачи“;
- Зголемување на самогенерираниот материјал дистрибуиран на чистата мрежа;
- Нема значителни промени во обемот на прекршоци со користење платформи за онлајн игри, но одредени игри се идентификувани како потенцијални ризични;
- Рани индикации дека комерцијална онлајн сексуална злоупотреба на деца за плаќање може да биде тренд што се појавува во одредени земји.

Примери на најнови операции во спречување на оваа нова глобална безбедносна закана:

- ✓ **Kidflix (април 2025)** – голема меѓународна операција предводена од германската BKA и Europol што затвори една од најголемите платформи за детска експлоатација; апсења, заплени и заштита на десетици жртви. Ова е пример на комерцијална платформа што функционирала со модел на монетизација и глобална релевантност (www.europol.europa.eu)
- ✓ **Меѓународни акции (2024 – 2025)** – низа операции што резултирале со апсења и заплени поради организирана дистрибуција/производство на CSAM (на пример, операции предводени од шпанската полиција со поддршка на INTERPOL/Europol) (www.interpol.int)
- ✓ **Глобални извештаи (IOCTA 2024, WeProtect, NCMEC)** – официјални извештаи што укажуваат на раст (и нови форми – sextortion, AI-CSAM) и на потреба за технички и правни мерки

Ризици и современи трендови

- ➢ **Експлозија на обемот на материјали и инциденти –** стапките на пријави и материјали се многу високи (милиони пријави годишно во NCMEC/CyberTipline). Ова создава „бригада“ на огромен обем на податоци што тешко се обработуваат и истражуваат (www.missingkids.org)
- ➢ **AI/Generative-AI –** брзо расте бројот на пријави за AI-генериран CSAM и deepfake содржини, што комплицира идентификација и жртвување (unicri.org, 2024)
- ➢ **Интернационалност –** инфраструктурата (хостинг, оператори, корисници) често е распрскана низ повеќе земји – потребна е меѓународна координација. Големи операции (пример: операции против Kidflix) покажуваат како соработка меѓу 35+ земји може да урне глобални мрежи (www.europol.europa.eu)
- ➢ **Техничката еволуција на криминалците –** користење енкрипција, приватни мрежи, миксер-услуги за крипто, и „bot“/алгоритми за ширење и монетизација (Internet Organized Crime Assessment, 2024).

Заклучок

Иако сè уште е рано да се процени влијанието на КОВИД-19 врз сексуалната експлоатација и злоупотреба на деца на интернет, тоа несомнено ја зголеми ранливоста на децата на сексуална експлоатација овозможена од технологија. Затворањето на училиштата ги принуди децата да влезат во дигиталната сфера неподготвени, без соодветно знаење за тоа како функционира дигиталната сфера или какви ризици со себе носи. Групите за онлајн игри и разговор станаа клучни места за средби и интеракции меѓу децата, со што се зголемува ризикот од комерцијална сексуална експлоатација на децата. Навистина, од почетокот на 2020 година има брз пораст на дигитализацијата на општеството на сите нивоа.

Онлајн игрите, групите за разговор, обидите за фишинг преку е-пошта, контактите преку социјалните мрежи и едукативните апликации станаа главни места за средби меѓу децата и сексуалните престапници. Ненадгледуваното време на интернет, исто така, го зголеми ризикот дека малолетните поединци можат да произведуваат и дистрибуираат непристоен материјал создаден самостојно.

Бидејќи технолошкиот напредок континуирано ја трансформира глобалната економија, ова доведе до појава и проширување на неколку видови киберкривични дела, вклучително и онлајн сексуална експлоатација и злоупотреба на деца, кое е едно од злосторствата што најбрзо се приспособуваат и ги користат можностите што ги нуди технологијата.

Европол (2020б) и Интерпол (2020) известуваат дека ограничувањата наметнати од владите влијаеле на трендовите и заканите за прекршоци поврзани со комерцијална сексуална експлоатација во светот. Тие забележаа нагол пораст на побарувачката за трговија со деца за онлајн сексуална експлоатација и дистрибуција на онлајн материјал за сексуална експлоатација на деца во многу делови на Европа, бидејќи повеќе грабливци и потенцијални сторители беа „затворени“ дома во време на пандемијата.

Всушност, безбедносните проценки од Европол и Интерпол предвидуваат дека во следните години ќе има нагло зголемување на количината самопроизведен непристоен материјал, што би можело да доведе до правопропорционално зголемување на онлајн подведување и експлоатација на деца.

ГЛАВА VIII

ЗАКЛУЧОК: ГРАДЕЊЕ ОТПОРНОСТ КОН НОВИТЕ ГЛОБАЛНИ БЕЗБЕДНОСНИ ЗАКАНИ ВО СОВРЕМЕНИОТ БЕЗБЕДНОСЕН КОНТЕКСТ

Во современиот безбедносен контекст, обележан со постојана трансформација на заканите и зголемена меѓусебна поврзаност на државите, градењето отпорност претставува суштинска компонента на националната и глобалната безбедност.

Отпорноста не се сведува само на способноста за реакција по настанување на заканата, туку подразбира превентивна подготвеност, флексибилност и капацитет за обновување на општествените, институционалните и технолошките системи. Тоа подразбира воспоставување силни институции, подобрена меѓусекторска координација, развивање култура на безбедност и подигнување на јавната свест за ризиците.

Во последниве години, отпорноста се појави како централен концепт во националните и меѓународните безбедносни дискурси, кој е истакнат во стратегиските рамки и политичките документи низ различни сектори.

Оваа Глава ќе анализира како отпорноста игра значајна дискурзивна улога во областа на националната и меѓународната безбедност. Анализата силно сугерира дека отпорноста стана нов звучен збор на националната безбедност. „Отпорноста“ е неопходна способност на критичниот ентитет да спречи, заштити, реагира, да се спротивстави, ублажи, апсорбира, приспособува и закрепнува од инцидент. Ова е потврдено со позиционирањето на отпорноста како основен концепт во многу клучни стратегиски документи. Во согласност со неговата широка применливост, терминот доминираше во безбедносниот дискурс на стратегиско ниво.

Концептот на издржливост се користи во многу различни контексти во современиот свет, вклучувајќи ги бизнисот, политиката, безбедноста, па дури и кај природните и општествените науки.

Неизвесноста и непредвидливоста на безбедносната средина се уште една причина да се прифати концептот на отпорност. Со оглед на широкиот спектар на закани и безбедносни предизвици, ширењето на конвенционалните и неконвенционалните конфликти, нејасните граници помеѓу воените, асиметричните и хибридните закани и предизвиците што ги донесе пандемијата на КОВИД-19, НАТО и ЕУ се свртеа кон потребата да се зајакне отпорноста на секоја земја членка.

Во современото безбедносно опкружување, границите помеѓу конвенционалните и неконвенционалните конфликти се нејасни, а примената на невоените инструменти на моќ од страна на различни државни и недржавни актери стана норма. Неочекуваните закани како тероризам, кибернапади и

други алатки за војување, покрај природните катастрофи како поплави, пожари и пандемии, вршат невиден притисок врз секоја земја и организација во светот.

Бидејќи сите нарушувања и напади не може да се предвидат и/или да се припишат на одредени актери, примената на традиционалните механизми за одвраќање и одбрана станува сè потешка. Во многу случаи, ова често се должи на отсуството на долгорочна ориентација во предвидувањето на заканите и недостатокот на ресурси што ги попречуваат подготовките за сите хипотетички закани и ризици. Затоа, за ефикасно да се подготват и да закрепнат од различни предизвици и закани, сè поголем број актери бараат одбранбени и безбедносни решенија преку концептот на отпорност.

Еволуција на концептот

Употребата на терминот „отпорност“ има долга традиција во различни науки и научни дисциплини – психологија, социологија, екологија, инженерство, менаџмент, додека во безбедносните студии е присутна само од почетокот на 21 век. Во последните неколку децении, употребата на овој термин во академскиот дискурс расте со „вртоглава“ брзина, а неговите концептуализација и операционализација (дури и меѓусебно спротивставени, речиси контрадикторни) се сè побројни и разновидни, како во академската литература така и во стратегиските и правните документи (Stanković, 2021).

Концептот на отпорност може генерално да се окарактеризира како „капацитет на системот постојано да се развива и да се приспособува на вознемиреност додека ги одржува својата основна функција и структура“ (Walker, 2006). Со оглед на оваа општа дефиниција, интуитивно може да се насети широкиот спектар на можни примени и цели на терминот во безбедносната политика и практика. Концептот првпат се појавил во неговата англиска верзија во речниците од 17 век за подоцна да биде прифатен од механичарите од 19 век и екологијата и психологијата од 20 век (Alexander, 2013).

