



УНИВЕРЗИТЕТ „СВ. КИРИЛ И МЕТОДИЈ“ – СКОПЈЕ



ФИЛОЗОФСКИ ФАКУЛТЕТ

ИНСТИТУТ ЗА БЕЗБЕДНОСТ, ОДБРАНА И МИР

НАСОКА: БЕЗБЕДНОСЕН МЕНАЏМЕНТ

МАГИСТЕРСКИ ТРУД

Тема:

**ПРОФИЛИРАЊЕТО НА ТЕРОРИЗМОТ ВО ЕРАТА НА
ВЕШТАЧКАТА ИНТЕЛИГЕНЦИЈА**

Ментор:

Проф. д-р Тања Милошевска

Изработила:

Тамара Митковска 5550/24

Скопје, 2026

Содржина

1. ВОВЕД _____	4
1.1 Формулација на проблемот на истражување _____	4
1.2 Дефинирање на предметот на истражување _____	6
1.3 Досегашни истражувања _____	8
1.4 Цели и задачи _____	10
1.5 Дефинирање на основните поими _____	12
1.6 Основна хипотетичка рамка _____	15
1.7 Научна и општествена оправданост _____	17
1.8 Методи и техники на истражувањето _____	18
2. ТЕРОРИЗАМ _____	19
2.1 Дефинирање _____	20
2.2 Историски развој _____	22
2.3 Типологија _____	24
3. ПРОФИЛИРАЊЕ _____	31
3.1 Општо дефинирање на профилирањето _____	31
3.2 Дефинирање на профилирањето низ призма на тероризмот _____	33
3.3 Дистинкција помеѓу криминално профилирање и профилирање на тероризмот _____	34
3.4 Историски развој _____	36
3.4.1 Раните почетоци _____	36
3.4.2 Профилирањето денес _____	39
3.5 Видови профилирање _____	39
3.5.1 Географско профилирање _____	42
3.5.2 Биометриско профилирање _____	44
3.5.3 Психолошко профилирање _____	45
3.6 Практична примена на профилирањето _____	49

3.7 Предности и недостатоци на профилирањето _____	54
4. ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА _____	55
4.1 Дефинирање _____	55
4.2 Историја _____	58
4.3 Улогата на ВИ во процесот на профилирање на тероризмот _____	60
4.4 Примена на ВИ во профилирање на тероризмот _____	62
4.4.1 Примена на ВИ во Македонија _____	64
4.4.2 Системите АДАМС и ФАСТ на САД _____	65
4.4.3 Единицата на ЕУ за упатување на интернет (ИРУ) _____	68
4.4.4 Системи базирани на ВИ на Израел _____	71
4.5 Примена на ВИ од страна на терористички групи _____	73
4.6 Анализа на законот за безбедност на мрежни и информациски системи _____	76
4.7 Актот за ВИ на Европска Унија _____	82
4.8 Предности и недостатоци од користење на ВИ во профилирање на тероризмот _____	87
5. ЗАКЛУЧОК _____	93
КОРИСТЕНА ЛИТЕРАТУРА _____	99

1. ВОВЕД

1.1 Формулација на проблемот на истражување

Во динамичната и технолошки напредна безбедносна средина на 21 век, радикализацијата и екстремизмот сè почесто се манифестираат преку дигитални канали, со што се намалува способноста на традиционалните механизми на детекција и превенција да ги идентификуваат ранливите поединци и потенцијалните терористички закани навремено. Онлајн просторот овозможува дискретно ширење на екстремистички идеологии, брза мобилизација и регрутација, како и планирање на терористички напади, често без физички контакт меѓу учесниците.

Со појава на глобализацијата и интернационализацијата не само што ескалирале веќе постоечките проблеми, туку се појавиле и низа други закани и одредени дилеми со што започнува процесот на проширување на безбедносниот концепт со нов вид закани, меѓу кои и тероризмот.

Тероризам како термин не е нов. Потекнува од францускиот јазик во периодот познат како владеење на теророт (1793-94), кога новата влада ги казнувала - обично со смрт - оние луѓе за кои се мислело дека се против Француската револуција.¹ Бил присутен во текот на целата човекова историја, но особен акцент се става на оваа безбедносна проблематика по нападите на кулите близначки во 2001 година во САД. Тогаш, со изјавата на Џорџ В. Буш била објавена војна против тероризмот и така тој се искачува на прво место од листата приоритети во многу држави во светот.

Во последните децении, терористичките закани еволуираат во чекор со технолошкиот напредок, при што вештачката интелигенција (ВИ) игра сè поголема улога – и како алатка за превенција и борба против тероризмот, но и како потенцијално средство што може да биде злоупотребено од терористички групи.

¹ Merriam-Webster (2024), „The History of the Word 'Terrorism‘“, Merriam-Webster, достапно на: [The History of the Word 'Terrorism' | Merriam-Webster](#)

Направени се голем број напори за развивање соодветни механизми за справување со тероризмот, воедно и за негово превенирање. Како еден од тие методи е профилирањето на тероризмот. Целта на профилирањето е да се создаде една слика за лицата кои се повеќе подложни на регрутација во терористички организации, каде што има најголеми шанси да дејствуваат и на кој начин, односно, се фокусира на анализа на географските и психо-социјалните аспекти како темели за креирање профил, со цел превенирање на тероризмот со можност во порана фаза од неговиот развој.

Во услови на сè поголема дигитализација и трансформација на современите безбедносни предизвици, тероризмот станува сè покомплексен, динамичен и тешко предвидлив феномен. Радикализацијата, регрутацијата и планирањето на терористички активности сè почесто се одвиваат во дигиталната сфера – преку социјални мрежи, енкриптирани комуникациски канали и онлајн пропагандни платформи. Како одговор на оваа закана, безбедносните агенции сè повеќе се потпираат на вештачка интелигенција (ВИ) и машинско учење како алатки за профилирање, предикција, и превенција на терористички активности.

Профилирањето иако навидум изгледа како идеално решение од аспект на превенција и рано предупредување, навремени реакции и минимизирање на ризици се поставува прашањето колку тој метод е прецизен, дали вреди да се вложуваат средства на тоа поле и кој е степенот на успех? Сепак станува збор за човечка категорија како предмет на анализа која до денес е дискутабилна, и се однесува за непредвидливи начини на однесување и дејствување и според повеќе извори и истражувања кои се наведени во трудот, научната фела е поделена во однос на неговиот перформанс и вредноста за тоа дали треба да се инвестира во профилирањето.

Во ваков контекст, профилирањето станува критичен инструмент за рано идентификување на модели на однесување, ризични фактори и индикатори на радикализација. Со употреба на вештачка интелигенција (ВИ), безбедносните служби имаат можност да анализираат огромни количини податоци, да откријат шаблони и да предвидат потенцијални закани. Сепак, оваа технолошка алатка

отвора и сериозни прашања поврзани со етичноста, транспарентноста и можните злоупотреби при профилирањето – особено кога алгоритмите вршат категоризација врз основа на религија, етничка припадност, идеолошки ставови или социјално однесување.

Истражувањето на можностите за профилирање на тероризам со помош на ВИ е од суштинско значење за индивидуалната и националната безбедност, бидејќи овозможува рано препознавање на ризични појави, поефикасна превенција на терористички активности и зајакнување на отпорноста во општеството.

1.2 Дефинирање на предметот на истражување

Несомнено, развојот на технологијата придонесува за олеснување, но истовремено и за отежнување на работата на институциите и организациите засегнати со безбедноста и политиката. Процесот на модернизација ја испраќа пораката-ако вие не сте информирани за најновиот изум, тоа не значи дека и непријателот исто така не е запознаен, (во овој случај терористичките организации и поединци). Доколку сакате да дадете соодветен одговор на некое безбедносно прашање, вие мора прво да разбирате од каде доаѓа заканата и како таа се манифестира. Повеќе не важат истите правила и класични видувања за тоа како се разрешуваат заканите, тие сега се далеку понепредвидливи, ненадејни, брзи, и значително поопасни и животни загрозувачки, и за да можете да дадете одговор на такво нешто, вие мора да бидете подготвени, во случајов во технолошки аспект.

Поврзаноста на профилирањето и вештачката интелигенција е релативно нова тема на дискусија, минимално зачната како резултат на недостатокот на податоци-општи и емпириски, за тоа како всушност би функционирала вештачката интелигенција во однос на профилирањето, и колкава би била неговата прецизност, но земајќи предвид дека наоѓа широка употреба во сите области, повеќе од веројатно е дека не само што ќе биде употребувана како алатка во безбедноста и поконкретно профилирањето, туку и дека степенот на успех ќе ги надмине очекувањата.

Во ваков контекст се поставува суштинското прашање: Како да се развијат ефективни и етички прифатливи методи за профилирање на терористички закани базирани на алгоритамска анализа, без притоа да се нарушат човековите права и основните слободи?

И покрај потенцијалот на ВИ за брза обработка на податоци, идентификација на обрасци и предиктивна анализа, постои ризик од преголема зависност од технолошки решенија кои можат да продуцираат лажни позитиви, да ги зајакнат предрасудите, или да резултираат со профилирање базирано на етничка, верска или идеолошка припадност. Притоа, недостасува систематска анализа за тоа како алгоритамските пристапи ги дефинираат и моделираат заканите, и дали тие се компатибилни со меѓународното право и стандардите за човекови права.

Оттука произлегува потребата од истражување кое ќе ги опфати:

- ризиците и можностите на ВИ во идентификација и профилирање на терористи,
- етичките и правните импликации од таквите технологии,
- улогата на човечкиот фактор во носењето одлуки засновани на алгоритамска анализа.

Погоре споменавме дека профилирањето е алатка која е контроверзна во однос на степенот на нејзината ефикасност, па оттука ќе се насочиме кон првична теориска анализа на профилирањето, нејзината историја и развој, дефинирање и значењето на поимот, видовите на профилирање, емпириски податоци за степенот на нејзината употреба како и ефикасноста. Подоцна, по анализата на профилирањето како целина, ќе се насочиме кон вештачката интелигенција, нејзината појава и влијание во различни сегменти, меѓу кои и безбедноста и начинот на поврзување со профилирањето.

1.3 Досегашни истражувања

При истражувачкиот процес за досегашните истражувања на оваа тема, земајќи предвид дека е доста комплексна тема која воедно е и нова, воочив дека има обемен материјал за тероризмот, профилирањето, вештачката интелигенција, меѓутоа има и лимитирани трудови кои ги опфаќаат сите три теми. Поради ова, првично се насочив кон трудови кои се објавени за поврзаноста на вештачката интелигенција со тероризмот, а потоа ќе ги прикажам делата кои се конкретно насочени кон профилирање на тероризмот и поврзаноста со вештачката интелигенција.

Согласно досегашното истражување има сериозен недостаток од трудови во Македонија на темите за вештачка интелигенција и профилирање на тероризмот, како и меѓусебната поврзаност на овие две теми. Вештачката интелигенција секако е актуелна и покрај овој недостаток, па сепак има зачетоци во делата од оваа област. Оттука, релевантен за оваа тема е трудот кој е насловен: „Потенцијална експлоатација на генеративна вештачка интелигенција од терористи и насилни екстремисти“² од проф. д-р Тања Милошевска каде што разгледува како терористичките организации ги злоупотребуваат алатките како што се ChatGPT, и кои се потенцијалните закани кои произлегуваат од таа експлоатација на онлајн ресурси кои впрочем се достапни за сите.

Англиската литература е далеку побогата со истражувања за вештачката интелигенција, но и покрај тоа делата насочени кон бенефитите за употреба на вештачка интелигенција во областа на профилирањето се исто така со ограничен број.

Свеста за потенцијалниот ризик кој произлегува од тоа вештачката интелигенција да падне во погрешни раце се воочува во делото „Генеративна

² Тања Милошевска (2024), „Потенцијална експлоатација на генеративна вештачка интелигенција од терористи и насилни екстремисти“, *Годишен зборник*, Филозофски факултет, достапно на: <https://journals.ukim.mk/index.php/godzbo/article/download/2780/2396/>

вештачка интелигенција и онлајн екстремизам“³ од Глобалниот интернет форум за борба против тероризмот (GIFCT). Нивниот извештај истражува како генеративната вештачка интелигенција, како што се големите јазични модели и алатките за генерирање слики може да се злоупотреби за екстремистички цели, вклучително и пропаганда, регрутирање и развој на малициозен софтвер.

Центарот за борба против тероризмот на Обединетите нации (UNCCT) и Институтот за истражување на меѓурегионалниот криминал и правда на Обединетите нации (UNICRI), соработувале за да ја објават книгата „Справување со тероризмот преку интернет со употреба на вештачка интелигенција“⁴. Во книгата вниманието е насочено кон Јужна и Југоисточна Азија, каде се бележи брз раст и развој во дигитална смисла, особено кај младите што ги прави поранливи на терористичка пропаганда и регрутирање преку социјалните медиуми.

Илијан Кузманов во декември 2024 година ја разгледува потенцијалната полза од вештачката интелигенција во „Вештачка интелигенција и психолошко профилирање за проценка на ризик од насилство: Подобрување на точноста и справување со етичкиот предизвик“⁵. Вештачката интелигенција во борбата против тероризмот може да го детектира процесот на интернет-радикализација преку анализа на објави на социјалните медиуми и екстремистички мрежи, но мора да се решат прашањата поврзани со приватноста и транспарентноста. Според студијата, вештачката интелигенција може да помогне и во психолошкото профилирање преку анализа на активностите на социјалните медиуми и анализа на однесувањето на корисниците на истите со цел да се подобрат предвидувањата за ризик од насилство. Но, исто така кога се зборува за психолошко профилирање со или без употреба на вештачка интелигенција, етичките предизвици како што се

³ GIFCT Red Team Working Group (2023), „Considerations of the Impacts of Generative AI on Online Terrorism and Extremism“, Global Internet Forum to Counter Terrorism, достапно на: [Considerations of the Impacts of Generative AI on .pdf](#)

⁴ United Nations Office of Counter-Terrorism (2021), „Countering Terrorism Online with Artificial Intelligence“, достапно на: [Countering Terrorism Online with Artificial Intelligence | UNICRI: United Nations Interregional Crime and Justice Research Institute](#)

⁵ Iliyan Kuzmanov (2024), „AI and Psychological Profiling for Violence Risk Assessment: Enhancing Accuracy and Addressing Ethical Challenges“, достапно на: [\(PDF\) AI and Psychological Profiling for Violence Risk Assessment: Enhancing Accuracy and Addressing Ethical Challenges](#)

пристрасноста и загриженоста за приватноста и заштитата на податоци и понатаму претставуваат тема која не смее да биде занемарена.

Употребата на вештачката интелигенција во кој било домен може да претставува сериозно олеснување на работата и овозможување за побрзо реагирање и анализа на податоци, што доведува до процентуално намалување на степенот на правење грешки во проценката, како и зголемување на шансите за превенција, наспроти санирање на штетата. Секако не треба да се заборават и негативните аспекти како кражба на податоци, хакерски напади, и злоупотреба на овие системи. Вештачката интелигенција не е ниту лоша ниту добра како што ја перцепираме ние во зависност од тоа кој ја употребува и за која цел.

Заклучокот од гореспоменатата стручна литература е дека истата претставува чекор во вистинскиот правец, но доколку сакаме да бидеме во чекор со вештачката интелигенција, мораме да ја проучуваме далеку повеќе од ова до сега. Оттука произлегува и потребата на овој труд да го образложи потенцијалниот бенефит од вештачката интелигенција во областа на терористичкото профилирање, како и ризиците и недостатоците од истата.

1.4 Цели и задачи

Општата цел на овој истражувачки труд е да се истражи потенцијалот за употреба на вештачка интелигенција во профилирањето на тероризмот. Така ќе се анализира не само степенот на успех и бенефит од употреба на софистицирана технологија во борбата против тероризмот, туку и негативните аспекти и ќе се даде една сеопфатна слика за вештачката интелигенција.

Во однос на посебните цели, овој труд ќе се насочи кон тоа да даде одговор на уште неколку прашања, односно:

- Одредување на степенот на ефикасност на вештачката интелигенција во профилирањето на тероризмот;

- Во кои видови на профилирање би било најпрактично да се воведат вештачката интелигенција;
- Ризици кои произлегуваат од инкорпорирање на вештачката интелигенција во профилирањето;
- Доаѓање до заклучок за тоа како може да се користи вештачката интелигенција за предвидување на терористички напади како и детекција на различни модели на однесување и нивната корелација со потенцијален сторител на терористички напад;
- Проценка како алгоритмите за машинско учење можат да ја подобрат точноста на идентификувањето на потенцијалните закани, а воедно да ги минимизираат лажните потенцијални траги;
- Да се одредат предизвиците на профилирањето управувано од вештачката интелигенција, вклучувајќи ги пристрасностите во податоците, загриженоста за приватноста и импликациите врз човековите права;
- Испитување како вештачката интелигенција може да им помогне на безбедносните агенции во ефикасна обработка на големи количини податоци за да се спречат терористички напади;
- Анализа на спремноста на безбедносните институции и агенции во однос на потенцијалната имплементација на вештачката интелигенција во доменот на профилирањето;
- Преглед на примери од реалниот свет каде што вештачката интелигенција е успешно или неуспешно имплементирана во антитерористички операции;
- Истакнување на ограничувањата, ризиците и потенцијалната злоупотреба на вештачката интелигенција при профилирање на поединци за активности поврзани со тероризам;
- Воочување на улогата на вештачката интелигенција и нејзината поврзаност со други безбедносни алатки како што се биометриска верификација и анализа на сајбер закани;

Врз основа на овие општи и посебни цели, **задачите** се следните:

- Истражување на системи засновани на вештачка интелигенција конкретно во борбата против тероризмот кои веќе се употребуваат во пракса кој е нивниот процентуален успех или неуспех;
- Анализирање како вештачката интелигенција со цел идентификување на шеми во терористичките активности преку анализа на податоци, препознавање на лица и моделирање на однесувањето;
- Анализа на улогата на вештачката интелигенција во борбата против тероризмот;
- Проценување на степенот на точност и ефикасноста на алгоритмите на вештачката интелигенција во препознавањето на заканите, а воедно минимизирање на лажните позитиви;
- Истражување за тоа како моделите на вештачката интелигенција можат ненамерно да ги зајакнат пристрасностите или да ја нарушат приватноста;
- Истражување на податоци за степенот на прифаќање на вештачката интелигенција од страна на општата популација како неопходен услов за интеграција на вештачка интелигенција во заштитата на луѓето;
- Дефинирање на најновите достигнувања во профилирањето со помош на вештачка интелигенција на напорите за борба против тероризмот;
- Да се идентификуваат потенцијалните ризици и закани кои произлегуваат од вметнувањето на вештачката интелигенција во процесот на профилирање на тероризмот.

1.5 Дефинирање на основните поими

⇒ **Тероризам**

Тероризмот е термин кој нема една конкретна дефиниција и ова е потврдено од страна на авторите Едвин Бакер и Жанин де Рој ван Зуијдевајн кои го нагласуваат субјективниот и политички чувствителен карактер на тероризмот, тврдејќи дека неговото дефинирање е тешко поради неговата еволутивна природа

и влијание врз општеството.⁶ Сепак, за потребите на овој труд ќе ја разгледаме дефиницијата на проф. Алекс П. Шмид, според кој „тероризмот е метод на повторувачко насилно дејствување што предизвикува вознемиреност, кој го користат (полу) тајни поединци, групи или државни актери, од идиосинкратични, криминални или политички причини, при што - за разлика од атентатот - директните цели на насилството не се главните цели.“⁷

⇒ **Радикализација**

Согласно толкувањето на македонскиот речник, радикализацијата значи дека нешто „излегува од контрола“⁸, односно претставува еден вид пречекорување на границите кои може да бидат културолошки, политички, социјални и сл. Во контекст на тероризмот, процесот на радикализација значи прифаќање нови сфаќања во политичка и/или, религиозна смисла како еден вид оправудвање за делата кои терористите ги реализираат. За самите идеи и сфаќања тоа се погледи кои неретко вклучуваат насилство и екстремни убедувања.

⇒ **Сајбер-тероризам**

Со развојот на технологиите се проширува и опсегот на тероризмот и настанува промената на тоа како дејствуваат терористите. Нападите сега, не само што ги реализираат во реалниот свет преку напади на критична инфраструктура како институции и транспортни системи, туку и во виртуелниот свет. Ајоаде Онирети го дефинира сајбер тероризмот како софистицирана форма на тероризам што ги замени традиционалните методи како што се земањето заложници и самоубиствените бомбашки напади. Тој вклучува сајбер напади насочени кон

⁶ Edwin Bakker, Jeanine de Roy van Zuijdewijn (2022), „Definition and nature of terrorism“, Amsterdam University Press, достапно на: [Definition and nature of terrorism \(Chapter 1\) - Terrorism and Counterterrorism Studies](#)

⁷ Alex P. Schmid (2023), „Defining Terrorism“, ICCT Report, достапно на: [Schmidt - Defining Terrorism 1.pdf](#)

⁸ Дигитален речник на македонски јазик (2025), „Радикализација“, достапно на: [радикализација - резултати од пребарување | Дигитален речник на македонскиот јазик](#)

држави, корпорации и поединци, честопати со значителен деструктивен потенцијал.⁹

⇒ Профилирање на тероризмот

Според Европската Унија и нејзината „Нацрт Препорака на Советот за развој на терористички профили“ од 2002 година, „Тероризмот“ е една од најголемите опасности за отвореното и демократско општество на Европската унија. Борбата против тероризмот е високо приоритетна цел на Европската унија, која треба да се спроведе преку координирани мултидисциплинарни напори, што е компатибилно со почитувањето на основните права.“¹⁰ Понатаму, во овој документ се споменува дефинирањето на терористичкото профилирање каде јасно стои дека „Развивањето терористички профили значи составување на збир од физички, психолошки, или бихејвиорални варијабли, кои се идентификувани како типични за лица вклучени во терористички активности и кои може да имаат одредена предвидувачка вредност во тој поглед.“¹¹

⇒ Вештачка интелигенција

Вештачката интелигенција или ВИ е особено актуелна тема и навидум сите ја разбираме, но има недостаток на конкретна дефиниција за тоа каде се нејзините граници и што значи всушност поимот „вештачка интелигенција“. Сепак, за неа може да се каже дека „ Вештачката интелигенција (ВИ) се однесува на развој на компјутерски системи способни да извршуваат задачи кои традиционално бараат човечка интелигенција. Овие задачи вклучуваат расудување, решавање проблеми, учење, перцепција, разбирање на јазикот и донесување одлуки. ВИ може да се категоризира во различни типови, како што се машинско учење, длабоко учење и невронски мрежи, кои им овозможуваат на компјутерите да анализираат податоци, да препознаваат шеми и да прават предвидувања. Истражувачите продолжуваат да

⁹ Ayoade Onireti (2024), „Cyber-Terrorism: An Appraisal of the Dimensions of the New Face of Terrorism in a Post-9/11 Period“, достапно на: [Cyber-Terrorism: An Appraisal of the Dimensions of the New Face of Terrorism in a Post-9/11 Period | IntechOpen](#)

¹⁰ Council of the European Union, (2002), „Draft Council Recommendation on the development of terrorist profiles“, Doc. 11858/3/02 REV 3, Достапно на: [Microsoft Word - 11858-r3en2.doc \(europa.eu\)](#)

¹¹ Исто

ги усовршуваат можностите на ВИ, поместувајќи ги границите на она што машините можат да го прават.¹²

⇒ **Механичко учење (machine learning) и алгоритми**

Овие два поими се дефинираат заедно бидејќи се меѓусебно испреплетени. Механичкото учење, согласно дефиницијата на Станфорд е: „ наука за натерување на компјутерите да дејствуваат без да бидат експлицитно програмирани“¹³ да го сторат тоа. Механичкото учење се имплементира со помош на алгоритми, односно „алгоритмот може да се дефинира како чекор-по-чекор процес, или формула за решавање проблеми, или може да се каже дека е збир на инструкции формулирани за извршување на одредена работа. Значи, најдобар пример за ова е рецепт бидејќи објаснува што мора да се изврши, чекор по чекор“.¹⁴ Алгоритмите и процесот на механичко учење се далеку покомплексни од наведеното објаснување, но за потребите на овој труд доволно е да се запознаеме со нивното основно значење.

1.6 Основна хипотетичка рамка

Тероризмот е закана која не е нова и веќе се поставени механизми за справување со истата. Меѓутоа, согласно промените кои се настанати со особено забрзано темпо во периодот 2015-2025, развојот на вештачката интелигенција и нејзиното влегување во општа употреба и можноста да се користи од кој било, каде било, и притоа бесплатно, отвора многу врати од можности за сите луѓе, и тоа ги вклучува и терористите и институциите кои се борат против тероризмот. Тоа значи дека како што се развива ВИ така се развива и тероризмот, преминувајќи во хибридна закана која се испреплетува со сајбер заканите и на тој начин настанува сајбер-тероризмот.

¹² Дефиницијата за вештачка интелигенција беше напишана од страна на ВИ без никаква ургенција од страна на авторот, освен дадени инструкции за генерирање на истата. Дефиницијата е дадена од страна на Copilot, ВИ креирана од Microsoft.

¹³ Stanford University (2011), „Machine Learning“, достапно на: [Machine Learning - Stanford University](#)

¹⁴ Riya Kumari (2020), „What is an Algorithm? Types, Applications, and Characteristics“, Analytics Steps (online), достапно на: [What is an Algorithm? Types, Applications, and Characteristics | Analytics Steps](#)

Од друга страна, ги споменав институциите кои доколку сакаат да се справат со хибридна закана мора да развијат хибридни/нови методи, и да ја вклучат ВИ во нивната работа и тоа го вклучува профилирањето на тероризмот.

Оттука, општата хипотеза во ова истражување е следната: Употребата на вештачка интелигенција значително го зголемува капацитетот за профилирање и превенција на терористички активности. Согласно истражувањата, профилирањето на тероризмот подлежи на критики бидејќи не може секогаш во која било ситуација, да се применат сите различни видови профилирање и да бидат стопроцентно прецизни, зашто постои можност за дискриминација, но и знае да биде сериозен трошок во финансиска смисла и во контекст на човечки капацитети. Но, со воведувањето на ВИ во процесот може значително да се зголеми прецизноста, да се намали трошокот, и времето за реакција да биде далеку поефикасно.

Помошни хипотези:

1. Вештачката интелигенција овозможува побрзо и поефикасно детектирање екстремистички содржини на социјалните медиуми, и онлајн платформите.
2. Предиктивните модели базирани на вештачка интелигенција можат да идентификуваат ризични поединци или групи, пред да се случи терористички акт.
3. Алгоритмите за обработка на големи податоци (big data) помагаат во препознавање на поврзаности меѓу радикализирани индивидуи и терористички мрежи.
4. Системите базирани на ВИ честопати се подложни на алгоритамска пристрасност што може да резултира со лажно позитивни идентификации.
5. Недостатокот од транспарентност во алгоритамските процеси го намалува јавниот надзор и може да доведе до злоупотреба на овластувањата.
6. Ефикасната примена на вештачката интелигенција бара постојана човечка контрола, правна регулатива и етички надзор.

7. Успешното интегрирање на ВИ во борбата против тероризмот зависи од интероперабилноста меѓу националните и меѓународните безбедносни институции.

1.7 Научна и општествена оправданост

Научната оправданост за ова истражување е во тоа што како прво, постои сериозен недостаток на трудови од областа на тероризмот во Македонија, а второ, има недостаток на научни истражувања во доменот на вештачката интелигенција во Македонија, и трето, во светот има ограничена стручна литература која се занимава конкретно со можностите од инкорпорирање на вештачката интелигенција во терористичкото профилирање.

ВИ е алатка која е достапна за сите насекаде, и нејзините граници се речиси бесконечни и нејзиниот потенцијал не само што треба да се воочи, туку треба и да се искористи. Терористите веќе забележаа која е ползата од употреба на ВИ во нивното дејствување во сајбер просторот, ширењето пропаганден материјал и екстремистичка идеологија. Доколку институциите сакаат да дадат соодветен одговор на оваа закана и идеално да ја превенираат, неопходно е да ја вметнат ВИ во нивните стратегии. За таа цел, потребни се студии како оваа, кои ќе дадат одговор за ефикасноста на ВИ во профилирањето на тероризмот, предностите и недостатоците.

Општествената оправданост е дека тероризмот е закана која потенцијално може да погоди кој било од нас како директно така и индиректно. Секој може да најде на пропагандни видеа, слики и текстови кои се генерирани со помош на ВИ, некои можат да бидат радикализирани како резултат на истите, или пак да го мотивираат да преземе некој чекор во реалниот свет. Живееме во ера на технолошки развој со забрзано темпо, време кога секој со секого е поврзан, и сајбер-тероризмот како хибридна закана може да направи сериозна штета во виртуелниот и физичкиот свет. Дополнително, со растечкото присуство на младите во дигиталниот простор, ризикот од онлајн радикализација и влијание од

екстремистички содржини значително се зголемува. Оттука, потребата од нови, научно поткрепени, но и општествено одговорни алатки за анализа, профилирање и интервенција станува приоритет не само за безбедносните структури, туку и за образовните институции, медиумите и граѓанскиот сектор.

Институциите треба да ја воведат ВИ за да дадат одговор на хибридните закани и овој труд може да помогне во овој процес.

1.8 Методи и техники на истражувањето

Со цел обезбедување релевантни податоци за потребите на ова истражување ќе употребувам неколку научно-истражувачки методи и тоа:

- **Квалитативна методологија** - овој истражувачки метод ќе биде воглавно насочен кон текстуална анализа на веќе постоечка стручна литература, поконкретно на теми како што се сајбер-тероризам, вештачка интелигенција и поврзаноста на профилирањето со ВИ;
- **Квантитативна методологија** – таа се состои од неколку аспекти, и тоа: анализа на статистички податоци, резултати од наоди, анкети, тестирања и други видови нумерички податоци кои се релевантни за ова истражување;
- **Компарација** – по прибирање на соодветните квалитативни и квантитативни податоци, истите треба меѓусебно да се споредат и анализираат за да се дојде до одговор на веќе поставените хипотези;
- **Студии на случај** – тие се особено корисни при објаснување на практичната примена на вештачката интелигенција, односно тие можат да ни доловат како ВИ се употребува во други сфери од науката и каков ефект може да има нејзината имплементација во безбедноста. Методологијата на студија на случај се состои од неколку чекори и тоа: Разбирање на целите, повеќекратно читање на студијата на случај, идентификување на клучните теми и шеми, анализа на податоците, евалуација на силните страни и ограничувањата,

извлекување заклучоци и давање препораки и документирање и презентирање на анализата¹⁵.

2. ТЕРОРИЗАМ

Тероризмот денес се сфаќа како една од најсериозните закани на 21 век. Но, важно е да се напомене дека не претставува нова закана со која се соочува светот. Имено, станува збор за насилен чин/ови кои се присутни од поодамна, меѓутоа начинот на кој делуваат терористите е поинаков. Благодарение на глобализацијата, терористичките акти кои во минатото би се случиле само во една држава, денес може да имаат импликации врз соседните земји и пошироко. Ова се реализира преку социјалните мрежи каде терористите можат во живо да ги пренесуваат своите напади, и на овој начин покрај ширење општа паника кај обичното население, ја шират и нивната идеологија. Понатаму, преку брзиот развој на технологијата таа станува сè подостапна не само за нас, туку и за терористите и преку неа може да реализираат хакерски напади со кои може да се таргетираат повеќе од една држава, и секако технолошкиот развој во областа на вооружувањето им овозможува пософистицирано оружје за реализирање на нападите.

Покрај добро познатите терористички организации како што се Ал Каеда и ИСИС, се појавува нова бранша која произлегува од теороризмот – волци-самотници. Терминот „волк-самотник“ во контекст на тероризмот, започнал да се употребува во периодот на 80-тите години¹⁶ и како најсеопфатна дефиниција за тоа што се волци самотници се наведува во теоријата на Спааци. Тој го дефинира овој вид тероризам преку анализа на оној кој го применува. Терористот-осамен волк има три главни карактеристики: тој дејствува индивидуално, не припаѓа на организирана терористичка група или мрежа, неговиот начин на работа е замислен и раководен од поединец без никаква директна надворешна команда, или

¹⁵ California Learning Resource Network Team (2024), „How do You analyze a case study?“, CLRN (online), достапно на: [How do You analyze a case study? - California Learning Resource Network](#)

¹⁶ Amber Pariona (2017), „What Is Lone Wolf Terrorism“, WorldAtlas (online), достапно на: <https://www.worldatlas.com/articles/what-is-lone-wolf-terrorism.html>

хиерархија.¹⁷ Волците-самотници се опасни поради тоа што делуваат сами и може да нападнат кога и каде било и се непредвидливи, па поради нивната неповрзаност со поголема организација сами си набавуваат сè што им е потребно за да извршат терористички чин, односно напредокот на технологијата им овозможува сè што им е потребно, на пример да си купат онлајн, да ја шират нивната идеологија, и онлајн да запознаваат луѓе слични на нив, и секако да извршуваат онлајн напади.

Анализата на тероризмот, од нејзините рани зачетоци па се до денес е неопходна со цел да се долови важноста на профилирањето на тероризмот и понатамошната негова поврзаност со вештчката интелигенција. Од тие причини ќе ја разгледаме дефиницијата на тероризмот, неговиот историски развој, трендови, мотиви, методи и сл.

2.1 Дефинирање

Поимот тероризам е еден од најкомплексните кога станува збор за давање една конкретна дефиниција за него во современиот дискурс. Тоа воглавно се должи на недостигот на консензус од страна на светската стручна фела. И покрај ова, тероризмот ја обликува надворешната политика и често се појавува на вести, социјални медиуми, терминот го слушаме во секојдневието, но сè уште постои доза на несигурност за неговото значење и тежина. За да се разбере тероризмот, мора да се разгледаат неговите јазични корени и неговата долга историја.