Во широката дисциплина на безбедносните студии, разбирањето на отпорноста фундаментално се разликува во однос на неговото значење и цел. Во текот на 2000-тите, прилично позитивистичкиот пристап кон отпорноста доби основа во областа на стратегиските студии (Fjäder, 2014) и управувањето со итни случаи (Rogers, 2017). Оваа перспектива ја гледа отпорноста како алатка за решавање проблеми што ја отвора безбедноста за низа нови актери и со тоа ја остава државата зад себе до одреден степен. Сфатена како аналитичка и практична алатка, отпорноста помага да се разбере сложеноста што ја дефинира тековната безбедносна средина и ги „демократизира“ одговорите со ангажирање – и овластување – други актери. Околу 2010 година, се појави алтернативен тек на литература за издржливост за да ги предизвика пристапите за решавање проблеми. Владините дискурси за издржливост беа испитани во однос на практиките што тие имаат тенденција да ги легитимираат. Односно, се поставуваа политички прашања за тоа што прави отпорноста и кому. Овој

пристап ја перципира отпорноста како главно неолиберална алатка, со држава – иако низ призма на логиката на зајакнување што придонесува за постојните и нееднакви структури на моќ (Chandler, 2014). Научниците тврдат дека нечија способност да биде отпорен зависи од нивната социјална и просторна положба – односно, отпорноста не функционира на рамноправно поле за играње. Затоа се смета за фундаментално политичко – и се поставуваат прашања за тоа кој треба да се направи отпорен, со какви средства и со какви последици (Vale, 2014).

Во екстремни случаи, безбедносните мерки означени со отпорност може да се сметаат како поткопување на безбедноста наместо како нејзино подобрување (Coaffee, Fussey, 2015). Голем дел од критичните безбедносни гледишта се фокусираа на „урбаната отпорност" – растечка истражувачка агенда особено по 11 септември, при што многу градови бараа антитеристички мерки што се движат од одбранбено урбанистичко планирање (Coaffee, 2009) до милитаризација на урбаниот јавен простор и надзор.

Одразувајќи го нејзиниот подем во академската средина, „отпорноста" исто така стана широко прифатена во националната безбедносна политика, особено по 2010 година. Додека земјите во светот ја инкорпорираа издржливоста во своите национални безбедносни стратегии, други – како што се Канада, Холандија или Австралија, дури усвоија специфични „стратегии за издржливост" (Fjäder, 2014). Наместо да ветува „тотална безбедност", која е недостижна во денешното сложено безбедносно опкружување, отпорноста ја прифаќа можноста за појава на прекини и кризи. Веќе не се работи за тоа дали тие ќе се случат – повеќе е за тоа како да се издржи кога ќе се случат. Како што станува очигледно кога се анализираат безбедносните стратегии и декларации, опсегот на можни безбедносни закани што може да се материјализираат е практично неограничен. Според тоа, се разликуваат два типа на отпорност – специфицирана во однос на познатите ризици и очекуваните безбедносни настани, и општо за справување со непознатото (Scholz at all, 2012).

Во аренатa за национална безбедност, Fjäder (2014) тврди дека издржливоста ја предизвикува традиционалната улога на државата како обезбедувач на безбедност. Широк опсег на други актери на различни нивоа влегува во игра, одразувајќи ја разновидноста на домени опфатени со отпорноста. Како што ќе биде прикажано во следните делови, отпорноста вклучува прашања од јавното здравје и социјалната кохезија до индустриските катастрофи и тероризмот. Во однос на неговиот опсег и цели, тој далеку ги надминува владините или воените власти. Отпорноста, исто така, има за цел да ја надмине материјалната димензија на безбедноста преку истакнување на меѓусебната поврзаност на природните, еколошките, демографските и социјалните домени (Pickett at all, 2014). Замаглувањето на овие различни димензии и на поранешната јасна разлика помеѓу внатрешната и надворешната безбедност станува јасно во анализата на дискурсот за издржливост на државите и меѓународните организации.

Проучените стратегии и декларации на високо ниво имаат тенденција да ја користат терминологијата на заканите, ризиците и ранливостите, од една

страна, а, од друга страна, нудат принципи на издржливост. Заштита, адаптација, соработка, зајакнување и градење капацитет се меѓу поимите што често се користат во однос на референтните објекти на безбедност – било тоа да се држави, општества, критични инфраструктурни мрежи или ранливи заедници. Отпорноста претставува сеопфатен принцип, кој служи за разбирање и анализа на заканите и одговорите на кое било ниво и скала што е пожелно. Исто така, отпорноста во смисла на истрајност, обновување и континуитет има важен нормативен аспект за неа, што е тешко да се контрааргументира. Накратко, извонредната аналитичка корист и флексибилноста на концептот го претворија во еден од главните зборови во денешниот безбедносен дискурс (Svitkova, 2017).

Дефинирање на отпорноста

Бидејќи концептот на издржливост е прилично нов за безбедносната политика, терминот често се меша со сродни концепти како отпор и подготвеност, а понекогаш се меша со некои поширoки пристапи на националните држави, како што се цела влада, цело општество или целосна одбрана. Постојат многу, честопати конфликтни, термини што ја опишуваат издржливоста од различни перспективи.

Отпорноста се дефинира како: „Способност на системот, заедницата или општеството изложено на опасности да се спротивстави, апсорбира, да се приспособи и да закрепне од ефектите на опасноста на навремен и ефикасен начин, вклучително и преку зачувување и обновување на неговите суштински основни структури и функции“ (UNISDR, 2009).

Меѓу комплексните и повеќеслојни дефиниции развиени од страна на државите и меѓународните организации, има неколку конкретно поврзани со националната безбедност. На пример, британската доктрина дава детална дефиниција за отпорноста: „способноста на заедницата, услугите, областите или инфраструктурата да се дефектираат, спречат и, доколку е потребно, да се спротивстават, да се справат и да закрепнат од нарушувачки предизвици“ (Cabinet Office, Civil Protection Lexicon Version 2013). Дефиницијата на САД е сосема слична: „способност да се приспособат на променливите услови и да издржат и брзо да закрепнат од прекини поради итни случаи“ (The White House, 2011).

НАТО ја дефинира отпорноста како способност на општеството да се спротивстави и да закрепне лесно и брзо од такви шокови како природна катастрофа, неуспех на критичната инфраструктура или хибриден или вооружен напад. Таквата способност ги комбинира и цивилната подготвеност и воениот капацитет. Цврстата отпорност преку цивилната подготвеност во сојузничките земји се смета за „суштинска за колективната безбедност на НАТО“ со голем придонес за „кредибилитетот на одвраќањето и одбраната на НАТО“. Пристапот на НАТО е вткаен во член 3 од неговиот основачки договор: со поединечно обврзување на одржување и зајакнување на отпорноста, сојузниците ја намалуваат „ранливоста на НАТО како целина“; оттука и отпорноста е

национална одговорност. Договорени се седум основни барања за таква национална отпорност – тие се однесуваат на основните функции на „континуитет на владата, основните услуги за населението и цивилната поддршка на војската“ (воените напори за одбрана на територијата на Алијансата и населението на кои им е потребна силна цивилна подготвеност за намалување на потенцијалните ранливости – воените сили повторно зависат од цивилните и комерцијалните комуникациски сектори, како што се основните комуникациски сектори за храна, вода и транспорт).

Отпорноста е, исто така, централниот столб на стратегијата на Европската Унија за справување со повеќедимензионални хибридни закани што комбинираат принудни и субверзивни мерки, вклучувајќи ги опасностите од пролиферација на оружјето за масовно уништување и дезинформациите. (European Council, 2018). Повторно, земјите членки се главно одговорни за зајакнување на отпорноста и зајакнување на капацитетите за одговор, додека институциите на ЕУ ги зајакнуваат националните напори.

Понатаму, Стратегијата за безбедност на ЕУ за 2020 година (European Commission, 2020) и агендата за борба против тероризмот ја нагласуваат важноста на издржливоста и, особено, отпорноста на критичните инфраструктури. Оттука, земајќи ги предвид новите политики и лекциите од имплементацијата на Европската директива за критична инфраструктура од 2008 година, Европската комисија предложи нејзина замена со нова директива насочена кон зајакнување на отпорноста на критичните субјекти што обезбедуваат основни услуги во ЕУ (European Commission, 2020).

И НАТО и ЕУ имаат тенденција да се придржуваат до своите традиционални мисии, принципи и вредности во анализираниот дискурс. Тоа е она што создава одреден контраст во нивното разбирање на отпорноста. НАТО дискурзивно примени отпорност на традиционалните принципи на одбранбена соработка и одвраќање, од една страна, и на „новите“ предизвици од инфраструктурна, еколошка или демографска природа, од друга страна. ЕУ, од своја страна, ја искористи отпорноста во контекст на градење држава, добро владеење, човекови права и одржлив развој. Со други зборови, мисијата и природата на овие две организации ги информираат начините на кои се користи отпорноста во двата случаи.

Во секој случај, се чини дека еластичноста е новата аналитичка рамка што ја користат и НАТО и ЕУ со цел да се разбере сложената безбедносна средина. Во контекст на широко разбирање на безбедноста, приспособливоста на концептот изгледа особено корисно.

Од многубројните дефиниции на поимот „отпорност“ во литературата, сè уште е можно да се истакнат три преовладувачки карактеристики што се појавуваат во повеќето од нив.