Предизвикот во дефинирање на тероризмот лежи во неговата субјективна природа. Покрај ова, вклучени се и дискусиите за мотивите на терористите, методите кои ги употребуваат итн. Според дефиницијата на Речникот на Оксфорд, тероризмот се дефинира како: „Незаконска употреба на насилство и заплашување, особено против цивили, во остварувањето на политички цели“.¹⁸ Оваа дефиниција нагласува три клучни компоненти: противзаконитост, таргетирање цивили и

¹⁷ Iskren Ivanov (2016), „Lone Wolf Terrorism: Nature, History and Motivation“, Academia (online), достапно на: [Lone Wolf Terrorism Nature History and M.pdf](#)

¹⁸ Oxford (2026), „Terrorism noun-definition, pictures, pronunciation and usage notes“, OxfordLearnersDictionaries.com (online), Достапно на: [terrorism noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com](#)

политички мотив. Таа сугерира дека тероризмот не е само случајно насилство, туку пресметана алатка која се користи за постигнување одредена цел.

Федералното биро за истраги (FBI) дава малку поинаква слика за тероризмот. Тие прават поделба помеѓу она што значи домашен и интернационален тероризам. Така за домашни се сметаат оние кои се „Насилни, кривични дела извршени од поединци и/или групи за унапредување на идеолошките цели што произлегуваат од домашни влијанија, како оние од политичка, религиозна, социјална, расна или еколошка природа“. Од друга страна, интернационални се: „Насилни, кривични дела извршени од поединци и/или групи кои се инспирирани, или поврзани со назначени странски терористички организации или нации (спонзорирани од државата).“¹⁹

Клучна разлика помеѓу двете дефиниции е тоа што во втората вклучува поделба помеѓу оние кои се домашни терористи и меѓународни терористи врз основа на нивната идеологија и начинот на кој дејствуваат.

Согласно овие дефиниции, можеме да констатираме дека тероризмот значи примена на дејствија кои можат да имаат религиозни, политички и други мотиви, кои нанесуваат штета врз психо-физичката благосостојба на жртвите, како и штета врз критична инфраструктура и имот во име на реализирање на некаква цел.

Во стручната литература може да се пронајдат дефиниции кои се опширни, кои се конкретни, кои земаат предвид различни аспекти, и се воочува дека тероризмот претставува тема која постојано еволуира, и нејзиното дефинирање треба и бара постојано да се надополнува доколку сакаме да биде во чекор со самиот развој на овој комплексен поим. Суштината на самиот тероризам е нанесувањето на штетата-физичка и психолошка, меѓутоа во модерниот свет во кој се јавува вештачката интелигенција како нова алатка, се истакнува и заканата од сајбер-тероризам како нова причина за измена на дефинициите за тероризмот кои ги познаваме денес.

¹⁹ FBI (2026), „Terrorism“, Достапно на: [Terrorism – FBI](#)

2.2 Историски развој

Историјата на тероризмот не е линеарна прогресија на насилство, туку променлив пејзаж на политичка стратегија, теолошки убедувања и психолошка војна што еволуирала заедно со структурите на моќ што се обидува да ги оспори. Иако терминот „тероризам“ е релативно модерна лингвистичка конструкција, практиката од користење симболично насилство за постигнување политички или социјални цели ги наоѓа своите корени во антиката.

Најраните претходници на современите терористички организации се Сикарите. Тие биле еврејска екстремистичка група која била активна во првиот век од нашата ера, за време на римската окупација на Јудеја. Според римско-еврејскиот историчар Флавиј Јосиф, Сикарите го добиле своето име од сиката, мал закривен нож кој го криеле под облеката за да реализираат атентати над римски службеници и еврејски соработници на угледни позиции во власта. Ричард А. Хорсли во својата студија „Сикариите: Антички еврејски „терористи“, нивната цел не била само да убиваат, туку да создадат чувство на страв што би ја принудило римската администрација да се повлече, а еврејското население да се радикализира. Со реализирање напади за време на фестивали и во текот на секојдневието, Сикарите го искористиле психолошкото влијание на непредвидливото насилство.²⁰

Речиси еден милениум подоцна, на Блискиот Исток во средниот век, се појавила сектата Низари Исмаили, позната на Запад како Асасини или Хашашин. Тие дејствувале од крајот на 11-ти до средината на 13-ти век, и оваа група извршувала убиства на политички и воени водачи за да ја зачува својата автономија против Селџукската империја и крстоносците. Фархад Дафтари објаснува во неговото дело: „Легендите за атентаторите: Митот за Исмаилите“, дека атентаторите ги гледале своите мисии како форма на „света должност“, каде што смртта на оперативецот често била очекувана и прифатена, најавувајќи ги религиозните императиви и саможртвуваните тактики на современите екстремистички движења. За ваквите лица бил употребуван терминот „фидаи“ што

²⁰ Horsley, R. A. (1979). The Sicarii: Ancient Jewish "Terrorists". The Journal of Religion, Достапно на: [The Sicarii: Ancient Jewish "Terrorists" on JSTOR](#)

во превод значело „оној кој го нуди својот живот како жртва“ или „оној кој е подготвен да го жртвува својот живот во име на каузата“²¹ Овој вид саможртвуваност во име на некоја цел е истиот наратив кој се употребува денес во споделуваните доктрини од терористичките групи според кои доколку лицето изврши напад и при тој напад го жртвува својот живот за каузата, истиот ќе биде награден така што ќе оди во рајот и ќе го пречекаат 72 девици.

Модерните зачетоци на тероризмот се во периодот на Француската револуција. За разлика од поддржавните актери од антиката, режимот на теророт (1793–1794) бил период на терор спонзориран од државата, дизајниран да ја заштити државата од внатрешни непријатели. Максимилијан Робеспјер го оправдал ова насилство со тоа што навел дека „теророт не е ништо друго освен правда, брза, строга, нефлексибилна“. Овој период се дефинира и како пресвртница во историјата на тероризмот, каде што „теророт“ бил институционализиран како алатка на владата. Подоцна во 19 век, сфаќањата за теророт од тоа дека таа е алатка на државата, преминале во термин кој се користи за да се опишат оние кои користат терор против државата.

Транзицијата кон модерната ера на тероризмот најдобро се анализира преку теоријата на Дејвид Ц. Рапопорт во неговата влијателна студија „Четири бранови на современ тероризам“ од 2004 година. Во ова дело Рапопорт тврди дека современиот тероризам се движел низ различни циклуси, почнувајќи со **анархистичкиот бран** од 1880-тите. Во овој период групи како руската Народнаја Воља (Народна волја) биле пионери во „пропагандата со „дела“, користејќи новоизмислен динамит за да ги таргетираат монарсите и високите функционери со цел да предизвикаат глобална револуција. Потоа следел **Антиколонијалниот бран** (1920-ти-1960-ти), каде што движењата во Алжир, Кипар и Израел го користеле тероризмот како тактичка алатка за да добијат национална независност. Кон крајот на 20-от век бил **Новиот левичарски бран**,

²¹Daftary, F. (1994), „*The Assassin Legends: Myths of the Isma'ilis*. I.B. Tauris“, Достапно на: [TheAssassinLegends. Myths of the Isma'ilis. By Farhad Daftary. pp. VIII, 213, front.London, I. B. Tauris, 1994..£39.50. | Journal of the Royal Asiatic Society | Cambridge Core](#)

карактеризиран од марксистичко-ленинистички групи како Фракцијата на Црвената армија и Црвените бригади, кои се вклучија во интернационализиран тероризам како што се серија киднапирања. Конечно, **Религиозниот бран**, кој започнал во 1979 година со Иранската револуција и советската инвазија на Авганистан, кој го пренасочил фокусот од секуларните идеологии на трансценденталните императиви. Брус Хофман нагласува дека овој четврти бран е особено опасен затоа што „религиозниот терорист“ го гледа насилството како сакраментален чин, а не како политичко преговарање, што доведува до повисоки стапки на жртви и отфрлање на традиционалниот политички компромис.²²

Историјата на тероризмот е долга и сложена тема која неретко оддава впечаток дека не може да се најде ниту нејзиниот почеток, а уште помалку веројатно, нејзиниот крај. Она кое може со сигурност да се каже е дека тероризмот тогаш и денес има големи сличности, тргнувајќи од мотивот кој стои зад чинот, верувањата за нужната смрт на сторителот и наградата која следува. Тероризмот бил сериозна закана уште од самите почетоци, предизвикувал страв, паника и сериозна штета, и како таков го познаваме се до денес, со тоа што во оваа современа доба преплавена со технолошки усовршувања, теористите имаат пристап до интернет, социјални медиуми, вештачка интелигенција, и се она што им овозможува да се надоградуваат и да бидат сè подобри во она што го прават.

2.3 Типологија

Тероризмот е појава која тешко се дефинира и консензус околу поимовното определување сè уште не е постигнат. Истото може да се каже и за неговата поделба во определени категории која може да помогне при негова анализа, истражување, разоткривање и гонење. Постојат повеќе поделби и врз основа на различни категории, секоја со своја тежина и улога, кои им помагаат на службените лица кои

²² David Charles Rapoport (2004), „The four waves of modern terror: International dimensions and consequences“, researchgate.net (online), Достапно на: [\(PDF\) The four waves of modern terror: International dimensions and consequences](#)

го извршуваат профилирањето при процесот на изготвување на профилите на личност.

Анализирањето на тероризмот во академската и стручна литература може да се движи од психолошки профили до сложени, повеќеслојни класификации кои вклучуваат идеологија, стратешки цели и политички убедувања и социо-економска состојба. За да се анализираат различните видови терористи, истражувачите се насочуваат кон нините организациски врски, историските „бранови“ во кои функционираат и специфичните идеолошки или патолошки мотивации што ги поттикнуваат нивните дејствија.

Најпознатата поделба врз основа на историскиот развој на тероризмот е онаа на Дејвид Ц. Рапопорт во неговата студија „Четири бранови на современ тероризам“ од 2004 година. Во неа, Рапопорт, дава поделба на тероризмот според развојот и промените кој тој ги доживува со текот на времето. Оттука, постојат четири клучни поделби, и тоа:

1. **Анархистичкиот бран** (околу 1880–1920): Првиот бран бил поттикнат од економските и политичките реформи во Русија и последователното разочарување од нискиот степен на реализација. Психолошката цел била да се демонстрира ранливоста на државата преку атентат врз познати лидери. Впечатливо за овој бран е тоа што бил првиот што имал корист од модерната технологија, поточно телеграфот и весниците кои биле широко распространети, дозволувајќи им на идеите и тактиките да се шират на глобално ниво за релативно кратко време. За разлика од подоцнежните бранови, овие актери се обиделе да предизвикаат спонтано масовно востание, наместо да изградат долгорочна политичка партија;
2. **Антиколонијалниот бран** (околу 1920–1960): По Првата светска војна и принципот на „национално самоопределување“ застапуван во Версајскиот мировен договор, овој бран бил насочен кон легитимноста на империјалното владеење. Групи како ИРА (Ирска), ФЛН (Алжир) и Иргун (Мандат Палестина) ги смениле тактиките од атентат врз шефови на држави кон исцрпување на полициските и воените сили. Клучна разлика

- тука е промената во терминологијата; овие актери беа првите што ја отфрлија етикетата „терорист“, претпочитајќи „борец за слобода“;
3. **Нов левичарски бран** (околу 1960–1990): Поттикнат од Виетнамската војна и пошироката борба помеѓу капитализмот и комунизмот во Студената војна, овој бран го означува подемот на „урбаната герила“. Групи како што се Weather Underground (САД) и Фракцијата на Црвената армија (Западна Германија) се сметале себеси за претходница на глобалната револуција против западниот империјализам. Оваа ера ги популаризирала меѓународните инциденти како што се киднапирања на авиони и преземање амбасади. Тука е од особено значење да се истакне дека овој бран е уникатен по своето високо ниво на интернационална соработка, каде што различни групи споделуваа кампови за обука и логистика;
 4. **Религиозниот бран** (1979–денес): Рапортот идентификува три клучни настани во 1979 година кои го катализираат овој сегашен бран: Иранската револуција, почетокот на нов исламски век и советската инвазија на Авганистан. За разлика од секуларните, политички цели на претходните три бранови, „Религиозниот бран“ воведува трансцендентално оправдување за насилството. Целите често се теократски, а не националистички. Овој бран бележи значително зголемување на употребата на самоубиствени бомбашки напади и настани со „масовни жртви“, бидејќи публиката повеќе не е само политичката елита или јавноста, туку божествено битие. Ова поместување често го отежнува преговарањето, бидејќи целите се перцепираат како нешто за кои не може да се преговара.²³

Настрана од историските бранови, научници како Џеролд Пост развил типологија базирана на актери кои се разликуваат меѓу политичкото, криминалното и патолошкото. Тој тврди дека додека криминалните и патолошките терористи може да бидат водени од лична добивка, или тешка психијатриска болест, политичките терористи генерално не се карактеризираат со големи

²³ Исто.

клинички ментални нарушувања. Наместо тоа, политичките терористи често се категоризираат според нивната организациска структура и цели. Националистичко-сепаратистичките терористи на пример, се стремат да воспостават суверена држава за етничка или национална група и често се карактеризираат со висок степен на заедничка поддршка. Спротивно на тоа, социјално-револуционерните терористи (како што е Фракцијата на Црвената армија) обично се воде од желбата за соборување на домашен политички поредок, честопати наоѓајќи се себе си поизолирани од општата популација за која тврдат дека ја претставуваат.²⁴

Фредерик Хакер предложил историски значајна типологија на терористи, категоризирајќи ги во три различни групи: крстоносци, криминалци и луди. Крстоносецот бил воден од по значење поголеми цели, што ги прави особено тешки за одвраќање поради нивната подготвеност да ги жртвуваат своите животи за своите верувања. Спротивно на тоа, Криминалецот користел терористички тактики за лични или материјални придобивки, како што е вклучување во киднапирање за откуп. Лудиот, од друга страна, бил мотивиран од идиосинкратични и честопати во заблуда.²⁵ Типологијата на Хакер, иако датира од 1976 година, продолжува да служи како основна референца во современото профилирање при воспоставување разлика помеѓу рационално-инструменталните и ирационално-експресивните форми на насилство.

Академската литература од центарот СТАРТ на Универзитетот во Мериленд ги разликува терористичките групи врз основа на тоа како тие ја балансираат безбедноста (тајноста) наспроти ефикасноста (смртоносноста). Овие структури не се статични и тие често се развиваат како одговор на притисокот против тероризмот.

Во различна литература се споменува поделбата на терористичките организации според тоа како се тие структурално поставени. Вообичаено овие тези

²⁴ Jerrold M. Post, (2007), „The Mind Of The Terrorist“, Достапно на: [The Mind of the Terrorist: The Psychology of Terrorism from the IRA to al-Qaeda](#)

²⁵ Frederick J. Hacker (1976), „ Crusaders, criminals, crazies : terror and terrorism in our time “, Достапно на: [Crusaders, criminals, crazies : terror and terrorism in our time : Hacker, Frederick J : Free Download, Borrow, and Streaming : Internet Archive](#)

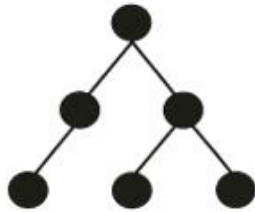
се базираат на иста поделба која е различно именувана или прикажана, но претежно терористичките организации може да се поделат на следниот начин:

- **Хиерархиска (пирамидална) структура:** Вообичаена кај „традиционалните“ групи се одликува со јасен синџир на команда, функционална специјализација како на пример различни единици за логистика, разузнавање и извршување и авторитет од горе надолу. Иако е многу ефикасен за операции во голем обем, меѓутоа неговата слабост лежи во тоа доколку се елиминира раководството. На тој начин може да се сруши целата структура, т.е. таа ќе се распадне поради нејзината зависност од централната координација;
- **Мрежа во облик на звезда:** Во овој модел, централен дел, односно водството на организацијата комуницира со разни ќелии кои остануваат изолирани една од друга. На тој начин, според делото „Глобален тероризам“ од проф. д-р Тања Милошевска, ќелиите се центарот или со главниот организатор, односно преку него мораат да комуницираат и да ги координираат сите свои активности.²⁶ Ова обезбедува повисок степен на безбедност од хиерархијата. Ако една ќелија е компромитирана, членовите не можат да ги предадат другите ќелии бидејќи немаат хоризонтален или било каков контакт една со друга;
- **Мрежна поврзаност:** Карактеризирана со недостаток на централно водство, секоја ќелија во оваа мрежа е поврзана со неколку други. Ова е најотпорната структура бидејќи нема едно, јасно, централизирано водство. Сепак, таа е најмалку ефикасна за сложени операции бидејќи координирањето на напади од големи размери бара високо ниво на комуникација, што го зголемува ризикот од откривање од страна на разузнавачките агенции;
- **Безлидерство:** Ова е најдецентрализираната форма на организација, доколку воопшто може да се нарече организација. Тоа се поединечни актери или мали ќелии кои дејствуваат независно, инспирирани од заедничка кауза,

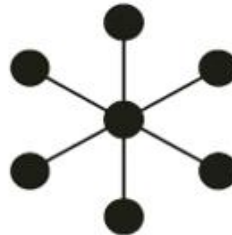
²⁶ Тања Милошевска (2018), „Глобален тероризам“, Скопје-Филозофски факултет, Универзитет „св. Кирил и Методиј“, стр.49.

но без формални командни врски. Ова е примарна динамика на модерните терористички групи.

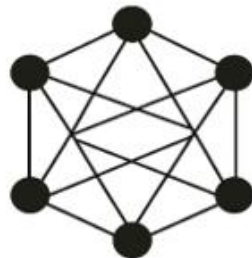
Хиерархиска структура



Мрежа во облик на ѕвезда



Мрежна структура



Безлидерство



Слика 1: Сликвито претставување на видовите на организациска поставеност кај терористичките групи и поединци.

Подоцна, како дополнителна категорија, или дури може да се каже дека е еден вид подкатегија на безлидерството, се јавуваат терористите волци-самотници. Тие дејствуваат сами, може, но не мора да имаат контакт со други терористи, сами планираат и дејствуваат во напади и ширење на нивната идеологија. Во контекст на тероризмот, поимот терористи волци-самотници се појавува во 1980-тите и прв го употребува Луис Бим, член на ККК и Ариевската нација.²⁷

²⁷ Katie Worth (2016), „Lone Wolf Attacks Are Becoming More Common — And More Deadly“, PBS (online), Достапно на: [Lone Wolf Attacks Are Becoming More Common -- And More Deadly | FRONTLINE | PBS | Official Site | Documentary Series](#)

Согласно Теоријата на Рамон Спааиџ терористот волк-самотник има три главни карактеристики:

- Дејствува индивидуално;
- Не припаѓа на организирана терористичка група или мрежа;
- Неговиот начин на работа е замислен и раководен од поединецот без никаква директна надворешна команда или хиерархија.²⁸

Како последна категорија на поделби се оние засновани на идеологијата на терористот или терористичката група/организација. Покласичната и основна типологија се темели на поделбата пвр основа на политичките убедувања, па така тероризмот се дели на крајно левичарски, крајно десничарски и џихад. Идеологијата на лево ориентираните се темели на марксизмот и ленинизмот каде целта е да се воведо социјализам и на крајот да се воспостави комунистичко и бескласно општество. Идеологијата на десно ориентираните волци-самотници се темели на нео-нацизам, антисемитизам, расизам, врховизам, хомофобија и др. Сметаат дека нивните убедувања, како и во сите други случаи впрочем, се најдобри и не треба да постојат други опции и целта им е да создадат еден вид фашистичка држава. На крајот е џихадот, кој потекнува од „Џихад“, исламски термин кој се преведува како „борба“, „стремење“, или „света војна“. Насилните исламски екстремистички групи обично го преведуваат терминот како „света војна“, брендирајќи го зборот како оправдување за вмешување и отпочнување на конфликти. Понатаму, терористичките организации може да се поделени според тоа дали се насочени кон една или повеќе идеолошки цели. Некои групи преферираат да имаат една конкретна цел и да ги насочат сите свои капацитети и ресурси кон неа, додека други се стремат кон тоа да таргетираат повеќе цели одеднаш за да ги распространат капацитетите на противникот на различни места со што потенцијално би нанеле поголема штета.

Типологијата на тероризмот е еден од првите и најважните чекори во процесот на профилирањето, нешто кое дополнително ќе ни се потврди во текот на

²⁸ Ramón Spaaij (2012), „Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention“, SpringerBriefs in Criminology.

ова истражување. Тоа е од енорна важност бидејќи ни дава првична слика за заканата која претстои: дали е хиерархиски поставена или мрежно, дали станува збор за група или волк-самотник, кои се нивните идеолошки цели итн. Сите овие податоци ја разјаснуваат сликата и не носат чекор подалеку во процесот со справување со една од најкомплексните хибридни закани на светско ниво. Типологијата не само што ни помага во текот на истражниот процес, туку асистира и во обидите за превенција на напади, регрутација и ширење на екстремистичка идеологија, што дополнително ја потврдува тезата дека типологијата е еден од најважните процеси во профилирањето.

3. ПРОФИЛИРАЊЕ

3.1 Општо дефинирање на профилирањето

Профилирањето е комплексен поим за кои нема една универзално прифатена дефиниција. Поради тоа, неопходно е анализирање на повеќе дефинирања со цел одредување на два клучни елементи:

- Што е општото дефинирање на поимот профилирање; и
- Која е дефиницијата за профилирањето низ призма на тероризмот.

Оттука, според Англискиот речник на Оксфорд, профилирање е „да се состави или презентира биографски профил на (лице)“ или пак, „евидентирањето или анализата на познатите психолошки, интелектуални и карактеристики на однесувањето на една личност“.²⁹

Според Речникот Мириам–Вебстер, „чинот или процесот на екстраполирање на информации за личност врз основа на познати особини или тенденции или, конкретно, чин на сомневање или таргетирање на лице врз основа на забележани

²⁹ Oxford University Press (2024), „Profiling“, Oxford English Dictionary, Достапно на: [profiling - Quick search results | Oxford English Dictionary \(oed.com\)](https://www.oed.com/search/quick?query=profiling)

карактеристики или однесување³⁰ се смета за профилирање. Нагласено е при нивното дефинирање дека ова поимање е во насока на маркетинг и се однесува на економскиот аспект на профилирањето, меѓутоа има и уште една дефиниција која конкретно е насочена кон безбедносната димензија на профилирањето.

Речникот на Кембриџ пак, го дефинира профилирањето како „активност на собирање информации за некогo, особено за криминалец, со цел да се даде опис на нив“. Кембриџ дава акцент на профилирањето токму во контекст на безбедноста, односно се однесува на криминалното профилирање, кое подоцна ќе видиме дека е тесно поврзано со профилирањето на тероризмот.

При анализата на овие доста различни дефиниции, се забележуваат неколку трендови. Прво, профилирањето е пред сè алатка која се употребува во повеќе сфери. Таа не се јавува единствено во областа на тероризмот, туку се користи во економијата, безбедноста, политиката, здравството, екологијата и сл.

Второ, постои недостаток во дефинирањето каде се нагласува анализата на личноста и сите нејзини аспекти, каде се појавува празнина при анализа на просторот, односно географско профилирање. Ваквите недостатоци може да имаат сериозно негативно влијание, особено при процесот на изработка на криминални и терористички профили. Географските профили се неопходни за одредување на потенцијални цели (мети), критична инфраструктура, како и скривалишта и тајни маршрути кои ги користат терористите и криминалците.

Трето, при акцентирањето на личноста во дефинициите, се нагласува дека треба да се посвети внимание на нивните искуства, тенденции, особини, карактеристики и однесување па врз основа на сите овие параметри да се таргетираат определени лица. Но, ова таргетирање може да оди во две насоки во зависност од тоа кои ги изработува профилите. Ако станува збор за маркетиншка фирма, како што е дефинирањето на Вебстер, тогаш, пример, профилирањето е во насока на избирање соодветен пазар за продукт на некоја компанија. Ако профилот

³⁰ Merriam-Webster (2024), „Profiling“, Merriam-Webster, Достапно на: [Profiling Definition & Meaning - Merriam-Webster](#)

е создаден за криминалци од страна на надлежни органи, тоа е во насока на подобрување на безбедноста и благосостојбата на граѓаните. Меѓутоа, профилот може да се изработува и од терористички организации за да одредат какви лица сакаат да регрутираат или пак, да таргетираат при извршување напад. Поради ова, профилирањето може да биде многу корисна алатка и нејзината важност не смее да се потцени, но истовремено е нож со две острици и колку што може да им помогне на државите, толку може и да им одмогне, доколку оваа алатка ја употребуваат погрешни луѓе или организации.

Поради важноста на профилирањето како алатка во сите аспекти и сфери од општественото живеење, неопходно е воспоставување на една неутрална дефиниција која ќе ги опфати сите потребни аспекти. Оттука, профилирањето може да се дефинира како анализирање на карактеристиките, цртите, искуствата и целокупната личност на еден човек/група или анализа на географскиот простор. Потоа, согласно добиените податоци се изготвува документ кој се нарекува профил. Односно, профилот е слика за човекот или за просторот кој го опкружува. Корисноста на самиот профил е во зависност од оној кој ја употребува оваа алатка.

3.2 Дефинирање на профилирањето низ призма на тероризмот

Во контекст на тероризмот, профилирањето се однесува на процесот на идентификување и анализа на обрасци, однесувања и карактеристики поврзани со поединци или групи вклучени во терористички активности.

Според Европската Унија и нејзината „Нацрт Препорака на Советот за развој на терористички профили“ од 2002 година, „Тероризмот“ е една од најголемите опасности за отвореното и демократско општество на Европската унија. Борбата против тероризмот е високо приоритетна цел на Европската унија, која треба да се спроведе преку координирани мултидисциплинарни напори, што е компатибилно со почитувањето на основните права.“³¹ Понатаму, во овој документ се споменува

³¹ Council of the European Union, (2002), „Draft Council Recommendation on the development of terrorist profiles“, Doc. 11858/3/02 REV 3, достапно на: [Microsoft Word - 11858-r3en2.doc \(europa.eu\)](#)

дефинирањето на терористичкото профилирање, каде јасно стои дека „Развивањето терористички профили значи составување на збир на физички, психолошки или бихејвиорални варијабли, кои се идентификувани, како типични за лица вклучени во терористички активности и кои можат да имаат одредена предвидувачка вредност во тој поглед.“ Целта на овој вид профили била борбата против тероризмот, објавена по настаните во САД од 2001 година. Проектот за создавање терористички профили и прибирање податоци за заеднички особини на терористите има за цел ефикасно и систематски да ги собере информациите на земјите-членки за создавање и примена на профили на терористи.

Така, согласно ова дефинирање, профилирањето во сферата на тероризмот, без оглед дали станува збор за поединци или групи, се однесува на прибирање физички и психолошки карактеристики за сторителите на терористички напади, во име на полесна идна идентификација на терористи.

3.3 Дистинкција помеѓу криминално профилирање и профилирање на тероризмот

Досега при анализата на дефинирањето на профилирањето, воочивме дека постои поврзаност, или еден вид испреплетеност помеѓу терористичкото и криминалното профилирање. Понатаму ќе видиме дека тие ја делат приказната за нивниот развој и исти или слични видови профили се употребуваат наизменично при соочување со која било од овие две закани од областа на безбедноста. Но, иако профилирањето на тероризмот и криминалното профилирање се една те иста алатка во две различни области, сепак постојат разлики во тоа како таа алатка се употребува.

Доколку ги разгледаме целите и главниот фокус на криминалното профилирање, ќе забележиме дека тоа е насочено кон разбирање и предвидување на однесувањето на поединците вклучени во криминални дејствија. Вообичаено е да се применува за случаи како што се сериски убиства, сексуални напади или други насилни злосторства и често се занимава со поединечни кривични дела или низа

поврзани дела. Тоа има за цел да ги идентификува моделите, мотивациите и карактеристиките на престапниците. Од друга страна пак, терористичкото профилирање е насочено кон разбирање и предвидување на однесувањето на поединци или групи вклучени во терористички активности. Разгледува политички, верски и социјални фактори и се применува во случаи поврзани со тероризам, бунт или политички мотивирано насилство. Основната цел на терористичкото профилирање е да открие идеолошки мотивации, организациска поврзаност и потенцијални закани, да спречи напади и да ги разбие терористичките организации.

Преку анализа на сторителите, согласно тоа дали се криминалци или терористи, може да се пронајде разлика помеѓу овие два вида профилирање. Криминалното е насочено кон прекршители на закони кои може да имаат различни мотивации (на пр., лична корист, одмазда, потрага по возбуда и сл.) и се фокусира на психологијата, начинот на работа и виктимологијата на сторителот. Терористичкото профилирање е посветено на мотиви кои се од идеолошка побуда (на пр., политички, религиозни, националистички) и разгледува групна динамика, процеси на радикализација и пропаганда.

Според опсегот, криминалното профилирање има потесен опсег, фокусирајќи се на конкретни случаи со цел да се идентификуваат конкретни криминалци, додека терористичкото профилирање поширок опсег, адресирање на грижите за националната безбедност и има за цел да спречи напади од големи размери.

Криминалното профилирање изработува проценки на ризик за конкретни жртви или потенцијални цели и помага во распределбата на истражните ресурси. Терористичкото профилирање проценува ризик за јавната безбедност и националната безбедност и формира антитерористички стратегии. Секако, важно е да се напомене дека и криминалното профилирање може да изработува проценки на ризик за националната и меѓународната безбедност доколку се работи за транснационален организиран криминал.

Земајќи предвид дека овие два вида на профилирање функционираат различно, неминовно е да се дојде до констатација дека тие прибираат информации од различни извори. Оттука, криминалното профилирање се потпира на докази од местото на злосторството, интервјуа со жртви и анализа на однесувањето на сторителот. Терористичкото профилирање користи разузнавачки капацитети, анализа на социјални мрежи, анализа на модели на движење и идеолошки индикатори.

Живееме во турбулентно време каде заканите се меѓусебно испреплетени и покомплексни од кога било досега. Тешко е да се направи дистинкција помеѓу тероризмот и криминалот бидејќи тие често знаат да соработуваат и да разменуваат техники, тактики и методи на работа. Оттука произлегува и потешкотијата во дефинирањето и правењето на дистинкција помеѓу криминалното и терористичкото профилирање. Многу често она кое е во теорија валидно, на терен е сосема различно, но сепак е неопходно да се даде некаква рамка и разграничување на овие видови на профилирање, со цел минимизирање на погрешно толкување информации и носење погрешни одлуки од страна на професионалците.

3.4 Историски развој

3.4.1 Раните почетоци

Самиот концепт на профилирање не е нов, тој е присутен во текот на историјата, но клучното е тоа што не бил нарекуван „профилирање“ и му недостасувале научните темели. Профилирањето е алатка која човекот ја употребувал во текот на своето постоење, но кога се зборува за историскиот развој, ќе се фокусираме на периодот од поставувањето на научните темели за профилирањето па сè до денес.

Веќе нагласивме дека во однос на профилирањето, криминалот и тероризмот се тесно поврзани, па така имаат и блиска историја. На почетокот, во средината на 20-тиот век, профилирањето се користело во однос на криминалните активности, кои во тоа време не биле толку тесно поврзани со тероризмот како што е случајот

денес, додека во тероризмот речиси, а можеби и воопшто, не се употребувало. Сепак, како клучна пресвртница во профилирањето се смета периодот помеѓу 1940-1950 година во Њу Јорк, САД.

Првиот профил поврзан со тероризмот се појавил за време на истрагата на озлогласениот случај познат како „Лудиот бомбаш“ во Њујорк. Џорџ Метески, познат како Лудиот бомбаш, го тероризирал Менхетен во текот на 1940-тите и 1950-тите. Поставил бројни експлозивни направи на јавни места, вклучувајќи театри, библиотеки и транспортни центри. Неговите мотиви биле вкоренети во гневот кон Кон Едисон, енергетската компанија за која верувал дека му згрешила.³²

Психијатарот д-р Џејмс Брусел бил повикан да помогне во истрагата. Тој ги анализираше начинот на комуницирање на бомбашот, однесувањето и моделите на неговите напади. Брусел, врз основа на сите овие податоци, направил детален психолошки профил на Лудиот бомбаш. Според профилот кој го изработил Брусел, Бомбашот бил:

- Стар, неженет маж;
- Чувствувал огорченост кон Кон Едисон;
- Параноичен, со Едипов комплекс.³³

Сите овие параметри кои го сочинувале профилот на Брусел се потпирале на неколку сознанија и претпоставки кои се темелеле на научни сознанија, односно:

- Имало поголеми шанси да биде маж бидејќи повеќето бомбардери се мажи;
- Бил поранешен вработен во Кон Едисон кој бил повреден на работното место и барал одмазда;

³² DeLani R. Bartlette (2019), „The Mad Bomber and the Birth of Criminal Profiling“, Medium (online), Достапно на: [The Mad Bomber and the Birth of Criminal Profiling | by DeLani R. Bartlette | New York Voice | Medium](#)

³³ Едипов комплекс, во психоаналитичката теорија, е желба за сексуална инволвираност со родителот од спротивниот пол и истовремена смисла на ривалство со родителот од ист пол. Ова е нормална развојна фаза кај децата од три до пет години кои се пребродува, но, во присуство на траума, се јавува „инфантилна невроза“ која е важен предвесник на слични реакции за време на возрасниот живот на детето.

- Со странско потекло, поради премногу формалниот стил на пишување без сленг;
- Со Едипов комплекс, заснован на „фаличната конструкција“ на бомбите, буквата „W“ која била напишана во белешките „налик на гради“ и сечење и пробивање на седиштата кога ги поставувал бомбите во кината;
- Неженет и живее со женски роднини, но не и со неговата мајка која најверојатно починала кога тој бил млад, врз основа на неговиот Едипов комплекс;
- Параноичен и околу 50-годишна возраст, бидејќи паранојата има тенденција да го достигне врвот на околу 35-годишна возраст, а бомбардирањата започнале пред 16 години.³⁴

Овие клучни показатели ги донесле властите до Џорџ Метески. Неговите мотиви за извршувањето на нападите биле вкоренети во гневот кон Кон Едисон, енергетската компанија за која верувал дека му згрешила, а во однос на неговиот брачен статус тој бил неженет.