1. Отпорноста се перципира како способност (или капацитет или способност – но не како реакција, одговор, особина или процес) на личност, група, заедница или општество (Ajdukovic at all, 2015).

2. Отпорноста вклучува динамична промена или трансформација на однесувањето (Berkes, Ross, 2014).
3. Отпорноста се карактеризира со динамичен адаптивен капацитет на системот да се приспособи на ситуацијата што се развива.

Предуслов за постоење на еластично однесување е појавата на нарушување. Ова е затоа што потребата за отпорност се појавува само во состојба каде што рамнотежата на системот е прекината. Нарушувањето може да биде предизвикано од човечки фактор, на пр., војна, терор, насилство или може да биде предизвикано од природата, на пример, земјотрес, цунами, поплави итн., доколку предизвикува значително нарушување во рутинскиот живот на луѓето (Padan, Gal, 2020).

Рамка за разбирање на нивоата и елементите на отпорност

„Моделот на принципи на еластичност“, понуден од Карл Гибсон и Мајкл Тарант (2010) во делото „Концептуални модели“, може да послужи како погодна и во исто време најсеопфатна почетна точка за разбирање на различните концептуални модели на организациска отпорност. Овој „модел“ на издржливост е создаден со идентификување на најчестите теми или концепти што се појавуваат во дефинициите за отпорност на различни науки и научни дисциплини и се заснова на шест клучни принципи:

1. „Отпорноста е исход“;
2. „Отпорноста не е статична особина“;
3. „Отпорноста не е единствена сопственост“;
4. „Отпорноста е повеќедимензионална“;
5. „Отпорноста постои преку повеќе форми“;
6. „Отпорноста се заснова на валидно управување со ризикот“ (Gibson & Tarrant, 2010).

Признавајќи го фактот дека отпорноста се одредува со интеракции со променлив контекст, организацискиот контекст може истовремено да има и стимулирачки и деградирачки ефект врз способностите за отпорност, што на крајот резултира со отпорност. Како една организација ќе се справи со таквата варијабилност зависи од тоа како таа ги следи, разбира и се справува со ризиците со кои се соочува (Gibson & Tarrant, 2010).

Отсуството на јасни дефиниции и универзални карактеристики ја прави отпорноста високоиндивидуализиран концепт што треба да биде приспособен за секој актер. Без оглед на точната дефиниција што се користи, за потребите на анализата, често е порелевантно да се фокусираме на варијаблите што ја сочинуваат отпорноста. Само анализата на тие опипливи променливи може да доведе до разбирање на различни фази од процесот што ја сочинува отпорноста. За таа цел, императив е да се дефинираат променливи и елементи што влијаат на различните физички и психолошки компоненти на отпорноста на сите мерливи нивоа: индивидуално, заедница, организациско, национално и мултинационално.

Главниот дел од академската литература ја опишува ефективната примена на отпорноста како почива на разбирање и управување со меѓузависноста помеѓу инструментите на моќта и нивните ефекти врз двете компоненти на еластичноста на сите нивоа.

Елементи на издржливост: Управувањето со современите мултидомени и сеопфатни закани бара усогласена употреба на сите достапни инструменти на националната моќ, вклучувајќи дипломатски, воени, информативни, економски, финансиски, разузнавачки, спроведување на законот итн. Моментално достапните и новите концепти бараат координација и соработка на оние што се вклучени на национално и меѓународно ниво.

Физичките елементи на потпирање се материјални и инструментални променливи како што се инструментите на моќ, критичната инфраструктура, ресурсите, мрежите, структурите, па дури и како е организирана група или институција во однос на односите, механизмите и системите за одлучување. На пример, НАТО смета дека тие физички аспекти на отпорноста се неопходни за да се обезбеди континуитет на владините и критичните владини служби. Ова може да ја вклучи способноста да се донесуваат одлуки, да се соопштуваат и да се спроведуваат во услови на криза (NATO, 2025).

Мултидимензионална матрица

Сеопфатната дефиниција спомената погоре може да послужи како јадро за неколку специфични дефиниции, кои претставуваат дванаесет различни типови на еластичност што се создаваат со пресекот на две релевантни димензии: содржина и ниво.

Димензијата на содржината во претстојната матрица се состои од четири домени:

1. социјален,
2. економски,
3. политички, и
4. безбедносен/воен.

Иако, очигледно, ова не се единствените домени во кои може да се проучува отпорното однесување (животната средина, климата и културата се примери на дополнителни домени каде што отпорноста игра главна улога), овие четири обезбедуваат подобра перспектива за испитување на различни нивоа, како што ќе се покаже наскоро. Главната причина за постоењето на димензијата на содржината е тврдењето дека капацитетите за издржливост потребни во овие четири домени не се нужно идентични. Од онтолошка перспектива, секој домен претставува посебна категорија (Fjäder, 2014).

Димензијата на ниво вклучува три нивоа на референца: поединец, заедница и држава. Неодамнешната пандемија КОВИД-19, која сериозно ги погоди сите земји на сите континенти, очигледно се залага за четврто ниво – глобално. Исто така, можно е да се додадат различни средни нивоа и на оваа димензија, како што се семејно, регионално (или етничко) или организациско

ниво. Меѓутоа, во тековниот труд ќе се фокусираме на овие три фундаментални нивоа.

Матрицата генерирана од комбинирање на содржината и димензиите на ниво произведува дванаесет ќелии, од кои секоја претставува поттип на отпорност (види Табела).

	Категории на содржина				
Ниво Категории	**Индивидуално**				**Безбедност**
					– Претходно искуство во слични ситуации; – Релевантни информации; – Факултативно учество во активности поврзани со закана; – Поддршка на членовите на семејството и заедницата.
	Заедница/ Општество				– Подготвеност за итни случаи; – Акумулирано искуство; – Ниво на доверба во безбедносните авторитети; – Пропорција на воени лица во заедницата; – Доверба во локалното раководство; – Постоење на базични услуги.
	Државно				– Харизматично лидерство; – Национален етос; – Колективен страв и борбен ентузијазам; – Доверба во институциите поврзани со безбедноста; – Патриотизам, оптимизам и општествен интегритет; – Воена сила; – Ниво на државно одвраќање; – Национална безбедносна перцепција.

Табела: Повеќедимензионална матрица за претставување на типови на отпорност

Табелата ги сумира најцитираните компоненти за градење отпорност во категоријата безбедност генерирани од нашата повеќедимензионална матрица.

Индивидуална отпорност при безбедносна (воена) вонредна состојба

Овде означуваме атрибути на издржливост што ги карактеризираат индивидуите, главно цивили, кои се наоѓаат во воени ситуации или под продолжена воена закана, повторени терористички акти или долготрајна безбедносна опасност. Таква беше ситуацијата со илјадници поединци во Њујорк по нападите од 11 септември, за време на периодот на терористички напади во Северна Ирска, како и во многу земји во Африка, Централна Америка и Југоисточна Азија во последните децении. Дефиницијата за отпорност во оваа конкретна „ќелија“ е како што следува:

капацитетот на поединецот да се однесува за време на безбедносна криза (на пример, војна, немири, терористички напади, контрабунтовници) или по нарушување од оваа природа, на адаптивен начин, со цел да се врати на претходното или дури и подобреното ниво на функционирање.

Најцитираните фактори во врска со овој тип на отпорност се претходното искуство во слични ситуации; количината релевантен и добро управуван проток на информации во врска со заканите; засилено ангажирање во активности поврзани со закана (Gal, Lazarus, 1975). За поединечни жртви на масовни терористички напади, поддршката од семејството и членовите на заедницата може да биде клучна (Desivilya at all, 1996).

Општествена отпорност под безбедносна (воена) вонредна состојба

Оваа категорија не мора да се однесува на ситуација со тотална војна (во кој случај заедницата е само компонента во напорите на целата држава). Наместо тоа, овде се фокусираме на ситуации кога една заедница, или неколку, е под безбедносна опасност или воена закана. Опасноста може да биде терористички напад или смртоносен воен напад експлицитно насочен против оваа заедница.

Дефиницијата за отпорност во оваа конкретна „ќелија“ е како што следува:

капацитетот на заедницата да се однесува, за време на безбедносна криза или по нарушување поврзано со безбедноста, на адаптивен начин, со цел да се врати на претходното, па дури и на подобрено ниво на функционирање на заедницата.

Во последниве години, концептите на „урбана отпорност“ и „дизајн на отпорност“ се развиени во различни градови низ светот, како што се Лондон и Њујорк. Овие концепти се однесуваат на користење на идејата за отпорност не само за да се помогне за закрепнување од напади туку и за инкорпорирање принципи на дизајнирање антитероризам за одвраќање, откривање и одложување на потенцијалните напади. (Sampaio, 2017).

На мнозинството јавни простори им недостасуваат безбедносни мерки специфични за заканата што се избрани и имплементирани преку систематска процена на процесот на ризик. Безбедносните мерки, доколку постојат, треба да

се идентификуваат, оценат и подобрат ако се сметаат дека се недоволни и застарени. Таквата постапка треба да вклучи и оцена за успешноста на тековните мерки и идентификација на области што остануваат изложени на одредени закани. Како што е забележано претходно, безбедносната закана еволуира со текот на годините, така што се применуваат мерки што можеби не се соодветни за зголемените потреби диктирани од современите безбедносни закани. Постојните безбедносни мерки, доколку се применуваат правилно, може значително да го намалат буџетот потребен за спроведување на новите безбедносни планови (European Commission, Joint Research Centre (JRC), 2022).