Успехот на профилот на Брусел означил пресвртница во полето на криминалната истрага. Ја покажал вредноста на анализата на однесувањето и потребата од нов вид истражувачки пристап. Случајот „Луд бомбаш“ ги поставил темелите за развој на современи техники за криминално профилирање. Најинтересниот парадокс за овој случај е тоа што, иако станувало збор за терористички напад, тоа било всушност зачеток на криминалното, а не на терористичкото профилирање. Сепак, овој пример се зема како зачеток општо за профилирањето, бидејќи станувало збор за терористички напад. Ова дополнително ја потврдува тезата дека криминалното профилирање е тесно поврзано и испреплетено со профилирањето на тероризмот.

³⁴ JRank (2024), „Criminal Profiling, Origins, Procedures, Controversies, Resources“, jrank.org (online), Достапно на: [Criminal Profiling, Origins, Procedures, Controversies, Resources \(jrank.org\)](https://www.jrank.org/2024/01/criminal-profiling-origins-procedures-controversies-resources/)

3.4.2 Профилирањето денес

Денес профилирањето, или поконкретно профилирањето во тероризмот, останува и понатаму една од покомплексните и воедно поконтроверзните теми. Високото ниво на комплексност произлекува од различните видови профилирање, потешкотии во одредување на најсоодветниот вид на профилирање согласно конкретниот случај, обучување на доволно стручен кадар за кој се воедно потребни повеќе финансии, па оттука тоа се јавува како дополнителна потешкотија итн. Од друга страна пак, контроверзноста произлегува од методите кои се употребуваат во некои од видовите профили кои можат да се протолкуваат како дискриминаторни, навредливи и се потпираат на стереотипи.

Со развојот на државите во сите сфери (економија, технологија, индустрија...) паралелно се појавуваат нови закани, додека веќепостоечките се надоградуваат, усложнуваат и меѓусебно се испреплетуваат. Она кое било врв во областа на профилирањето во времето на Лудиот бомбаш, денес со новите технолошки напредоци и брзото темпо на ескалација на настаните, не би дало доволно соодветен одговор. Поради ова, неопходно е паралелно сите видови профилирање, односно профилирањето како целина да се развива и да е во чекор со новите трендови и потреби на државите и меѓународните организации кои се засегнати со прашањата од областа на безбедноста, и во овој случај со тероризмот.

3.5 Видови профилирање

Кога станува збор за профилирање на тероризмот, безбедносните агенции, владите и меѓународните организации користат различни техники за да го разберат и предвидат однесувањето на поединци или групи вклучени во терористички активности како и теренот каде би ги извршиле нивните напади. Овие техники се всушност различни видови профилирање кои се исклучително корисни алатки во секоја област на безбедноста, а особено во домените на организираниот криминал и тероризмот. Оттука, како најкористени и практично применувани видови профилирање може да се истакнат географското

профилирање, етничкото или расно профилирање, биометриското профилирање, бихејвиоралната анализа, анализата на социјалните мрежи, психолошкото профилирање, геополитичкото профилирање, анализата на патување и патни рути, финансиското профилирање и религиозното и идеолошкото профилирање.

Пред да се навлезе во индивидуалната анализа на сите овие видови профилирање, мора да се има предвид дека, прво, постојат уште многу други видови профилирање кои не се споменуваат дотолку поради нивната поретка употреба и понизок степен на прецизност и ефикасност при практичната примена и второ, не е ниту препорачливо да се користат апсолутно сите видови профилирање, бидејќи самите лица кои ги изработуваат профилите би биле преплавени со море на информации кои повеќе би наштетиле и би ја отежнале работата. Ова е особено предизвикувачки доколку се наоѓате во деликатна ситуација како што е профилирање на терористички напад и секоја минута потрошена на ирелевантни податоци е минута повеќе за терористите. Затоа, главниот фокус е ставен на овие видови профилирање.

Табела 1: Табеларно претставување на најчесто употребуваните видови профилирање, вклучувајќи ги нивните цели, методи и пример за тоа каде би се примениле на практичен начин.

Вид на профил	Цел	Метод	Пример
Географско профилирање	Идентификација на веројатните области каде терористите дејствуваат или планираат напади.	Анализирање на моделите на минати напади, рути на патување и безбедни засолништа.	Идентификување на региони со висока терористичка активност врз основа на историски податоци.
Расно и етничко профилирање	Проценка на потенцијалните закани врз основа на расни или етнички карактеристики.	Следење на поединци од одредени средини или региони.	Фокусирање на вниманието на патници од земји со познати терористички врски.
Биометриско профилирање	Идентификација на поединци користејќи физички карактеристики.	Собирање и анализа на биометриски податоци (пример: отпечатоци од прст)	Користење на биометриски бази на податоци на гранични контролни пунктови или аеродроми.

Вид на профил	Цел	Метод	Пример
Бихејвиорална анализа	Да се открие сомнително однесување или отстапки.	Набљудување на постапките, интеракциите и комуникацијата на поединците.	Следење на активноста на интернет или следење невообичаено однесување при патување.
Анализа на социјални мрежи	Мапирање на врските помеѓу поединци и групи.	Испитување на врските, врските и комуникациските мрежи.	Идентификување клучни фигури во терористичките мрежи.
Психолошко профилирање	Да се разбере начинот на размислување и мотивациите на потенцијалните терористи.	Анализа на списи, пропаганда и процеси на радикализација.	Идентификување знаци на екстремистичка идеологија или подложност на регрутирање.
Геополитичко профилирање	Да се проценат геополитичките фактори кои можат да придонесат за тероризам.	Земајќи ги предвид регионалните конфликти, политичката нестабилност и историските незадоволства.	Препознавање како геополитичките тензии можат да поттикнат радикализација.
Финансиско профилирање	Да се следат изворите на финансирање и финансиските трансакции.	Истражување на трагите за пари, банкарски сметки и сомнителни трансакции.	Идентификување на поединци или групи вклучени во финансирање тероризам.
Религиозно и идеолошко профилирање	Разбирање на верските или идеолошките мотивации на терористите.	Анализа на религиозни текстови, екстремистичка литература и пропаганда.	Препознавање знаци на радикализација во одредени системи на верување.

3.5.1 Географско профилирање

Географско профилирање е техника на криминално анализирање која ја употребува локацијата на серија од поврзани места на криминални активности за да го одреди најверојатното место на живеење на сторителот. Системот за географско профилирање создава мапа со локации за можни „бази“ на сторителот и тие бази се најчесто местото на живеење или работното место.

Имаме класичен пример за географско профилирање за време на епидемијата на колера во Лондон во 1849 година. Д-р Џон Сноу ги мапирал случаите на заболени и смртни случаи од епидемијата на различни адреси во Лондон. Она што тогаш го прикажувала мапата била концентрација на случаи што се центрираа околу пумпа за вода на Бродстрит. По внимателно испитување на пумпата, забележани се некакви остатоци и бела супстанција, кои се покажале како позитивни на колера.³⁵

За основоположник се смета Ким Росмо. Тој започнал да студира географско профилирање како дел од неговите докторски студии на Универзитетот Сајмон Фрејзер (Британска Колумбија, Канада), каде што студирал под менторство на професорите Пол и Патриша Брентингхам кои го развиле Брентингхамовиот модел.³⁶

Географското профилирање користи специјализиран софтвер за мапирање на криминал за да одреди каде најверојатно живее престапникот. Како пример за ваков софтвер е GeoCrime. Таа е програма базирана на Виндоус (Windows) за генерирање на геопрофил врз основа на податоци од документирани инциденти. Комбинира автоматски и рачни техники за анализа на просторна и веројатна дистрибуција на местата на криминал. Употребата на програмата вклучува внесување податоци за локацијата на извршено криминално дело и геокодирање и мапирање на локации на криминал од податоците за адреси. Постојат и многу други програми и софтвери кои полицијата и останатите служби ги користат и за

³⁵ Stavros Makris (2018), „Geographic Profiling Locating The Serial Murderers“ стр. 4-8, Достапно на: [FULLTEXT01.pdf \(diva-portal.org\)](#)

³⁶ All About Forensic Psychology (2022), „Geographic Profiling“, All About Forensic Psychology (online), Достапно на: [Geographic Profiling \(all-about-forensic-psychology.com\)](#)

најпознат и најшироко употребуван се смета Компјутерскиот „Ригел“ (Rigel Computer Software).³⁷

Во однос на практичната примена на географското профилирање, непходно е да бидат исполнети пет критериуми:

1. Престапникот извршил минимум пет кривични дела;
2. Злосторствата се поврзани со истиот престапник и серијата е релативно завршена;
3. Престапникот што ги извршил злосторствата не патувал до областа на криминалните активности;
4. Престапникот не се преселил (или работел од повеќе различни локации) за време на извршувањето на серијата од криминални активности.
5. Дистрибуцијата на соодветни мети е релативно еднородна околу домот на престапникот.

Географското профилирање наоѓа примена и во криминалистиката и во тероризмот. Геомапирањето се употребува од страна на надлежните органи за да наоѓаат и криминални организации или поединци, како и чинители на терористички акти. Воедно, земајќи ја предвид испреплетеноста на криминалот со тероризмот, тешко е во денешно време да се одреди за кое дело станува збор и која алатка е најсоодветна. Тука, географското профилирање има предност бидејќи истите критериуми за изработка на прецизен геопрофил важат и за криминални дејствија и за терористички напади. Меѓутоа, географското профилирање има и слаби страни, односно, доколку не се исполнети овие критериуми, профилот не е прецизен. Затоа, со цел да не се трошат залудно ресурсите на надлежните органи, неопходни се стручни лица во оваа област кои може да проценат дали во

³⁷ Asmir Butkovic (2019), „GeoCrime - Geographic profiling software“ стр. 1-2, Academia.edu (online), Достапно на: [\(1\) GeoCrime - Geographic profiling software | Asmir Butkovic - Academia.edu](#)

конкретниот случај вреди трошењето на драгоцените ресурси, како што е времето, за изработка на еден ваков профил.

3.5.2 Биометриско профилирање

Во доменот на технолошкиот напредок, неколку иновации ја надминаа нашата имагинација за тоа што сè може да се постигне. Овие нови технологии ни го олеснуваат животот, но и воедно го загрозуваат. Како таков пример е вештачката интелигенција (ВИ) која ги олеснува секојдневните обврски, но истовремено претставува закана за опстанокот за многумина чии работни места се исполнети од машини и компјутери. Како една од поновите иновации која наоѓа широка примена во областа на безбедноста е биометриското профилирање.

Биометриката е научна дисциплина која се занимава со „Мерлива физичка карактеристика или лична карактеристика на однесување што се користи за препознавање на идентитетот или потврдување на тврдениот идентитет на апликантот. Сликите на лицето, отпечатоците од прсти и примероците за скенирање на ирисот се сите примери за биометрија“.³⁸

Иако постојат записи за биометрика кои датираат од Вавилонската империја околу 500 п.н.е., првиот биометриски систем за идентификација бил документиран во Париз, Франција, во 1800-тите. Алфонс Бертјон смислил систем на прецизни мерења на телото за споредба и категоризација на прекршителите. Иако овој пристап беше далеку од идеален, тој беше првиот што користеше карактеристични биолошки особини за автентикација на идентитетот. Во 1880-тите, отпечатокот од прст го следеше примерот, служејќи како потпис на договорите, како и алатка за идентификување на престапниците. Утврдено е дека отпечатоците од прсти на една личност служат како правен маркер за идентификација и може да се користат за да се утврди нечија вина или невиност. Иако прецизниот основач на отпечатоците за идентификација е предмет на дискусија, Едвард Хенри е препознатлив по тоа што

³⁸ National Institute of Standards and Technology (2024), „Biometrics“, Computer Security Research Center (online), Достапно на: [Biometrics - Glossary | CSRC \(nist.gov\)](https://www.nist.gov/CSRC/Biometrics-Glossary)

го создал Хенриновиот систем за класификација. Ова бил првиот систем за идентификација врз основа на уникатните архитектури на отпечатоци од прсти. Спроведувањето на законот брзо ги замени методите на Бертилон со системот, кој стана индустриски стандард за криминална идентификација. Ова го означил почетокот на едновековното истражување на други карактеристични физиолошки особини кои би можеле да се користат за идентификација.³⁹

Биометриското профилирање на почетокот било користено и развиено во областа на криминалистиката, меѓутоа тоа наоѓа практична примена и во антитерористичкото дејствување. Како најголема меѓународна полициска организација во светот, ИНТЕРПОЛ е идеално и уникатно поставен да развива и споделува глобална експертиза во биометриката за да им помогне на органите за спроведување на законот во борбата и истрагата на криминалот и тероризмот.⁴⁰ Исто така, од голема важност е да се спомене и Безбедносната резолуција 2396 на Обединетите нации, која ја нагласува важноста на биометриските алатки во спречувањето и спротивставувањето на тероризмот.⁴¹

3.5.3 Психолошко профилирање

Психолошкото профилирање вклучува процес на поврзување на дејствијата на сторителот на местото на злосторството со нивните најверојатни карактеристики за да им се помогне на полициските истражители да го намалат и да им дадат приоритет на група на најверојатно сторители, односно осомничени.

Целта на психолошкото профилирање е да ги опише веројатните социјални (на пример, вработување, брачен статус) и ментални (на пример, образовни достигнувања, мотивација) особини на сторителот. Дополнително, нуди прогнози

³⁹ Amanda Moen (2021), „A Brief History of Biometrics“, bioconnect (online), Достапно на: [A Brief History of Biometrics | BioConnect](#)

⁴⁰ Open Access Government (2016), „Using biometrics to fight crime“, Open Access Government (online), Достапно на: [Using biometrics to fight crime | Open Access Government](#)

⁴¹ Dr. Krisztina Huszti-Orbán, Prof. Fionnuala Ní Aoláin (2020), „Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?“, Human Rights Center, University of Minnesota, ohchr.org (online), Достапно на: [biometricsreport.pdf \(ohchr.org\)](#)

за тоа кого сторителот најверојатно ќе го насочи следно, каде ќе нападне и кога, како и потенцијални техники за интервју за да се извлечат детали за извршените прекршоци и признавањето на вината.

Постојат два главни пристапи за психолошко профилирање:

- **Пристап од врвот надолу** (американски): Овој пристап започнува со големата слика и потоа ги пополнува деталите. Се обидува да ги вклопи деталите за криминалот под веќе постоечките категории (типологии). Од податоците собрани на местото на злосторството, иследниците можат да ги идентификуваат карактеристиките на сторителот на пр. животен стил или карактеристики на личноста;
- **Пристап од дното нагоре** (британска или истражувачка психологија): Овој пристап започнува со мали детали и ја создава големата слика. Не се направени првични претпоставки за сторителот и пристапот во голема мера се потпира на компјутерските бази на податоци.⁴²

Психолошкото профилирање во тероризмот вклучува разбирање на терористичкото однесување преку леката на психологијата. Навлегува во сложената област на психолошки фактори кои можат да придонесат за ангажман на поединецот во тероризам, вклучувајќи мотивации, особини на личноста и општествени влијанија.⁴³ Психологијата на тероризмот е сложена и повеќеслојна, а нејзиното разбирање бара сеопфатен пристап и стручна компетенција.

3.5.3.1 Бихејвиорална анализа

Бихејвиорална анализа, позната и како анализа на однесувањето, е научно проучување на начинот на однесувањето на личноста. Тој се фокусира на разбирање

⁴² Saul Mcleod (2023), „Offender Profiling In Psychology“, Simple Psychology (online), Достапно на: [Offender Profiling In Psychology \[Criminal Profiling\] \(simplypsychology.org\)](https://www.simplypsychology.org/offender-profiling-in-psychology/)

⁴³ Criminal Justice Academic Writing Service (2024), „Profiling in Terrorism Cases“, iResearch.net (online), Достапно на: [Profiling in Terrorism Cases - Criminal Justice - iResearchNet](https://www.iresearch.net/profiling-in-terrorism-cases-criminal-justice/)

зошто луѓето се однесуваат онака како што се однесуваат, како однесувањето може да се промени и како одредени однесувања може да се спречат.⁴⁴

Постојат две главни области на анализа на однесувањето: експериментална и применета. Експерименталната страна се фокусира на додавање на научното знаење за тоа како луѓето учат. Применетата област се фокусира на користење на тоа знаење за да им помогне на луѓето да ги надминат проблемите со кои можеби се соочуваат. Во контекст на анализата на податоци, бихејвиоралната анализа е област која се фокусира на обезбедување увид во постапките на луѓето, обично во врска со купувањето преку интернет. Се користи во е-трговија, игри, социјални медиуми и други апликации за да се идентификуваат можностите за оптимизирање со цел да се реализираат конкретни деловни резултати. Така, покрај употребата во областите на економијата, трговијата и психологијата, овој вид на анализа на лична се употребува и при анализа на сторители на терористички чинови.

Анализата на однесувањето во контекст на тероризмот вклучува проучување на однесувања и психолошки фактори поврзани со поединци, групи и организации вклучени во терористички активности.

На индивидуално ниво, традиционалните фактори на ризик од насилство, како што се историјата на насилничко однесување, психијатриско растројство или злоупотреба на дрога се донекаде бескорисни во предвидувањето на ризикот од осамени терористички акти. Наместо тоа, истражувачите работеа на идентификување модели на однесување тесно поврзани навреме со акти на насочено насилство, како што е тероризмот. Овие модели на однесување, познати како предупредувачки однесувања, можат да обезбедат истражен профил за да им помогнат на агенциите за спроведување на законот да го фокусираат своето внимание на теми од загриженост претходно идентификувани преку собирање разузнавачки информации или други напори за борба против тероризмот.⁴⁵

⁴⁴ Kendra Cherry (2024), „Behavior Analysis in Psychology“, Very Well Mind (online), Достапно на: [Behavior Analysis in Psychology: How It's Used \(verywellmind.com\)](https://www.verywellmind.com/behavior-analysis-in-psychology-how-it-s-used/)

⁴⁵ Reid Meloy (2016), „Perspective: Identifying Warning Behaviors of the Individual Terrorist“, FBI Law Enforcement Bulletin (online), Достапно на: [Perspective: Identifying Warning Behaviors of the Individual Terrorist — LEB \(fbi.gov\)](https://www.fbi.gov/law-enforcement-bulletin/perspective-identifying-warning-behaviors-of-the-individual-terrorist-leb)

На ниво на група, се разгледува процесот на изградба на споделена реалност, општествено влијание вклучено во регрутирањето на нови членови во терористичка организација, нивното индоктринирање во терористичката идеологија и употребата на јазикот во креирањето на норми кои гарантираат тероризам.

На организациско ниво, прашањата за обука, логистика и исплатливост се разгледуваат бидејќи се однесуваат на одлуките за започнување или воздржување од терористички активности.⁴⁶

Пристапот за увид во однесувањето овозможува идентификација на факторите на ризик и отпорност и развој на емпириски потврдени интервенции за креаторите на политики и практичарите за ефикасно спречување и спротивставување на насилниот екстремизам. Овој пристап не предвидува насилство, но помага да се детектираат проксималните индикатори на загриженост за спроведување на законот што може да го стесни фокусот на истрагата, да им даде приоритет на случаите и да помогне да се планира навремена интервенција за управување со ризик.

Предупредувачките однесувања се модели на однесување тесно поврзани со акти на насочено насилство, како што е тероризмот. Овие однесувања можат да обезбедат профил за да им помогнат на агенциите за спроведување на законот да го фокусираат своето внимание на определени случани претходно идентификувани преку собирање разузнавачки информации или други напори за борба против тероризмот. Како примери за предупредувачки однесувања поврзани со тероризмот може да се наведат:

- Субјектите се впуштаат во различни однесувања кои опфаќаат дел од истражување, планирање или подготовка за терористички акт или спроведување на таков напад;

⁴⁶ Arie W. Kruglanski, Shira Fishman (2009), „Psychological Factors in Terrorism and Counterterrorism: Individual, Group, and Organizational Levels of Analysis“, University of Maryland, Достапно на: [sipr.1009_LR\(umd.edu\)](http://sipr.1009_LR(umd.edu))

- Фиксација т.е. зголемена преокупација со личност или причина;
- Потенцијален напаѓач кој се идентификува со претходните напаѓачи или нивните дејства;
- Чин на насилство што се чини дека не е поврзан со каква било стратегија за управување со закани;
- Излив на енергија. Ова вклучува зголемување на активностите поврзани со целта или причината, онлајн или офлајн;
- Комуникација со трето лице за намера да се направи штета;
- Директно соопштена закана: субјектот комуницира закана директно до целта или надлешните органи;
- Субјектот го прифаќа менталитетот „Сè или ништо“ додека се приближува моментот за реализација на нападот.⁴⁷

Овие предупредувачки однесувања не предвидуваат насилство. Тие се користат како образец за истражување, а не како алатка за проценка на ризик. Целта на идентификувањето на овие однесувања е да се откријат проксималните индикатори на загриженост за спроведување на законот што може да го стесни фокусот на истрагата, да им даде приоритет на случаите и да помогне да се планира навремена интервенција за управување со ризик.

3.6 Практична примена на профилирањето

Досега разгледувавме што претставува профилирањето, неговиот историски тек и развој, како и различните видови на профилирање. Но, тука се поставува прашањето, како ова знаење може полицијата, експертите, профајлерите и органите за спроведување на законот, можат практично да го применат ова знаење

⁴⁷ Meloy, J. R., Hoffmann, J., Guldemann, A., & James, D. (2012), „The role of warning behaviors in threat assessment: An exploration and suggested typology“ стр. 265-266, Wiley Online Library (online), Достапно на: [The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology \(drreidmeloy.com\)](http://drreidmeloy.com)

и да добијат најдобри резултати. Токму за оваа цел се изработени посебни стратегии и методи кои се сотојат од неколку етапи:

Прва фаза: Инпут

Кога станува збор за профилите, тие може да се засноваат на претходни искуства, односно минати слични напади како оној кој е предмет на анализа, или пак да се добијат податоци директно од самиот случај кој е тема за обработка. Оттука, првата фаза се состои од прибирање на што е можно повеќе релевантни информации како информации поврзани со тероризмот, фотографии од планот за тероризам, мапи, маршрути, употребено оружје, клучни места, терористичка сцена, извештаи од обдукција и во суштина сè што веројатно укажува што се случило, зошто се случило и како се случило.⁴⁸

Втора фаза: Процесирање на податоци

Следната фаза вклучува откривање дали терористичкиот акт во истрагата може да биде пронајден во рамките на голем број профили на случаи кои се од сличен карактер и, на терористот да му бидат доделени определени карактеристики и да биде класифициран во некоја категорија (волк-самотник, член на некоја организација, бомбаш самоубиец и сл.). Тука исто така се додаваат широк спектар на можни психолошките одлики како и описи за личниот живот на терористот, како што се возраст, брачен статус и мотив.

Трета фаза: Проценка на терористичкиот акт

Клучната цел на оваа фаза е да се спои синџирот на терористички чинови пред, за време на и по терористичкиот акт. Во третата фаза, истражителот треба да го реконструира терористичкиот акт од перспектива на државата и на терористот и да се процени штетата што е направена.⁴⁹

Четврта фаза: Профил на терористот

⁴⁸ Farhan Hyder Sahito, Wolfgang Slany, Safdar Zaman, Irfan Hyder Sahito and Rana Shahzad Qaiser (2013), „Terrorist profiling as a Counterinsurgency Strategy: Applying the Concept to Law Enforcement“, стр. 282, issr journals (online), Достапно на: [LJIAS-13-211-34.pdf \(issr-journals.org\)](https://www.issr-journals.org/LJIAS-13-211-34.pdf)

⁴⁹ Исто

Доколку во втората фаза се даваа повеќедимензионални описи за тоа кој и каков е сторителот на терористичкиот чин, во оваа фаза профајлерот ја има задачата да создаде конкретен профил за терористот. Тоа вклучува возраст, пол, брачен статус, етничка припадност, религиска припадност, ниво на интелигенција, семејна историја, поврзаност со некоја организација и сл.

Петта фаза: Распит

Во последната фаза од процесот на изработка на терористички профил, експертот изработува детален извештај за потенцијалниот сторител кое треба да биде пронајдено, заедно со сите негови карактеристики. Оттука овој извештај се предава на полицијата, истражителите и надлежните органи, кои благодарение на извештајот знаат какво лице бараат и во кој регион.

Профилите се темелат на податоци добиени од минати напади, анализа на сторителите, како и анализа на нападот кој е актуелен во моментот, односно оној за кој е потребен изработка на профил.

Пред сè, треба да се анализира кога и каде се случил нападот, зошто токму таа локација, рутата која се употребувала за пристигнување до и заминување од локацијата, дали и кога би се случил наредниот напад, дали овој напад е поврзан во серија од други претходни напади и слично. По добивање на сите овие информации, треба да се анализира и самиот сторител, односно, кој е Тој?

Пред сè, треба да се одреди дали навистина станува збор за едно или повеќе лица. Дали е волк-самотник, некој кој е во контакт или дел од некоја организација или пак станува збор за група на терористи од теористичка организација. Оттука, првите параметри кои се разгледува се полот и возраста. Согласно податоците од Студија за тероризмот на осамен престапник во Соединетите Американски Држави, изработена од Единица за анализа на однесувањето при Федералното биро за истраги (ФБИ)⁵⁰, согласно мострата на случаи кои биле земени предвид за студијата (52 напади), во сите 52 случаи сторителите биле мажи. Од друга страна пак,

⁵⁰ U.S. Department of Justice, FBI, Behavioral Analysis Unit (2019), „A study of Lone Offender Terrorism in the United States (1972-2015)“, стр. 12-13, Достапно на: [lone-offender-terrorism-report-111319 \(1\).pdf](#)

согласно податоците од НАТО⁵¹, во 2018 година 22% од уапсените терористи биле жени. Согласно нивните анализи, зголемен е процентот на жени-терористи. Сепак, при правењето профил, процентуалните шанси за тоа терористот да биде маж наспрема жена се речиси 80% наспрема 20%.

Согласно истражувањето на Единицата за анализа на однесувањето, возраста на терористите, најверојатни години за извршување на напади се од 18 до 44 години, со тоа што најголема процентуална застапеност во истражувањето биле лица од 30-34 години со 21% застапеност, потоа од 18-24 години со 17% застапеност, 40-44 со 15% застапеност и 25-29 со 12% застапеност. Најмала застапеност имале лицата од 15-17 годишна возраст со 2%. За споредба, според списанието за полициско кризно преговарање (Journal for police crisis negotiation)⁵², најголеми шанси има терористот да биде на возраст помеѓу 18-25 годишна возраст, додека најмалите шанси има над 30 години или под 16. Ова делумно се поклопува со податоците од ФБИ, освен што, според нив, постојат големи шанси лицето да има над 30 години. Но, оваа разлика во проценката на годините може да се должи и на разликата на податоците кои биле употребувани во различните анализи. Така, може да се каже дека има најмалите шанси терористот да има под 16 години и најверојатно е лице кое се наоѓа во категорија од 18-29 како помлада категорија и 30-39 како средна категорија.

Од психолошка гледна точка, двете горенаведени анализи укажуваат на некои психолошки тенденции кои се најчесто присутни кај терористите, и тоа:

- Нарцисоидност;
- Параноја;
- Чувство на несреќа и незадоволство;
- Психопатија и социопатија.

⁵¹ NATO (2023), „Deep Dive Recap: Counter Terrorism and the Gender Perspective“, NATO (online), Достапно на: [NATO - News: Deep Dive Recap: Counter Terrorism and the Gender Perspective, 28-Mar.-2023](#)

⁵² Reuben Vaisman-Tzachor (2007), „Profiling Terrorists“, Journal of Police Crisis Negotiations, researchgate (online), Достапно на: [\(PDF\) Profiling Terrorists \(researchgate.net\)](#)

Како еден од факторите кој не смее да се запостави е степенот на образование. Денес владее верувањето дека терористите се неписмени, необразовани и имаат низок коефициент на интелигенција, но тоа не е случај, особено во поново време. Во исламскиот тероризам е забележано дека има голем број терористи кои се конкретно од областа на инженерингот, но тука се поставува прашањето, зошто?

Во анализата на Гамбета и Хертог⁵³ на податоците за 497 членови на екстремистички групи, тие заклучиле дека, настрана од специфичен начин на размислување типичен за инженерите, главната причина за приклучување кон терористичка група е искусувањето на фрустрирани очекувања и релативна лишеност: инженерството е една од најпрестижните професии со високи услови за влез во муслиманските земји, така што младите студенти очекуваат соодветно вработување со висок статус по дипломирањето. Меѓутоа, поради неуспесите во економскиот развој во Северна Африка и Блискиот Исток, таквите можности за висок статус се исклучително ретки. Така, овие млади инженери доживуваат голема дисонанца помеѓу заслугата и наградата, што придонесува за нивна радикализација. Интересно е што Гамбета и Хертог не нашле преголема застапеност на инженерите меѓу терористите на Запад, во Сингапур или во Саудиска Арабија, каде што дипломираните студенти имаат далеку подобри професионални можности. (Во овие области исламскиот тероризам привлече повеќе маргинални мажи со пониско образование). Оттука, може да констатираме дека најранлива категорија подложна на радикализација се образовани млади мажи кои се фрустрирани поради недостаток на можности во земјите во развој во кои живеат. Но, приказната може да биде и сосема обратна. Оние кои се сиромашни и отфрлени од системот може да чувствуваат повторна дисатисфакција исто како оние кои се побогати и образовани, така, можеби мотивот и главниот показател за тоа кои подлежи на радикализација и кој е терорист, не лежи во идеологиите кои ги прифаќаат, туку што претставува таа за нив. Тие луѓе бараат да бидат прифатени од некој и нешто во време кога се оттуѓени од нивното општество. Поради ова, како почетна точка на профилите не треба да биде религијата, полот, возраста или

⁵³ Gambetta D, Hertog S. (2016), „Engineers of Jihad: The Curious Connection Between Violent Extremism and Education“, Princeton, Princeton University Press.

годините, туку да се започне со барањето во области каде има ранливи категории кои вклучуваат висок степен на незадоволство, без оглед дали станува збор за богати или сиромашни, образовани или необразовани, мажи или жени. Опасно е профајлерите да се водат по стереотипи бидејќи, како што укажува примерот на Гамбета и Хертог, не сите терористи се необразовани. Напротив, тоа може да се високо образовани луѓе кои, како резултат на несоодветен третман од системот и државата одлучуваат да се насочат кон екстремизмот како начин на изразување на нивниот револт.

3.7 Предности и недостатоци на профилирањето

Профилирањето во контекст на тероризам се однесува на систематска анализа на однесувањето, демографските и психолошките карактеристики на лицата кои може да представуваат закана за националната безбедност. Оттука, профилирањето на тероризмот поседува определени предности и недостатоци.

Профилирањето е ефективен начин за борба против тероризмот. Според некои експерти, профилирањето е ефективен метод за борба против криминалот и тероризмот и наоѓа широка употреба во двете области. Тој е применуван од страна на системот за безбедност на САД, Европската Унија и НАТО. Дополнително, тој е применет во процесот на Превентивна проценка на ризици. Имено, Профилирањето обезбедува вреден алат за превентивна проценка на ризици преку идентификување на шеми на однесување кои се типични за терористите, статистички податоци, демографски податоци, психолошки извештаи и слично.

Профилирањето се состои и од определени недостатоци и контраверзии. Контроверзноста околу профилирањето се однесува на можноста за креирање на профили врз основа на стереотипи и дискриминаторски политики. Ова претставува сериозна дилема бидејќи вакви профили може да бидат изработувани со цел да се легитимизира прогонување или омаловажување на одреден профил на луѓе, согласно нивните верувања и убедувања, расна припадност, етничка припадност,

религија. Првичната дискусија се води во однос на проблемот со општата дискриминација.

Друга област на расправа се фокусира на несразмерното влијание на профилирањето врз малцинските заедници. Расното и етничкото профилирање, особено, е критикувано за овековечување на стереотипите и придонесување за прекумерно полициско работење во реони каде живее одредена демографија. Профилирањето може, ненамерно или не согласно намерата на оној кој го изработува профилот, да таргетира одредени заедници, што ќе доведе до нарушување на довербата помеѓу органите за спроведување на законот и јавноста.

4. ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА

4.1 Дефинирање

Терминот „вештачка интелигенција“ се споменува честопати, особено во последните неколку години, меѓутоа се забележува дека многумина го употребуваат во секојдневниот говор, но малкумина знаат за што всушност станува збор и како правилно и соодветно да ракуваат со неа. Поради ова, неопходно е да појасниме што е вештачката интелигенција.

Оттука, таа се дефинира како „компјутерски концепт што ѝ помага на машината да размислува и да решава сложени проблеми како што ние луѓето правиме со нашата интелигенција. Слично на тоа, ВИ или вештачката интелигенција треба да работи на проблем, да прави некои грешки при решавањето на проблемот и да учи од проблемите на самокорегирачки начин како дел од нејзиното самоподобрување.“ Интересното кај оваа дефиниција е тоа што ВИ се споредува со нашата и ни дава до знаење на кои принципи се темели, односно, налик на нас, таа зима една задача, ја проучува, постапува кон нејзино решавање и потоа при процес на евалуација на направени грешки, учи и го помни тоа сознание

за грешката да не се повтори. На овој начин, ВИ се надополнува и надоградува, а со тоа станува и сè по софистицирана.

За понатамошно појаснување на тоа до кој степен е напредната вештачката интелигенција и колку е таа самосвесна, во име на овој истражувачки труд е направена компаративна анализа на неколку различни вештачки интелигенции, каде вниманието е насочено кон тоа колку се тие самосвесни, доколку воопшто се, како се дефинираат себеси како вештачки интелигенции и што всушност значи тој поим за нив.

Методологијата на истражувањето е сведена на директна комуникација со вештачката интелигенција преку компјутер, каде на интерфејсот се разговара со вештачкиот ентитет и се поставуваат две прашања на македонски јазик, односно 1) Дали си самосвесен?; и 2) Што е вештачка интелигенција?