Државна отпорност под безбедносна (воена) вонредна состојба

Оваа категорија се однесува на ситуација кога отпорноста на државата на крајот е предизвикана од тотална војна или екстремен пораст на тероризмот. Нашата дефиниција за отпорност на државата при вонредни состојби поврзани со војна е:

капацитетот на државата да се однесува за време на национална безбедносна криза или по нарушување поврзано со безбедноста на адаптивен начин, со цел да се врати на претходното, па дури и на подобрено ниво на функционирање.

Најцитираните фактори во врска со овој тип на издржливост се харизматичното лидерство; националниот етос, колективниот страв и борбениот ентузијазам; довербата во институциите поврзани со безбедноста (на пример, војска, полиција); патриотизмот; оптимизмот; и социјалниот интегритет. Кога се фокусираме на воените показатели на отпорност, списокот се состои од воена сила (материјална, морална и доктринална) и воено лидерство, согледано ниво на одвраќање, стратегија за национална безбедност и перцепција (Prior, 2018).

Очекуваниот исход и цел е да се спречат нови и да се намалат постојните ризици од катастрофи преку имплементација на интегрирани и инклузивни економски, структурни, правни, социјални, здравствени, културни, образовни, еколошки, технолошки, политички и институционални мерки што ги спречуваат и намалуваат изложеноста на опасност и ранливоста од катастрофи, ја зголемуваат подготвеноста за одговор и закрепнување, а со тоа ја зајакнуваат отпорноста (Sendai Framework for Disaster Risk Reduction 2015 – 2030).

Заклучок

Отпорноста брзо еволуираше од периферен поим во централен столб на модерното безбедносно размислување. Растечката важност во рамките на националните и меѓународните политики ја нагласува промената на парадигмата во тоа како државите и институциите ги разбираат и реагираат на безбедносните закани во сè покомплексниот и меѓусебно поврзан свет.

Оваа последна глава обезбедува концептуална рамка за дефинирање на отпорноста, и општо и особено, во однос на одреден домен, рамка која може да

обезбеди сет за можни мерења и процени на отпорноста на различни нивоа и домени. Концептуалната матрица понудена во оваа глава ќе им овозможи на државите подобро да учат и да ги мапираат своите силни и слаби страни, со што ќе им помогне да ги водат ставовите и однесувањата на нивниот систем (вклучувајќи ги индивидуите, заедниците итн.).

Сепак, широката перспектива на отпорноста, исто така, претставува нови предизвици. Нејзината концептуална еластичност, иако овозможува разновидни примени, ризикува да го намали нејзиното практично значење. Исто така, постои загриженост дека дискурсите за отпорност може да го префрлат товарот на безбедноста од државите на поединците и заедниците, поставувајќи прашања за одговорноста, правичноста и управувањето.

Градењето отпорност не е крајна цел, туку динамичен процес на учење, приспособување и иновација**,** кој го одржува општеството способно да се справи со непредвидливоста на новите безбедносни реалности.

Користена литература

1. Acharya, A. (2009). *Targeting Terrorist Financing: International Cooperation and New Regimes*, New York: Routledge.
2. Ajdukovic, D at all. (2015). *Resiliency: Enhancing Coping with Crisis and Terrorism*, NATO Science for Peace and Security series, Vol. 119, Amsterdam: IOS Press.
3. Albert Réka, Albert-Lásló Barabási. (2002). Statistical Mechanics of Complex Networks, *Reviews of Modern Physics*, Vol. 74.
4. Albert-Lásló Barabási. (2003). Linked: How Everything is Connected to Everything Else and What it Means for Business, *Science, and Everyday Life*. New York: Plume.
5. Alexander, D. (2013). Resilience and Disaster Risk Reduction: an etymological journey. *Natural Hazards and Earth Systems Sciences*. Vol. 13, pp. 2707-2716.
6. Alfonso III F. (2021). The pandemic is causing an exponential rise in the online exploitation of children, experts say. Достапно на: https://edition.cnn.com/2020/05/25/us/child-abuse-online-coronavirus-pandemic-parents-investigations-trnd
7. Aliens, C (2016). "Darknet Bust: Global Law Enforcement Raids Massive Counterfeiting Organization," *Deep.Dot.Web*, December 17.
8. All Things Generative AI," generativeai.net, n.d.
9. Allan, H at all. (2015). *Drivers of Violent Extremism: Hypotheses and Literature Review*. London: Royal United Services Institute.
10. Alvarez, L, Perez-Pena, R. (2016). "Praising ISIS, Gunman Attacks Gay Nightclub, Leaving 50 Dead in Worst Shooting on U.S. Soil," *New York Times*, June 13. Достапно на: https://www.nytimes.com/2016/06/13/us/orlando-nightclub-shooting.html
11. A/70/174 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015). Достапно на: https://docs.un.org/en/a/70/174
12. Aroua, A. (2018). *Addressing Extremism and Violence. The Importance of Terminology*. Geneva: The Cordoba Foundation of Geneva. Достапно на: https://www.cordoue.ch/images/pdf/Papers/CFG_ConflictTransformationPerspective.pdf
13. Atran, S. (2006). The Moral Logic and Growth of Suicide Terrorism, *The Washington Quarterly*, 29(2).
14. Augustus Norton. (1998). Terrorism in the Middle East, in Vittorfranco Pisano (ed), *Terrorist dynamics: a geographical perspective*, Arlington: International Association of Chiefs of Police, 1-44.
15. Bandura, A. (1990). "Mechanisms of Moral Disengagement in Terrorism," in Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*. Cambridge: Cambridge University Press.

16. Basra R., Neumann P.R. (2017). Development in the crime-terror nexus in Europe, *CTC Sentinel*, Vol.10, Issue 9, Combating Terrorism Centre at West Point, USA.
17. BBC News. (2019). Instagram biggest for child grooming online – NSPCC finds, 1 March. Достапно на: https://www.bbc.com/news/uk-47410520
18. Berkes, F., Ross, H. (2013). "Community Resilience: Toward an Integrated Approach," *Society & Natural Resources* 26, no. 1, 5-20. Достапно на: https://www.researchgate.net/publication/263529519_Community_Resilience_Toward_an_Integrated_Approach
19. Berntzen, L.E, Sandberg, S. (2014). The Collective Nature of Lone Wolf Terrorism: Anders Behring Breivik and the Anti-Islamic Social Movement. *Terrorism and Political Violence*. Vol 26 (5).
20. Borchgrevink, A. (2012). *A Norwegian Tragedy: Anders Behring Breivik and the Massacre on Utoya*. Cambridge: Polity Press
21. Borum, R., Bartel, P., & Forth, A. (2006). SAVRY: *Professional Manual for Structured Assessment of Violence Risk in Youth*. Lutz, FL: Psychological Assessment Resources Inc.
22. Brian Reed. (2007). A Social Network Approach to Understanding an Insurgency, *Parameters: U.S. Army War College Quarterly*, Vol. 37, No.
23. Brus Hoffman. (2003). *Al Qaeda, trends in terrorism and future potentialities: an assessment*, Rand Corporation. Достапно на: https://www.ojp.gov/ncjrs/virtual-library/abstracts/al-qaeda-trends-terrorism-and-future-potentialities-assessment
24. Burke, J. (2017). The myth of the 'lone wolf' terrorist. *The Guardian*. Достапно на: https://www.theguardian.com/news/2017/mar/30/myth-lone-wolf-terrorist
25. Burton, F, Stewart, S. (2008). "The 'Lone Wolf' Disconnect," STRATFOR Global Intelligence. Достапно на: https://worldview.stratfor.com/article/lone-wolf-disconnect
26. Cabinet Office. (2013). Civil Protection Lexicon Version.
27. Cambridge Dictionary, "Cryptocurrency," *Cambridge Dictionary*.
28. Carlo Morselli, Christian Giguere, K Petit. (2007). The efficiency/security trade-off incriminal networks, *Social Networks*, 29, 143–153.
29. Casadei B. (2019). Terrorist Use of Cryptocurrencies-A Blockchain Compliance White Paper, Blockchain Consultus, London, United Kingdom.
30. Cauffman, E. E., & Steinberg, L. (2000). (Im) maturity of judgment in adolescence: Why adolescents may be less culpable than adults. *Behavioral Sciences and the Law, 18*, 1-21.
31. Centre for Strategic and International Studies. (1994). *Global Organized Crime: the New Empire of Evil*, Washington.
32. Centre for the Prevention of Radicalization Leading to Violence (2018). *Types of Radicalization*.
33. Chandler, D. (2014). *Resilience: The Governance of Complexity*. Routledge: New York.