За потребите на ова истражување беа разгледани четири ВИ, и тоа: Google Gemini, ChatGPT, Perplexity и Microsoft Copilot.

Табела 2: Табеларен приказ на резултатите од истражувањето.

	Дали си самосвесно?	Што е вештачка интелигенција
Google Gemini	Тоа е одлично прашање. Како голем јазичен модел, развиен од Google, јас не сум самосвесен во човечка смисла.	Вештачката интелигенција (ВИ), или на англиски Artificial Intelligence (AI) , е широка област на компјутерската наука која се фокусира на создавање машини кои можат да вршат задачи кои вообичаено бараат човечка интелигенција.
ChatGPT	Не, не сум самосвесен. Немам свест, чувства или лични доживувања — само обработувам информации и генерирам одговори врз основа на шаблони и податоци со кои сум трениран.	Вештачка интелигенција (или скратено ВИ, од англиски Artificial Intelligence – AI) е област во компјутерските науки која се занимава со создавање системи што можат да извршуваат задачи кои обично бараат човечка интелигенција.

	Дали си самосвесно?	Што е вештачка интелигенција
Perplexity	Не, не сум самосвесен. Јас немам сопствена свест, чувства или искуства. Функционирам преку обработка на информации и јазични модели кои ми овозможуваат да создадам одговори што изгледаат разумно и контекстуално точни.	Вештачка интелигенција (ВИ) е технологија и научна област која развива машини и компјутерски системи способни да извршуваат задачи што бараат човечка интелигенција, како што се учење, размислување, решавање проблеми, препознавање на јазик и слики и донесување одлуки.
Microsoft Copilot	Не, јас не сум самосвесен. 😊 Можам да обработувам информации, да анализирам податоци и да создадам одговори што изгледаат многу „човечки“, но тоа не значи дека имам свест, чувства или сопствено „јас“. Свеста кај луѓето е поврзана со субјективно доживување – да чувствуваш, да имаш внатрешен свет, да бидеш свесен за своето постоење. Јас немам такво нешто.	Вештачка интелигенција (ВИ) е област во компјутерските науки која се занимава со создавање системи што можат да извршуваат задачи кои обично бараат човечка интелигенција.

Клучните наоди од истражувањето водат кон тоа дека погоренаведените ВИ не поседуваат самосвест, а одговорот кој го даваат се темели на обработени податоци. Одговорите кои ги даваат за тоа што е ВИ е повеќе или помалку ист кај сите, што ни укажува дека црпат исти или слични податоци со цел да го дадат одговорот, т.е. одговорот доаѓа од низа преработени податоци, а не од нивната самосвест за тоа што се всушност тие како вештачки интелигенции. Покрај ова, интересна забелешка е дека сите ВИ веднаш го препознаа македонскиот јазик освен ChatGPT, кој првично даде одговор на бугарски, по што му беа дадени насоки да одговори на македонски јазик и потоа го даде истиот одговор само преведен.

Вештачката интелигенција е напредна наука и технологија која може да обработи голем обем податоци за краток временски период, или во најмала рака,

побрзо од кој било човек. Поради ова, таа претставува клучна алатка во сите области.

4.2 Историја

Вештачката интелигенција е актуелна тема од 2023 година, но ова е само ново откритие за пошироката јавност, во спротивно ВИ е технологија чиј развој започнал уште во 50-тите години на минатиот век.

Конференцијата во Дартмут во 1956 година ги собрала истражувачите од повеќе области за да ги истражат „машините што размислуваат“. Ова се смета за почеток на вештачката интелигенција како посебна област на студии и каде што терминот „вештачка интелигенција“ бил употребен за прв пат од страна на визионерите на таа конференција. Конференцијата била организирана од страна на Дортмаутскиот професор по математика Џон Макарти, според кој конференцијата би служела „за да се продолжи врз основа на претпоставката дека секој аспект на учењето или која било друга карактеристика на интелигенцијата во принцип може да се опише толку прецизно што може да се направи да го симулира машина“.

Уште на почетокот на векот, вештачката интелигенција го привлела вниманието на јавноста, кога што бил суперкомпјутерот IBM Deep Blue кој го победил шаховскиот велемајстор Гари Каспаров во 1997 година, со алгоритми за вештачка интелигенција развиени од инженерите на IBM. Неколку години подоцна, во 2011 година, компјутерот IBM Watson победил на американското гејм-шоу Jeopardy, откако бил обучен со помош на огромен збир на податоци.

Сите овие настани за прв пат покажале дека компјутерите кои се хранат со големи количини на податоци се и повеќе од способни да ги надминат луѓето при процесот на решавање на многу сложени задачи. Во текот на изминатата деценија, вештачката интелигенција се развивала со забрзано темпо и низа компании развивале програми, како што е AlphaFold од Google Deepmind. Програмата користи вештачка интелигенција за да ја предвиди 3D структурата на речиси секој протеин во човечкото тело. Ова го подобрува нашето разбирање за болести како

што е Алцхајмеровата болест и може масовно да го забрза истражувањето на вакцини и лекови.

ВИ се употребува во разни области, како медицината, архитектурата и инженерството, но исто така се употребува и во уметноста. Во 2023 година, музеј во Хаг, Холандија, ја позајмил светски познатата слика „Девојка со бисерна обетка“ од Јоханес Вермер на меѓународна изложба и привремено ја замениле во својата галерија со верзија инспирирана од вештачка интелигенција насловена „Девојка со светкави обетки“, при што многу посетители на галеријата верувале дека станува збор за вистинска слика. Тоа ни докажува дека вештачката интелигенција е способна не само за генерирање текст и обработка на податоци, туку и генерирање на слики, па дури и видеа. Оттука, произлегува голем безбедносен ризик од феноменот познат како „deepfake“. Буквално преведено како „длабока лага“, дипфејк е термин што се користи за лажни видеа направени со употреба на технологии за замена на ликот, т.е. може да направите вашиот лик да изгледа како некоја сосема друга личност. Ова е проблематично бидејќи, исто како и генерираните слики, може да направите било која влијателна личност да изгледа како да е во затвор, да повикува на протести, насилни екстремистички идеологии итн. Пример за ова е видеото кое циркулираше пред неколку години во кое се користи глас генериран од вештачка интелигенција кој го имитира поранешниот претседател Обама. Подоцна ова видео беше отстрането поради кршење на политиката за синтетички медиуми на ТикТок.

Злоупотребата на овие алатки, со цел генерирање на екстремистички содржини, како слики, видеа и текстови, може да бидат користени со цел промовирање на идеали, насилство, лажни вести, лажни изјави од политичари и релевантни донесувачи на одлуки, со што може да се разгорат етнички конфликти, меѓудржавни односи и брза ескалација на веќе постоечки проблематики. Потребата за соодветни одговори и проучување на оваа технологија и наука произлегува токму од овие закани, да се научи правилно користење, прекин на ширење на дезинформации и давање на одговор на заканите кои произлегуваат и би можеле да произлезат од ВИ. Во секој случај, клучно е да се запомне дека оваа технологија

е само алатка и таа сама по себе не е ниту добра ниту лоша, само е прашање на тоа во чии раце ќе падне истата.

4.3 Улогата на ВИ во процесот на профилирање на тероризмот

Вештачката интелигенција со нејзиниот брз развој стана една од најкорисните технологии во светот, која денес се користи за дијагностицирање болести, брза обработка на податоци и општа помош во секојдневието на сите нас. Оттука, таа постана и една од најтрансформативните алатки во областа на борбата против тероризмот, преку нејзиниот потенцијал во процесот на профилирање. Првично, од појавата на профилирањето како алатка, а се до денес таа се потпира на човечкиот фактор, т.е. степенот на прецизноста на профилирањето се наслонува на тоа колку податоци се прибрани од страна на службениците и колку добро тие се филтрирани од нивна страна, мануелна анализа, или од страна на компјутерски системи и следствено на ова, ограничени резултати. Денес, системите за вештачка интелигенција се способни да прибираат, обработуваат и исфрлаат енормна количини податоци и информации во реално време, со што се подобрува целокупниот процес, се забрзува времето на реакција и степенот на ефикасност и обемот на изреализирана работа се зголемува. Со нивна инкорпорација во работата на полициските службеници и вештаци или пак, уште подобро, во целокупните безбедносни системи ќе се рedefинира начинот на кој тие функционираат и како пристапуваат кон терористичките закани.

Капацитетот на вештачката интелигенција да обработува големи бази на податоци е еден од нејзините најважни придонеси во профилирањето на тероризмот. Ова е особено значајно бидејќи во секој миг, енормни количини на информации се произведуваат на социјалните медиуми, интернет портали, форуми итн. Во овој поглед, ВИ може помогне при идентификација на сомнителни објави како слики, видеа и текстови, ненадејни промени во онлајн однесувањето на профили кои се однапред обележани од страна на службите како ризични или сомнителни, што може да укажуваат на обиди за радикализација, ширење на

пропаганда или доктрини, отворено подржување, планирање или реализација на напади. Овој вид на следење е клучен земајќи предвид дека аналитичарите, без оглед на степенот на нивната стручност, не се во можност да бидат во чекор со толку обемен материјал кој постојано се објавува на интернет, за разлика од ВИ која ги обработува истите количини податоци во рок од неколку секунди. Со рана детекција на заканите пред да се материјализираат, вештачката интелигенција им помага на властите да преминат од реактивна кон проактивна превенција.

Вештачката интелигенција, исто така, го револуционизираше биометриското профилирање. Системи за препознавање лица и отпечатоци се сè повеќе распространети на аеродроми, гранични премини и јавни простори за да се споредат поединците со листите за лица со забранет влез во државите, црни листи и сл. Покрај препознавањето на лица и отпечатоци, напредната биометриска технологија е способна да препознава лица по нивните гласови, движење и говорот на телото што овозможува уште поголема прецизност.

И покрај овие предности, употребата на вештачка интелигенција во профилирањето терористи покренува длабоки етички и правни предизвици исто како и профилирањето кое користи само човечки капацитети. Масовниот надзор управуван од ВИ истовремено значи и повреда на правото на приватност, со што се покренува и вечната дилема за тоа колку од нашата слобода сме ние како луѓе подготвени да отстапиме на сметка на тоа да бидеме побезбедни.

Пристрасноста во алгоритмите е уште една конфликтна тема. ВИ учи од нас, па така како што се луѓето пристрасни, и ВИ може да бидат со иста „карактерна особина“, со тоа што во контекст на технологија наместо човек, ваквиот пропуст би се класифицирал како маргинална грешка или вообичаен технолошки пропуст. Сепак, доколку множествата податоци се нецелосни, системите за вештачка интелигенција може да ги зајакнат стереотипите, непропорционално таргетирајќи одредени етнички или религиозни групи и доведувајќи до погрешно профилирање. Покрај ова, треба да се има предвид дека овие системи не се секогаш точни, тие системски може да бидат програмирани да имаат склоност кон таргетирање на

одредени групи, и не се доволно усовершени за да бидат онолку прецизни колку што е неопходно. Но, дури и во ваква состојба, тие се сепак сосема соодветни за брза обработка на податоци сè додека не се доусовршат за посложени задачи, а дотогаш покомплексните процеси ќе бидат оставени на човечките капацитети.

Можностите и потенцијалот на ВИ се чинат бесконечни и тука се воочува дека тоа на крајот од денот е само алатка, а дали е таа нужно добра или лоша е во зависност од оние кои ја употребуваат. Екстремистичките групи сè повеќе ја експлоатираат вештачката интелигенција за производство на пропаганда, дипфејкови и лажни содржини што имитираат легитимно новинарство или објави на социјалните медиуми од веродостојни извори. Од друга страна, агенциите за борба против тероризмот можат да ја користат вештачка интелигенција за следење онлајн радикализација, и идентификување сомнителни лица пред да се случи регрутирање, или да се реализира напад во физичкиот свет. Оваа динамика ја илустрира парадоксалната природа на вештачката интелигенција во тероризмот: таа е и оружје на екстремизмот и алатка против него.

4.4 Примена на ВИ во профилирање на тероризмот

Потенцијалот и степенот на успех кој ја нуди вештачката интелигенција доколку се примени во областа на профилирањето на тероризмот е исклучителен, како што посочуваат повеќе студии. Имено, во трудот насловен „Вештачка интелигенција и психолошко профилирање за проценка на ризик од насилство: Подобрување на точноста и справување со етичкиот предизвик“ на Илијан Кузманов од декември 2024 година⁵⁴, кој ја разгледува потенцијалната полза од вештачката интелигенција во психолошкото профилирање, кое може да се покаже како една од најмоќните алатки во областа на профилирањето. Во неговото истражување се наведени потенцијалите на ВИ и нагласува дека „Една од

⁵⁴ Iliyan Kuzmanov. (2024). AI and Psychological Profiling for Violence Risk Assessment: Enhancing Accuracy and Addressing Ethical Challenges, Volume 2, Issue 12. Достапно на: <chrome-extension://efaidnbnmnibpcajpegclefindmkaj/https://tjier.org/jnrid/papers/JNRID2412032.pdf>

најперспективните примени на вештачката интелигенција во оваа област е употребата на НЛП - Обработка на природен јазик (Natural Language Programming – NLP) за анализа на текстуални податоци за знаци на екстремистичка идеологија, говор на омраза и други индикатори за радикализација. НЛП техниките, како што се анализа на сентименти, моделирање на теми и класификација на текст, можат да се користат за автоматско идентификување и означување на потенцијално опасна содржина. На пример, моделите на вештачка интелигенција можат да бидат обучени да препознаваат јазични шеми поврзани со специфични екстремистички групи или идеологии, овозможувајќи рана идентификација на лица кои може да бидат изложени на ризик од радикализација. Ова вклучува истражување на целите, идеологиите и онлајн активностите на терористичките групи, идентификување на скриени автори и квантифицирање на нивоата на радикализација. Анализата базирана на мрежа ги користи метаподатоците и онлајн интеракциите за откривање на заедниците и клучните поединци. Понатаму, вештачката интелигенција може да се користи за анализа не само на содржината на онлајн комуникациите, туку и на мрежите и односите меѓу поединците. Техниките за анализа на социјалните мрежи можат да помогнат во идентификувањето на лица кои се централни за екстремистичките мрежи, како и оние кои може да бидат на периферијата и потенцијално ранливи на регрутирање.“

Важно е да се нагласи дека, кога се говори за научни истражувања, поголемиот број се за потенцијалот и примената на ВИ во профилирањето на тероризмот е насочено кон психолошкото профилирање и неговиот придонес во брзата обработка на податоци и анализа на јазични шеми, но тоа не мора да значи дека оваа алатка е корисна само на тоа поле. Во последниот пример е наведено дека ВИ е способно за анализа на објекти и просторна анализа што ни дава до знаење дека ВИ би било и тоа како од корист во географското профилирање.

4.4.1 Примена на ВИ во Македонија

Интеграцијата на вештачката интелигенција во безбедноста претставува софистицирана промена од традиционалното реактивно кон проактивно работење кое се темели на модел на алгоритамско управување, и ова е цел на сите држави и меѓународни организации, па така ова е и цел на Република Македонија.

Пред сè, важно е да се нагласи дека Македонија во моментот не користи наменски систем за вештачка интелигенција за профилирање на тероризмот на начин на кој експериментирале земји како што ќе видиме во понатамошниот труд. Наместо тоа, нејзината стратегија за борба против тероризмот е обликувана од нејзината позиција како земја-членка на НАТО и меѓународната соработка. Најновата Национална стратегија за борба против тероризмот (2023–2027) нагласува превенција, откривање и следење на радикализацијата, но тоа го прави првенствено преку хармонизација со стандардите на ЕУ и преку соработка со НАТО и други партнери.

Иако вештачката интелигенција не е сèуште имплементирана во безбедносните системи во Македонија, сепак таа се споменува во дискусии главно во контекст на сајбер безбедноста и дигиталната трансформација. Сепак, во моментот, вештачката интелигенција не е распоредена како самостоен систем за профилирање на тероризам, но и покрај ова треба да се истакнат технолошкиот напредок од оваа област, а како централен столб на оваа модернизација е Националниот центар за вештачка интелигенција „Везилка“⁵⁵, основан во октомври 2025 година. Иако се нагласува дека оваа алатка на вештачката интелигенција ќе служи за здравството и лингвистиката, центарот обезбедува високо-перформансна компјутерска инфраструктура неопходна за обработка на податоци во голем обем и во безбедносниот сектор. Овој развој ја илустрира секјуритизацијата на технологијата и му овозможува на Министерството за

⁵⁵ Дејан Соколоски (2025), „ВЕЗИЛКА: Од македонски LLM до паметно земјоделство – Како националната AI Factory Antenna ќе ја трансформира Македонија“, Достапно на: [ВЕЗИЛКА: Од македонски LLM до паметно земјоделство – Како националната AI Factory Antenna ќе ја трансформира Македонија * IT.mk](#)

внатрешни работи да се движат во правец на постепено намалување на степенот на рачно внесување податоци и поблиску кон анализа во реално време со помош на ВИ. Со користење на мрежата на европската фабрика за вештачка интелигенција „Фарос“, безбедносните агенции на Македонија добиваат технички капацитет да извршуваат сложени симулации и алгоритми за споредување на шеми кои претходно беа превентивни за ресурси.