34. Clarisa Nelu (2024). Exploitation of Generative AI by Terrorist groups, достапно на: https://icct.nl/publication/exploitation-generative-ai-terrorist-groups?
35. Coaffee, J. (2009). *Terrorism, Risk and the Global City. Towards Urban Resilience*. Burlington: Ashgate.
36. Coaffee, J., Fussey, P. (2015). Constructing resilience through security and surveillance: The politics, practices and tensions of security-driven resilience. *Security Dialogue*. Vol. 46:1, pp. 86-105.
37. "Considerations of the Impacts of Generative AI on Online Terrorism and Extremism. (2023). GIFCT Red Team Working Group.
38. Council of Europe Handbook. (2016). *For prison and probation services regarding radicalization and violent extremism*, Strasbourg, p.10.
39. Council of Europe. (2016). Octopus Conference 2016 "Cooperation against Cybercrime. Key messages". Достапно на: https://www.coe.int/en/web/cybercrime/octopus-interface-2016#:~:text=Service%20provider%20/%20law%20enforcement%20cooperation,Committee%20(T%2DCY).
40. Council of the European Union. (2022). "The Metaverse in the Context of the Fight Against Terrorism", Special Report. Достапно на: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://data.consilium.europa.eu/doc/document/ST-9292-2022-INIT/en/pdf
41. Countering Terrorism Online With Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia," United Nations Office of Counter-Terrorism and United Nations Interregional Crime and Justice Research Institute. (2021). Достапно на: https://unicri.org/Publications/Countering-Terrorism-Online-with-Artificial-Intelligence-%20SouthAsia-South-EastAsia
42. Crenshaw, M. (2008). Theories of terrorism: Instrumental and organizational approaches, *Journal of Strategic Studies*, Volume 10.
43. Cynthia Stohl, Michael Stohl. (2007). Networks of terror: theoretical assumptions and pragmatic consequences, *Communication Theory*, 17(2), 93–124.
44. Dalins, J. at al. (2017). *Criminal motivation on the dark web: A categorisation model for law enforcement*. Digit. Investig.
45. Dandurand, Y. (2015). Social Inclusion Programmes for Youth and the Prevention of Violent Extremism, in: Marco Lombardi et al. (eds.). *Countering Radicalisation and Violent Extremism Among Youth to Prevent Terrorism*. Amsterdam: IOS Press.
46. Debuire, D. (2022) "Terror-ist use of the Metaverse: new opportunities and new challenges", *The Security Distillery*. Достапно на: https://thesecuritydistillery.org/all-articles/terrorism-and-the-metaverse-new-opportunities-and-new-challenges

47. Dell's, (2015) Annual Security Report. Достапно на: http://www.huffingtonpost.com/daniel-wagner/the-growing-threat-of-cyb_b_10114374.html
48. Desivilya, H, at all. (1996). "Extent of Victimization, Traumatic Stress Symptoms, and Adjustment of Terrorist Assault Survivors: A Long-term Follow-up," *Journal of Traumatic Stress* 9, no. 4: 881-889. Достапно на: https://link.springer.com/article/10.1007/s00737-018-0824-3
49. European Commission. (2020) "Communication from the Commission on the EU Security Union Strategy," Brussels, COM (2020) 605 final. Достапно на: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/resource.html?uri=cellar:74d1acf7-3f94-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF
50. Desta, T. A. (2016). *Preventing violent extremism: A new paradigm or evolving approach?* Bern: Swisspeace. Достапно на: https://varia.swisspeace.ch/apropos/preventing-violent-extremism-new-paradigm-evolving-approach/
51. DiPiero, C. (2017). Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web. U. *Ill. L. Rev.*1267.
52. Duncan Watts, Steven H Strogatz. (1998). Collective Dynamics of 'Small-World Networks, *Nature,* Vol. 393.
53. Early terrorist experimentation with generative artificial intelligence services. (2023). Tech Against Terrorism. Достапно на: https://techagainstterrorism.org/hubfs/Tech%20Against%20Terrorism%20Briefing%20-%20Early%20terrorist%20experimentation%20with%20generative%20artificial%20intelligence%20services.pdf
54. Easley, M. (2022). "How Interconnected, Simulated Worlds Could Transform Military Training." *NDIA Business & Technology Magazine*. Достапно на: www.nationaldefensemagazine.org/articles/2022/11/23/how-interconnected-simulated-worlds-could-transform-military-training
55. ECPAT International. (2017). Online child sexual exploitation: A common understanding. Достапно на: https://ecpat.org/resource/online-child-sexual-exploitation-a-common-understanding/
56. ECPAT International. (2020). Why children are at risk of sexual exploitation during COVID-19. Достапно на: https://ecpat.exposure.co/covid19?utm_source=Website&utm campaign=Hero
57. Edward G. Amoroso. (2011). *Cyber Attacks Protecting National Infrastructure*, Elsevier Inc, USA.
58. Edward Silva. (2020). The HCR-20 and violence risk assessment, *BJPsych Bull.* и Douglas KS, Hart SD, Webster CD, Belfrage H. (2013). *HCR-20V3: Assessing Risk of Violence – User Guide*. Mental Health, Law, and Policy Institute, Simon Fraser University.
59. Elson, J at all. (2022). "The metaverse offers a future full of potential – for terrorists and extremists", *The Conversation*. Достапно на:

https://theconversation.com/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too-173622
60. Engjellushe, M at all. (2019). *Community Perspectives on Preventing Violent Extremism Lessons learned from the Western Balkans*. Research Report. Достапно на: https://www.rcc.int/swp/docs/289/community-perspectives-on-preventing-violent-extremism--lessons-learned-from-the-western-balkans-2019
61. Enternmann, E., Willem van der Berg. (2018). *Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?* International Centre for Countering Terrorism, Hague.
62. Esmailzadeh, Y. (2023). "Potential Risks of ChatGPT: Implications for Counterterrorism and International Security," *International Journal of Multicultural and Multireligious Understanding* 10:4.
63. European Commission, Joint Research Centre (JRC) (2022). *Security by design: Protection of public spaces from terrorist attacks*, Luxembourg: Publications Office of the European Union.
64. European Commission. (2020). "Proposal for a Directive of the european parliament and of the Council on the Resilience of Critical Entities," Brussels, COM (2020) 829 final. Достапно на: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022SC0289
65. European Commission. (2022). "Automated Serious Game Scenario Generator for Mixed Reality Training." *CORDIS*. Достапно на: https://cordis.europa.eu/project/id/653590
66. European Commission's Expert Group on Violent Radicalization (2008). *Radicalisation Processes Leading to Acts of Terrorism*. Report. Достапно на: https://www.clingendael.org/sites/default/files/pdfs/20080500_cscp_report_vries.pdf
67. EUROPOL. (2019). IOCTA 2019. Достапно на: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019
68. EUROPOL. (2019). Operation Chemosh: How encrypted chat groups exchanged emoji 'stickers' of child sexual abuse. Достапно на: https://www.europol.europa.eu/media-press/newsroom/news/operation-chemosh-how-encrypted-chat-groups-exchanged-emoji-%E2%80%98stickers%E2%80%99-of-child-sexual-abuse
69. EUROPOL. (2020a). Beyond the pandemic: How COVID-19 will shape the serious and organised crime landscape in the EU. Достапно на: https://www.europol.europa.eu/publications-events/publications/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu
70. EUROPOL. (2020b). Catching the virus cybercrime, disinformation and the COVID-19 pandemic. Достапно на: https://www.europol.europa.eu/publications-events/publications/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

71. EUROPOL. (2020c), Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic.
72. Everette J, (2017) *Public-Private Analytic Exchange Program: Risks and Vulnerabilities of Virtual Currency,* Washington: Director of National Intelligence.
73. FBI. (2020). School Closings Due to COVID-19 Present Potential for Increased Risk of Child Exploitation. Достапно на: https://www.fbi.gov/news/pressrel/press-releases/school-closings-due-to-covid-19-present-potential-for-increased-risk-of-child-exploitation.
74. Fjäder, C. (2014). "The Nation-state, National Security and Resilience in the Age of Globalization," *Resilience: International Policies, Practices and Discourses* 2, no. 2: 114-129.
75. Forbes. (2020). Child Exploitation Complaints Rise 106% To Hit 2 Million In Just One Month: Is COVID-19 To Blame?. Достапно на: https://www.forbes.com/sites/thomasbrewster/2020/04/24/child-exploitation-complaints-rise-106-to-hit-2-million-in-just-one-month-is-covid-19-to-blame/
76. Francesco Badia, Dalmases. (2010). Small-World Networks, Violence and Global Distress, chapter 9 in Martin Jones, David Lane, Ann and Paul Schulte (eds) *Terrorism, Security and the Power of Informal Networks*. Cheltenham, UK: Edward Elgar Publishing Limited, 217-240.
77. Gal, R., Lazarus, R. (1975). "The Role of Activity in Anticipating and Confronting Stressful Situations," *Journal of Human Stress* 1, no. 4: 4-20. Достапно на: https://pubmed.ncbi.nlm.nih.gov/1235121/
78. Garcia M, Pasic, L. (2018). Youth work against violent radicalization-Theory, concept and primary prevention in practice, Council of Europe and European Commission, Council of Europe Publishing: Strasbourg Cedex.
79. George Loukas. (2015). *Cyber-Physical Attaks- A Growing Invisible Threat*, Elsevier Inc, USA.
80. Gibson, C.A., Tarrant, M. (2010). A 'Conceptual Models' Approach to Organisational Resilience. *Australian Journal of Emergency Management*, 25(2), 6-12.
81. Gilbert, D (2023). "Here's How Violent Extremists Are Exploiting Generative AI Tools," *Wired*. Достапно на: https://www.wired.com/story/generative-ai-terrorism-content/
82. Gill, P. (2015). *Lone- Actor Terrorism: A Behavioral Analysis*. New York: Routledge.
83. "GIFCT's Hash-Sharing Database," (2023). Global Internet Forum to Counter Terrorism.
84. Glaser, M. (2017). "Extremist, militant, radicalised?" in Glaser et al. (Eds.) *Young and Radical. Political Violence During Adolescence*, Deutsches Jugendinstitut: Munchen.
85. Global Terrorism Index. (2015). *Measuring and understanding the impact of terrorism*. Institute of Economisc and Peace, Sydney.

86. Global Terrorism Index. (2024). *Measuring and understanding the impact of terrorism*. Institute of Economisc and Peace, Sydney.
87. Government of the Republic of Macedonia. (2018). National Committee for Countering Violent Extremism and Countering Terrorism, *National strategy of the Republic of Macedonia for countering violent extremism (2018-2022),* Skopje.
88. Graham-McLay, C. (2019). Death Toll in New Zealand Mosque Shootings Rises to 51. *The New York Times,* May 2. Достапно на: https://www.nytimes.com/2019/05/02/world/asia/new-zealand-attack-death-toll.html
89. Hamm, M. S. (2002). *In Bad Company: America's Terrorist Underground*. Boston: Northeastern University Press.
90. Hemmingby, C, Bjørgo, T. (2016). *The Dynamics of a Terrorist Targeting Process: Anders B.Breivik and the 22 July Attacks in Norway*. London/New York: Palgrave Macmillan.
91. Herath, C., Jarnecki, J. (2022). "Securing Future Realities: What Can We Expect from the Metaverse?" *RUSI*. Достапно на:https://rusi.org/explore-our-research/ publications /commentary/securing-future-realities-what-can-we-expect-metaverse
92. Hewitt, C. (2003). *Understanding Terrorism in America: From the Klan to Al-Qaeda*. New York: Routledge.
93. Hoffman, B. (2006). *Inside Terrorism*. New York: Columbia University Press.
94. Holmer, G., Baumann P. (2018). *Taking Stock. Analytic Tools for Understanding and Designing C/PVE Programs*. Washington, DC: United States Institute of Peace.
95. Holmer, G., Baumann P. (2018). *Taking Stock. Analytic Tools for Understanding and Designing C/PVE Programs*. Washington, DC: United States Institute of Peace.
96. Hower S. (2011). *Cyberterrorism,* Santa Barbara, CA: Greenwood.
97. http://luxembourgguidelines.org/
98. https://assets.publishing.service.gov.uk/media/5a78966aed915d07d35b0dcc/prevent-strategy-review.pdf
99. https://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf
100. https://cybermaterial.com/north-macedonias-ministry-of-economy-hacked/
101. https://ics-cert.kaspersky.com/publications/reports/2024/04/11/h2-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/?
102. https://new.mia.mk/en/story/mepso-hit-by-cyberattack-power-grid-and-electricity-supply-not-threatened?
103. https://telegrafi.com/en/Kosovo-institutions-targeted-by-hackers--new-wave-of-cyber-attacks-from-Russia-warned/?
104. https://thesoufancenter.org/intelbrief-2024-october-16/
105. https://unicri.org/sites/default/files/2024-09/Generative-AI-New-Threat-Online-Child-Abuse.pdf?

106. https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users
107. https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users?
108. https://www.fbi.gov/investigate/cyber/news?
109. https://www.ft.com/content/49a49961-0dc9-4d19-bb26-7020e07e465c?
110. https://www.hashtag.al/en/index.php/2024/05/27/infrastruktura-kritike-u-sulmua-49-here-nga-hakeret-ne-vitin-2023/?
111. https://www.interpol.int/en/News-and-Events/News/2025/20-arrested-in-international-operation-targeting-child-sexual-abuse-material?
112. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata?
113. https://www.techradar.com/pro/security/nsa-says-volt-typhoon-was-not-successful-at-persisting-in-critical-infrastructure?
114. https://www.theguardian.com/world/2025/aug/14/russian-hackers-control-norwegian-dam-norway?
115. ICT4PEACE Foundation. (2016). "Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes,". Достапно на: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/private-sector-engagement-in-responding-to-the-use-of-the-internet-and-ict-for-terrorist-purposes.pdf
116. Il-Chul Moon, Kathleen M Carley, and Alexander Levis. (2008). *Vulnerability Assessment on Adversarial Organization: Unifying Command and Control Structure Analysis and Social Network Analysis*, SIAM International Conference on Data Mining, Workshop on Link Analysis, Counterterrorism and Security, Atlanta, GA.
117. Independent. (2020). Matthew Falder: One of Britain's most prolific paedophiles challenges 32-year prison sentence for 'sadistic' crimes. Достапно на: https://www.independent.co.uk/news/uk/crime/matthew-falder-paedophile-appeal-_prison-sentence-blackmail-cambridge-a8585881.html
118. IntelBrief (2020). IntelBrief: Terrorists' Use of Cryptocurrency, The Soufan Center, New York, USA, December 10. Достапно на: https://thesoufancenter.org/intelbrief-2020-december-10/
119. International Centre for Counter-Terrorism (2025). Достапно на: https://icct.nl/
120. International Centre for the Prevention of Crime. (2015). Study on *"Preventing Radicalisation: A Systematic Review"*. Достапно на: https://www.researchgate.net/publication/303896097_Preventing_Radicalization_A_Systematic_Review

121. Internet Organized Crime Assessment (2024), EUROPOL, достапно на: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
122. "Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats," (2018). Joint Communication to the European Parliament, the European Council and the Council, JOIN/2018/16 final (Brussels: European Commission. Достапно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018JC0016
123. Internet Watch Foundation. (2018). Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse. Достапно на: https://www.iwf.org.uk/media/23jj3nc2/distribution-of-captures-of-live-streamed-child-sexual-abuse-final.pdf
124. INTERPOL. (2020). Threats and trends: child sexual exploitation and abuse, COVID-19 impact.
125. INTERPOL. (2022). "INTERPOL launches first global police Metaverse.". Достапно на: https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse#:~:text=NEW%20DELHI%2C%20INDIA%20%2D%20The%20Metaverse,designed%20for%20law%20enforcement%20worldwide.
126. Jackson, R at all. (2011). *Terrorism: A Critical Introduction,* Palgrave Macmillan.
127. Jenkins, B. (2011). *Stray Dogs and Virtual Armies: Radicalization and Recruitment to Jihadist Terrorism in the United States since 9/11*. Santa Monica, CA: RAND
128. Jennifer Xu,Hsinchuen Chen. (2008). The topology of dark networks. *Communications of the ACM* 51(10), New York, NY. Достапно на: https://experts.arizona.edu/en/publications/the-topology-of-dark-networks/
129. John Arquilla, David Ronfeldt. (2001). *Networks and netwar: The Future of Terror, Crime and Militancy*, Santa Monica, CA: RAND Corporation.
130. John Baylis, at all. (2022). *Strategy in the Contemporary World*, 7th edition, Oxford University Press, USA.
131. John Lichfield. (2015). TV5Monde hack: 'Jihadist' cyber attack on French TV station could have Russian link, Independent, London, United Kingdom.
132. Joscelyn, T. (2016). Terror Plots in Germany, France Were 'remote-Controlled' by Islamic State Operatives. *FDD's Long War Journal*. Достапно на: http://www.longwarjournal.org/archives/2016/09/terror-plots-in-germany-france-were-remote-controlled-by-islamic-state-operatives.php
133. Kathleen M Carley. (2006). Destabilization of Covert Networks, Computational and Mathematical Organization Theory 12, No. 1.

134. Kathleen M. Carley. (2002). *Inhibiting Adaptation*, Proceedings of the 2002 Command and Control Research and Technology Symposium, Monterrey, CA: Naval Post Graduate School.
135. Kissel R., (ed.). (2011). *Glossary of Key Information Security Terms*.
136. Levin, J. (2024). Violent Extremists in the Metaverse, *Global Affairs Review*, The Center for Global Affairs, New York University. Достапно на: https://wp.nyu.edu/schoolofprofessionalstudies-ga_review/violent-extremists-in-the-metaverse/
137. Lewis, J. (2007). *Cyber Attacks Explained*. Center for Strategic and International Studies (CSIS). Достапно на: https://www.comw.org/rma/fulltext/070615lewis.pdf
138. Lucia B. et al. (2020), *Transformative technologies: How digital is changing the landscape of organized crime*, Global Initiative against Transnational Organized Crime. Достапно на: https://globalinitiative.net/wp-content/uploads/2020/06/Transformative-Technologies.pdf
139. Maksim Tsvetovat and Kathleen M Carley, (2007). On Effectiveness of Wiretap Programs in Mapping Social Networks, *Computational and Mathematical Organization Theory* 13, No. 1, 67-68.
140. Maksim Tsvetovat, Kathleen M Carley. (2003). Bouncing Back: Recovery Mechanisms of Covert Networks, Proceedings of the 2003 North American Association of Computational Social and Organization Science, Kathleen M Carley (ed.), Pittsburgh, PA:Carnegie Mellon University.
141. Malik N. (2018). When it comes to Child Sexual Exploitation, we cannot ignore the Darknet, Forbes, 4 September 2018. Достапно на: https://www.forbes.com/sites/nikitamalik/2018/09/04/when-it-comes-to-child-sexual-exploitation-we-cannot-ignore-the-darknet/
142. Malik, N. (2018). "How Criminals And Terrorists Use Cryptocurrency: And How To Stop It," *Forbes,* August 31st. Достапно на: https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/
143. Malthaner, S, Waldmann, P. (2014). "The Radical Milieu: Conceptualizing the Supportive Social Environment of Terrorist Groups." *Studies in Conflict & Terrorism* 37(12).
144. Malthaner, S. et al. (2017). "*D5.4 Lone Actor Radicalisation Subscript*", FP7 PRIME Project.
145. Marc Sageman. (2004). *Understanding terror networks*. Philadelphia: University of Pennsylvania Press.
146. McGuffie, K., Newhouse, A. (2020). "The Radicalization Risks of GPT-3 and Advanced Neural Language Models," Достапно на: Arxiv.
147. McKendrick, K. (2019). "Artificial Intelligence Prediction and Counterterrorism," International Security Department, *Royal Institute of International Affairs*.

148. McLagan, G, Lowles, N. (2000). *Mr. Evil: The Secret Life of Racist Bomber and Killer David Copeland.* London: John Blake Publishing.
149. Melanie Mitchell. (2006). Complex Systems: Network Thinking. *Artificial Intelligence*, Vol. 170, Issue 18.
150. Michael Stohl. (1983). The international network of terrorism, *Journal of Peace Research*, 20(1), 87–94.
151. Michael Stohl. (2008). Networks, terrorists and criminals: the implications for community policing. *Crime Law Social Change,* Springer Science+ Business Media.
152. Moghaddam, F.M. (2005). *The Staircase to Terrorism; A Psychological Exploration*, Georgetown University.
153. Monica Lloyd. (2019). *Extremism Risk Assessment: A Directory*, Centre for Research and Evidence on Security Threats, University of Birmingham.
154. Montgomery, B. (2024). "Sora: OpenAI launches tool that instantly creates video from text," *The Guardian*. Достапно на: https://www.theguardian.com/technology/2024/feb/15/openai-sora-ai-model-video
155. Morgan, M. J. (2004). The origins of the new terrorism. *Parameter, 34*, 29-43.
156. Muro, D. (2016). *What does radicalization look like? Four visualizations of socialization into violent Extremism*, Barcelona Centre for International Affairs.
157. Nairn Moises. (2005). *Illicit: How Smugglers, Traffickers, and Copycats are Hijacking the Global Economy*, New York: Doubleday.
158. NCMEC CyberTipline. (2021). Достапно на: https://www.missingkids.org/gethelpnow/cybertipline.
159. Nickolov E. (2008). "Modern Trends In The CyberAttacks Against The Critical Information Infrastructure", ITU, Regional Cybersecurity Forum, Sofia, Bulgaria.
160. NYPD. (2014). Threat to U.S. 'Growing Exponentially with ISIS.' *CBS News*, September 11. Достапно на: https://www.cbsnews.com/news/terror-threat-to-us-growing-exponentially-with-isis-nypd-says/.
161. Oftedal, E. (2015). *The Financing of Jihadi Terrorist Cells in Europe*, Norway: Forsvarets Forskningsinstitutt.
162. OSCE. (2018). *The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism*. A Guidebook for South-Eastern Europe. Transnational Threats Department: Vienna, Austria. Достапно на: https://www.osce.org/resources/publications.
163. OSCE. (2019). *Understanding Referral Mechanisms in Preventing and Countering Violent Extremism and Radicalization That Lead to Terrorism Navigating Challenge and Protecting Human Rights*. A Guidebook for South-Eastern Europe, Transnational Threats Department: Vienna, Austria. Достапно на: https://www.osce.org/resources/publications.

164. Oxford Learner Dictionary. (2008). *Fourth Edition,* China: Oxford University Press.
165. Ozdamar, O. (2008). "Theorizing Terrorist Behavior: Major Approaches and Their Characteristics", *Defence Against Terrorism Review 1,* No. 2.
166. Padan, C., Gal, R. (2020). A Multi-dimensional Matrix for Better Defining and Conceptualizing Resilience, *Connections Quarterly Journal* 19, no. 3, 33-46.
167. Pantucci, R. (2011). "*A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists"*. The International Centre for the Study of Radicalisation and Political Violence, London.
168. Partnering to Help Curb Spread of Terrorist Content," (2016). Meta. Достапно на: https://about.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/
169. Peter Monge, Janet Fulk. (1999). *Shaping Organizational Form: Communication, Connection, and Community*, Thousands Oaks, Sage.
170. Peter R Monge, Noshir Contractor. (2003). *Theories of communication networks*, Oxford: Oxford University Press.
171. Peter Sheridan Dodds, Roby Muhamad, Duncan J. Watts. (2003). An Experimental Study of Search in Global Social Networks*, Science*, Vol. 30.
172. Phil Williams. (1999). Transnational criminal networks, in John Arquilla and David Ronfeldt (eds), *Networks and netwars*, Santa Monica: RAND.
173. Pickett, S et al. (2014). Ecological resilience and resilient cities. *Building Research & Information*. Vol. 42:2, pp. 143-157.
174. PPD-21. (2013). Presidential policy directive/PPD-21. The White House.
175. Pressman, D.E. (2009). *Risk Assessment Decisions for Violent Political Extremism*. Достапно на: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2009-02-rdv/index-en.aspx
176. Prior, T. (2018). "Resilience: The 'Fifth Wave' in the Evolution of Deterrence," in *Strategic Trends 2018: Key Developments in Global Affairs*, ed. O. Thränert and M. Zapf, Zurich: Center for Security Studies, ETH Zurich.
177. Pursiainen C., (2009). *The Challenges for European Critical Infrastructure Protection*, European Integration, vol. 31, no. 6.
178. Resilience and Article 3, *NATO Topics*. Достапно на: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse213-EN.pdf
179. Rogers, P. (2017). 'The etymology and genealogy of a contested concept', in David Chandler and Jon Coaffee (eds.). *The Routledge Handbook of International Resilience*. New York: Routledge.
180. Russel Howard. (2004). *Terrorism and Counterterrorism*, The McGraw-Hill/Dushkin, Connecticut.

181. Sampaio, A. (2017). "Resilience Gains Ground in Counter-Terrorism Strategies," *Jane's Intelligence Review* 29, no. 12: 18-21.
182. Sandbrink. J. (2023). "ChatGPT could make bioterrorism horrifyingly easy," *Vox*. Достапно на: https://www.vox.com/future-perfect/23820331/chatgpt-bioterrorism-bioweapons-artificial-inteligence-openai-terrorism.
183. Schmid, A (Ed.) (2011). *The Routledge Handbook of Terrorism Research*. London and New York: Routledge.
184. Schmid, A. P. (2013). *Radicalization, De-Radicalization, Counter-Radicalization: A Conceptual Discussion and Literature Review*. ICCT Research Paper.
185. Schmitt, S. (2017). Lessons Learned from Countering Violent Extremism Development Interventions, *Small Wars Journal*.
186. Scholz, R. et al. (2012). Risk, vulnerability, robustness and resilience from decision-theoretic perspective. *Journal of Risk Research*. Vol. 15:3, pp. 313-330.
187. Schuurman, B, et al. (2015). "The Hofstadgroup Revisited: Questioning its Status as a 'Quintessential' Homegrown Jihadist Network,". *Terrorism and Political Violence* 27 (5).
188. Schuurman, B, et al. (2017). "Lone Actor Terrorist Attack Planning and Propaganda: A Data Driven Analysis.", *Journal of Forensic Sciences*. Достапно на: https://www.researchgate.net/publication/320581916_Lone_Actor_Terrorist_Attack_Planning_and_Preparation_A_Data-Driven_Analysis
189. Search for Common Ground (2017). *Transforming Violent Extremism – A Peacebuilder's Guide*. Достапно на: https://documents.sfcg.org/wp-content/uploads/2017/04/Transforming-Violent-Extremism-V2-August-2017.pdf
190. Seierstad, A. (2016). Is Norwegian mass murderes Anders Breivik still a threat to Europe? *Newsweek*. Достапно на: https://www.newsweek.com/anders-breivik-neo-nazi-suing-norway-asne-seierstad-447247
191. Sendai Framework for Disaster Risk Reduction 2015 – 2030, *United Nations Office for Disaster Risk Reduction, UN General Assembly*, Достапно на: https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030
192. Shapiro, J. N. (2012) "Terrorist Decision-Making: Insights from Economics and Political Science," *Perspectives on Terrorism*, Vol. 6, No. 4–5.
193. Simon, J. (2013). *Lone Wolf Terrorism: Understanding the Growing Threat*. Amherst, NY: Prometheus Books.
194. Sloan, S. (2006). *Terrorism: The Present Threat in Context*. Oxford: Berg Publishers.
195. Solon, O. (2021). Child sexual abuse images and online exploitation surge during pandemic. Достапно на: https://www.nbcnews.com/tech/tech-

news/child-sexual-abuse-images-online-exploitation-surge-during-pandemic-n1190506
196. Spaaij, R. (2012). *Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention*. New York: Springer.
197. Stalinsky, S. (2018). "The Cryptocurrency-Terrorism Connection Is Too Big to Ignore," *Washington Post*, December 17.
198. Stanković, N. (2021). Resilience: Conceptual framework and methodological tool for assessing and improving the state of regional security, Trapara, V., N. Šekarić (eds.), *Regional security: approaches, elements, dynamics, Institute for International Politics and Economy*, Belgrade.
199. Steven H Strogatz, (2001). Exploring Complex Networks, *Nature* 410, No. 6825.
200. Steven Simon, Daniel Benjamin. (2000). America and the New Terrorism, *Survival*, Vol. 42, no. 1, 70.
201. Stop It Now. (2021). How People Use the Internet to Sexually Exploit Children and Teens. Достапно на: https://www.stopitnow.org/ohc-content/prevention-on-the-internet
202. STRATFOR (2015). "The Coming Age of Cyberterrorism". Достапно на: https://www.stratfor.com/weekly/coming-age-cyberterrorism
203. STRATFOR. (2015). "Examining the Islamic State's Cyber Capabilities", 2015. Достапно на: https://www.stratfor.com/analysis/examining-islamic-states-cyber-capabilities
204. Svitkova, K. (2017). *Resilience in the national security discource*, Defense and Strategy.
205. Taher, A. (2023). "AI chatbots could be 'easily be programmed' to groom young men into launching terror attacks, warns top lawyer," *Daily Mail*. Достапно на: https://www.dailymail.co.uk/sciencetech/article-11952997/amp/AI-chatbots-easily-programmed-groom-young-men-terror-attacks-warns-lawyer.html?s=03
206. Tamara Makarenko. (2004). The crime-terror continuum: tracing the interplay between transnational organised crime and terrorism, *Global Crime*, 6(1), 129–145.
207. Tech Against Terrorism (2025), достапно на: https://techagainstterrorism.org/home
208. Tech Trends Position Statement – Generative AI. (2023). eSafety Commissioner.
209. The impact of Large Language Models on Law Enforcement. The Hague: EUROPOL Innovation Lab.
210. The United States Department of Justice (2020). Office of Public Affairs, *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*, August 13. Достапно на: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.
211. Thomas A. Johnson (ed). (2015). *Cyber Security-Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press.

212. Turpin-Petrosino, C. (2015). *Understanding Hate Crime: Acts, Motives, Offenders, Victims, and Justice*. New York: Routledge.
213. UN Security Council Resolution 1368, 12. September 2001, SC. Res.1373, 28 September 2001.
214. UNICEF. (2020). COVID-19: Children at heightened risk of abuse, neglect, exploitation and violence midst intensifying containment measures. Достапно на: https://www.unicef.org/press-releases/covid-19-children-heightened-risk-abuse-neglect-exploitation-and-violence-amidst
215. United Nations Office for Disaster Risk Reduction (UNISDR). (2009). "2009 UNISDR Terminology on Disaster Risk Reduction", Geneva, Достапно на: https://www.undrr.org/publication/2009-unisdr-terminology-disaster-risk-reduction
216. US Office of the Director of National Intelligence (ODNI). (2020) "Counterterrorism Guide for Public Safety Personnel." *JCAT*. Достапно на: https://www.dni.gov/nctc/jcat/index.html
217. Vale, L. (2014). The politics of resilient cities. Whose resilience and whose city? *Building Research & Information*. Vol. 42:2, pp. 191-201.
218. Verhelst, H.M. at all. (2020). "Machine Learning against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma," *Science and Engineering Ethics* 26.
219. Wagner L, Thi Hoang. (2020). Aggravating circumstances: How corona virus impacts human trafficking, Global Initiative Against Transnational Organized Crime. Достапно на: https://globalinitiative.net/wp-content/uploads/2020/06/Aggravating-circumstances-How-coronavirus-impacts-human-trafficking-GITOC-1.pdf
220. Wagner L. at all. (2021). Exploited in Plain Sight-An assessment of commercial sexual exploitation of children and child protection responses in the Western Balkans, Global Initiative against Transnational Organized Crime's Observatory of Illicit Economies in South Eastern Europe (SEE-Obs), Geneva, Switzerland.
221. Wagner, A. (2007). "Intelligence for Counter-Terrorism: Technology and Methods," *Journal of International Affairs* 2:2 (2007): pp. 48-61.
222. Walker, B., Salt, D. (2006). *Resilience Thinking: Sustaining Ecosystems and People in a Changing World*. London: Island Press.
223. Ward, A. (2018). "Bitcoin and the Dark Web: The New Terrorist Threat?" *RAND Corporation,* January. Достапно на: https://www.rand.org/pubs/commentary/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html
224. Ware, J. (2023). "The Violent Far-Right Terrorist Threat to the U.S. Military." *Council on Foreign Relations*. Достапно на: https://www.cfr.org/blog/violent-far-right-terrorist-threat-us-military.
225. Watts J Duncan, (2003). *Six Degrees: The Science of a Connected Age*, New York: W.W. Norton and Co.

226. Weimann, G. (2005). *Terror on the Internet, The New Arena, the New Challenges*, Washington, D.C.: United States Institute of Peace Press.
227. Weimann, G. (2015). *Terror in Cyberspace: The Next Generation*, New York: Columbia University Press.
228. Weimann, G. (2016). "Going Dark: Terrorism on the Dark Web", *Studies in Conflict&Terrorism* 39, 195-206. Достапно на: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546.
229. Wells, D. (2022). "Why outsourcing counter-terrorism online won't work in future," Lowy Institute. Достапно на: https://www.lowyinstitute.org/the-interpreter/why-outsourcing-counter-terrorism-online-won-t-work-future
230. What is Generative AI? (2023). Goaltide.
231. White, R. J. (2003). *Terrorism: An Introduction*. Belmont, CA: Wadsworth.
232. WHO (2020). Joint Leader's statement - Violence against children: A hidden crisis of the COVID-19. Достапно на: https://www.who.int/news-room/detail/08-04-2020-joint-leader-s-statement---violence-against-children-a-hidden-crisis-of-the-covid-19-pandemic
233. Wiktorowicz, Q. (2004). "Joining the Cause: Al-Muhajiroun and Radical Islam", *The Roots of Radical Islam*, Department of International Studies, Rhodes College.
234. Wiktorowicz, Q. (2005). *Radical Islam Rising: Muslim Extremism in the West*. London: Rowman & Littlefield.
235. World Economic Forum, (2016), "Network Name ; "Industrial IoT.".
236. World Economic Forum. (2016). White Paper. "*Global Agenda Council on Cybersecurity"*. Достапно на: https://assets.publishing.service.gov.uk/media/66f6d04cc71e42688b65ee14/GST_the_future_starts_today_ARCHIVE.pdf
237. Yonah, A. (1976). *International Terrorism: National, Regional and Global Perspectives*. New York: Praeger.
238. Бакрески, О, Милошевска, Т. (2021). *Безбедноста на информациите и критичната инфраструктура*, Дирекција за безбедност на класифицирани информации, Скопје.
239. Калач Ј. (2017). Сајбер тероризмот како закана кон безбедноста на државата, *Правдико*.
240. Милошевска Т. (2106). *Модели на поврзаност на тероризмот и на транснационалниот организиран криминал*, Универзитет Св. Кирил и Методиј, Филозофски факултет, МАР-САЖ Скопје.
241. Мишевски Д. (2017). Осигурување од сајбер ризици, *Осигурување*, Национално биро за осигурување-Македонија, бр.11, Скопје.
242. Национална стратегија за сајбер безбедност на Република Македонија (2018-2022), јули 2018. Достапно на: https://www.itu.int/en/ITU-

D/Cybersecurity/Documents/National_Strategies_Repository/Macedonia_ns_sajber_bezbednost_2018-2022.pdf
243. Петровић, Р.С. (2007). *Полицијска информатика*, Криминалистичко-полицијска академија, Београд.
244. Правна рамка за обезбедување на критичната инфраструктура. (2016). Комора на РМ за приватно обезбедување, Скопје.
245. Стратегија за сајбер безбедност (2025-2028), 2025. Достапно на: https://mdt.gov.mk/files/sodrzina_na_CCB_2025_2028_usoglasen_tekst.pdf