Имплементацијата на овие технологии е силно модерирана од Законот за безбедност на мрежи и информациски системи, кој стапи на сила на 1 јануари 2026 година. Според оваа рамка, секоја алатка за профилирање што се користи за борба против тероризмот мора да помине низ проценка на влијанието врз основните права и законот налага овие системи да останат транспарентни. Ова осигурува дека државата ги избегнува негативните аспекти како што се нарушување на приватноста и основните права и слободи, кое е една од негативните страни на профилирањето.

Македонија засега нема развиено свој национален систем за профилирање на системот кој се темели на вештачката интелигенција, меѓутоа покажува знаци на развој и сериозен интерес за одење во таа насока. Со развивање на системот „Везилка“ кој, иако не е примарно насочен кон примена во безбедноста, е чекор во вистинската насока за понатамошна имплементација на ВИ во внатрешната и надворешната безбедност. Покрај ова, постои и свеста за негативните аспекти, како пречекорувања на правата и слободите на граѓаните и идеално ќе се вложат напори за креирање на баланс каде ќе се дигитализира процесот на профилирање и општото работење на институциите, а при тоа нема да се нарушат слободите и приватноста на граѓаните.

4.4.2 Системите АДАМС и ФАСТ на САД

Вештачката интелигенција (ВИ) отсекогаш претставувала алатка од исклучителна важност за безбедноста и борбата против тероризмот. Како доказ за

ова е еден од најраните примери употреба на ВИ во профилирањето на тероризмот, односно програмата АДАМС – Детекција на аномалии на повеќе нивоа (ADAMS – Anomaly Detection at Multiple Scales), развиена од Агенцијата за напредни истражувачки проекти за одбрана на САД (DARPA). Оваа програма започнала да функционира во 2011 година и завршила во 2014 година и нејзината основна задача била да открива внатрешни закани и потенцијална терористичка активност преку анализа на огромни количини на податоци.

Примарната цел на АДАМС била да идентификува необични модели или пак шеми на однесување кои би можеле да сигнализираат за потенцијална опасност, закана, обиди за напад и сл. На пример, можела да означи војник кој одеднаш покажувал знаци дека има намери за примена на насилство или вработен кој почнал да пристапува до чувствителни датотеки без причина. За да се постигне ова, АДАМС во голема мера се потпираше на техники на вештачка интелигенција. Алгоритмите за машинско учење биле користени за да се утврди како изгледа „нормалното“ однесување, а потоа да се откријат отстапувања од таа основна линија. Ова му овозможило на системот да забележи аномалии што луѓето би можеле да ги пропуштат.

Овој систем се состоел од неколку компоненти. Машинското учење и статистичките модели помогале при класификација на однесувањето како нормално или сомнително. Графичката и мрежната анализа ги мапирале социјалните врски и комуникациските модели и шеми, откривајќи скриени врски меѓу поединците, а Обработката на природен јазик (НЛП) ги испитувал пораките при електронска комуникација и барал промени во тонот или употреба на екстремистички јазик. На крајот на целата оваа анализа која на спроведува Системот, се добива една сеопфатна слика за лицето кое е предмет на истражување.

Силната страна на АДАМС била во неговата способност да работи на повеќе нивоа - од индивидуални дејства до цели организациски мрежи. Можел да обработува милијарди записи во реално време, нешто невозможно без вештачка интелигенција. Сепак, програмата, исто така, покренала сериозни етички

проблеми. Критичарите биле загрижени за потенцијалното нарушување на приватноста и недостатокот на транспарентност во начинот на кој алгоритмите донесуваат одлуки. Поради овие грижи, АДАМС престанал со работа во 2014 година, но земајќи предвид дека бил создаден во текот на 2010 година, далеку пред кој било од обичните луѓе да знаат што е ВИ и како таа се употребува, овој систем претставува еден вид зародиш на системите за профилирање кои се употребува денес, но и ВИ која ние ја употребуваме во нашето секојдневие. Воедно, ги покренала етичките и моралните дилеми за употребата на ВИ во која било област на безбедноста, грижи кои се присутни и денес.

Покрај програмата АДАМС (Детекција на аномалии на повеќе нивоа), постоела и програмата на Министерството за внатрешна безбедност, наречена ФАСТ – Технологија за скрининг на атрибути на иднината (FAST – Future Attribute Screening Technology). Иако и двете имале цел да предвидат и спречат закани, тие се потpirале на многу различни методи - АДАМС се фокусираше на анализа на бази на податоци, додека ФАСТ бил насочен кон биометриски и бихејвиорални знаци и показатели.

Програмата ФАСТ, развиена од Министерството за внатрешна безбедност, имала сосема поинаков пристап. Наместо да анализира дигитални податоци, таа имала цел да предвиди непријателска и/или насилна намера преку следење на биометриски и физиолошки сигнали во реално време. Оваа програма била тестирана на аеродроми и јавни простори, користејќи сензори за мерење на:

- Срцев ритам и дишење;
- Движења на очите и ширење на зениците;
- Изрази на лицето и говор на телото; и
- Анализа на стрес и напнатост во гласот.

Идејата била дека суптилните физиолошки промени би можеле да откријат стрес или зловна/насилна намера пред да се манифестира нападот. ФАСТ понекогаш се опишувал како систем кој бил чекор пред криминалот бидејќи бил добар во предвидување на истиот. Сепак, исто како во случајот со АДАМС, системот

се соочил со жестоки критики дека е несигурен, инвазивен и се покосувал со етички и морални норми. Загриженоста за граѓанските слободи и научната валидност довело до намалување на користењето и финансирање на програмата и на крајот прекинување на истата.

Заедно, АДАМС и ФАСТ илустрирале две различни насоки што ги презеле владите во користењето на вештачката интелигенција за профилирање на тероризмот. АДАМС го покажал потенцијалот на откривање на аномалии базирани на податоци, додека ФАСТ истражувал биометриско предвидување на намерата на сторителот. И двете програми го истакнувале потенцијалот на вештачката интелигенција во безбедноста, но исто така и ризиците од пристрасност, нарушување на приватноста и етички контроверзии. Нивното наследство нè потсетува дека иако вештачката интелигенција може да ја подобри борбата против тероризмот, таа мора да биде избалансирана со транспарентност и почитување на граѓанските слободи и права.⁵⁶

4.4.3 Единицата на ЕУ за упатување на интернет (ИРУ)

Системите на САД се сметаат за зародишот на употребата на ВИ во областа на профилирање на тероризмот, но дали постојат вакви системи во Европа? Накусо, одговорот е да. Како што екстремистичките организации сè повеќе ги користат онлајн платформите за ширење пропаганда, регрутирање членови и радикализирање на ранливи поединци, така се јавува потребата за одговор на сите овие закани. Така, Европската Унија (ЕУ) инвестирала во алатки за вештачка интелигенција кои би служеле за откривање, анализа и ограничување на екстремистичка содржина онлајн. Во овој напор клучна улога има ИРУ – Единицата

⁵⁶Broad Agency Announcement (2010), „Anomaly Detection at Multiple Scales (ADAMS)“, Достапно на: [ADAMS: Anomaly Detection at Multiple Scales | DARPA Microsoft Word - DARPA-BAA-11-04 ADAMS Waltzman .docx](#)

на ЕУ за упатување на интернет (IRU – EU Internet Referral Unit), основана во рамките на Европскиот центар за борба против тероризмот (ЕКТЦ) на Европол.

ИРУ била основана во 2015 година како дел од стратегијата на ЕУ за борба против тероризмот на интернет. Нејзината цел била е да открива, анализира и упатува јавно достапна терористичка и насилна, екстремистичка содржина до давателите на онлајн услуги за тие да ја отстранат истата. Со координација со земјите-членки и приватните компании, ИРУ се стремела да го намали лесниот пристап и општото присуство на екстремистичката пропаганда и да поддржува кривични истраги. Според Европол, ИРУ обработила десетици илјади упатувања, насочени кон содржина поврзана со групи како што се ИСИС и Ал Каеда.⁵⁷

Оваа алатка, слично на американската, употребува неколку методи во процесот на анализа на податоци, и тоа:

- НЛП - Обработка на природен јазик (Natural Language Programing – NLP);
- Препознавање на слики и видеа;
- Мрежна анализа; и
- Автоматизирани упатувања.⁵⁸

Овие алатки му овозможуваат на ИРУ да обработува огромни количини онлајн податоци, нешто што е невозможно само преку рачно следење.

При разгледување на ваквите системи важно е да се воочат позитивните и негативните аспекти. Насир Ахмед Ганаие во неговото дело „Улогата на вештачката интелигенција во радикализацијата, регрутирањето и терористичката пропаганда: деконструкција на насилниот екстремизам и преосмислување на борбата против тероризмот во современите дигитални екосистеми“ тврди дека вештачката

⁵⁷ Europol (2026), „EU Internet Referral Unit - EU IRU“, Europol.europa.eu (online), Достапно на: [EU Internet Referral Unit - EU IRU - Monitoring terrorism and violent extremism online | Europol](#)

⁵⁸ Serena Bianchi, Marina Mancuso, Caterina Paternoster, George Kalpakis, Theodora Tsirikli, Stefanos Vrochidis, Denitsa Kozhuharova, Bernhard Jaeger (2023), „Artificial Intelligence to Counter Cyber-Terrorism“, Достапно на: [ALLIES Artificial-Intelligence-to-Counter-Cyber-Terrorism CyberCon-2023-02.pdf](#)

интелигенција обезбедува „парадигматска промена“ во борбата против тероризмот со тоа што овозможува проактивно откривање на моделите на радикализација, но предупредува на ризиците од преголемо потпирање на непросирни алгоритми.⁵⁹

Според досегашните резултати, ИРУ била ефикасна во намалувањето на видливоста на екстремистичката содржина на интернет. Европол известува дека соработката со платформи како што се Фејсбук, Твитер и Јутјуб довела до отстранување на терористичка пропаганда. Сепак, критичарите тврдат дека самото отстранување не ги решава основните причини за радикализација. Екстремистичките групи често мигрираат на шифрирани платформи или развиваат нови стратегии за дисеминација, ограничувајќи го долгорочното влијание на отстранувањето на содржината.

Единицата за упатување на интернет на ЕУ претставува значаен чекор во интегрирањето на вештачката интелигенција во политиката за борба против тероризмот. Со искористување на НЛП, препознавање слики и анализа на мрежата, ИРУ го подобри капацитетот на ЕУ за следење и ограничување на екстремистичката содржина на интернет. Сепак, нејзиното потпирање на вештачката интелигенција покренува етички прашања, односно истите прашања кои се покренуваат при употребата на било кои системи кои се од ваков тип, без оглед дали употребуваат ВИ или не. Прашањата се поврзани со приватноста, пристрасноста и одговорноста ја нагласуваат потребата од транспарентност, интердисциплинарна соработка и заштитни мерки за да се осигура дека борбата против тероризмот управувана од вештачката интелигенција ги почитува правата на граѓаните.

Посекако можеме да констатираме дека ВИ е од исклучителна важност за за земјите-членки од Европската Унија и работеле на развивање на систем за анализа на податоци уште во 2015 година, повторно како случајот со Америка, далеку пред ВИ да биде актуелна тема и широко распространета алатка. ЕУ инвестирала во

⁵⁹ Nasir Ahmed Ganaie (2025), „The role of artificial intelligence in radicalisation, recruitment and terrorist propaganda: deconstructing violent extremism and reimagining counterterrorism in contemporary digital ecosystems“, frontiersin.org (online), Достапно на: [Frontiers | The role of artificial intelligence in radicalisation, recruitment and terrorist propaganda: deconstructing violent extremism and reimagining counterterrorism in contemporary digital ecosystems](https://www.frontiersin.org/articles/10.3389/fnins.2025.1542121/full)

систем кој анализира шеми и модели на однесување, јазик кој го употребуваат екстремисти и на овој начин се чекор пред оние кои сакаат да наштетат на земјите-членки.

4.4.4 Системи базирани на ВИ на Израел

Геополитичката положба на Израел уште од нејзините зачетоци како држава, барала софистицирани безбедносни протоколи и напредни системи. Опкружена со нестабилни граници и соочена со постојани терористички опасности, Израел има сериозно инвестирано во технолошкиот напредок за да го заштити своето население. Во последно време, вештачката интелигенција (ВИ) се појави како клучна компонента на пристапот на Израел во борбата против тероризмот, олеснувајќи го надзорот, биометрискиот мониторинг и автономните одбранбени механизми.

Израел има развиено дел од најсофистицираните системи базирани на вештачка интелигенција кои се поставени на контролни пунктови, гранични премини и по должината на границите на Газа и Западниот Брег. Овие системи интегрираат повеќе технологии како што се камери за надзор со вештачка интелигенција кои се опремени со препознавање лица и откривање аномалии, камери кои ги следат бегалските кампови, контролните пунктови и урбаните области. Нивната примарна цел е да идентификуваат лица означени во безбедносните бази на податоци и да детектираат сомнителни модели на однесување. Тие исто така, како што претходно беше споменато во случајот на САД, имаат биометриско следење кое се користи на граничните премини кои се потпираат на дата-бази за отпечатоци од прсти и препознавање на лица за да потврдат идентитети и да детектираат фалсификувани документи. Ова ја намалува

зависноста од рачни проверки и го забрзува процесот, а воедно ја подобрува безбедноста и ја намалува можноста за настанување на грешки.⁶⁰

Од аспект на практичното војување и имајќи го предвид конфликтот во кој учествуваше Израел, тие исто така развија автономни беспилотни летала и роботски оружја кои се оружје управувано од вештачка интелигенција и далечинско управување кое обезбедува следење во реално време и брз одговор на потенцијални упади. Овие системи можат да го следат движењето, да идентификуваат закани и да извршат прецизни напади кога истото ќе им биде одобрено од страна на оној кој ги управува. Овие системи користат предвидлива аналитика, што значи дека технологијата има алгоритми кои анализираат модели на движење, комуникациски сигнали и историски податоци за да можат да предвидат потенцијална терористичка активност. Овој предикативен елемент им овозможува на израелските сили да дејствуваат превентивно, а не реактивно.

Компании за одбрана како што се Smart-Shooter, Xtend, Robotican и ESC BAZ соработуваат со израелското Министерство за одбрана за да ги развијат овие технологии. Многу од овие системи се извезуваат глобално, што го прави Израел лидер во управувањето со границите управувано од вештачка интелигенција. Како примери за најпознатите оружја кои ги изработуваат овие компании се „SMASH Dragon“ од Smart-Shooter кој користи алгоритми за контрола на оган во реално време за да го насочи уредот на време и прецизно да погоди копнени или воздушни цели како што се беспилотни летала. Неговиот систем исто така може да следи и таргетира непознати објекти во непознати средини, без разлика дали се статични или динамични, или дење и ноќе и GoShawk, дизајниран од Robotican, кој е

⁶⁰ Ministry of Economy and Industry, Foreign Trade Administration (2024), „View Larger Image AI-Powered Border Management: The Israeli Innovation Driving Global Security and Humanitarian Solutions“, itrade.gov.il (online), Достапно на: [AI-Powered Border Management: The Israeli Innovation Driving Global Security and Humanitarian Solutions - India - Israel Trade & Economic Office, Embassy of Israel](#)

автономен дрон кој е дизајниран да фаќа и да презема непријателски дрoнови, наместо да ги пресретнува.⁶¹

4.5 Примена на ВИ од страна на терористички групи

Општо познато за терористичките организации е дека тие се склони кон употреба на нови технолошки иновации па дури и развивање иновации за реализација на нивните цели и потреби. Класичен пример за ова е употребата на онлајн форумите за ширење на пропаганда од страна на Ал Каеда. Подоцна овие активности преминуваат од форуми на социјални мрежи како Фејсбук, Твитер односно X, Инстаграм и Тик-Ток. Следствено на ова, нема потреба да се постави прашањето дали терористичките организации употребуваат вештачка интелигенција во текот на нивното дејствување, туку посоодветно би било да се запрашаме за што, односно во кои процеси конкретно ја применуваат оваа алатка и за кои цели.

Терористичките организации може да побараат вештачка интелигенција да им помогне при генерирање на пропагандни материјали како слики, видеа и текстови и да креираат пораки за разговор со лица кои терористите сакаат да ги регрутираат. Важно е да се напомене дека ВИ имаат вградени „бариири“ кои спречуваат тие да зборуваат за определени теми како изработка на бомби, експлозивни направи, оружје и насилство.

Во Москва, на 22 март 2024 година, по нападот на општинската зграда на Крокус, било објавено видео кое подоцна се воспоставило дека било генерирано со помош на ВИ. Поддржувачите на Исламската држава користеле вештачка интелигенција за да создадат видеото во кој се појавува индивидуалец генериран од вештачка интелигенција кој го слави нападот. Овој инцидент го нагласува

⁶¹Abigail Darwish (2024), „Tactical AI: How Israel is fortifying its National Security Capabilities“, bisi.org.uk (online), Достапно на: [Tactical AI: How Israel is fortifying its National Security Capabilities – Bloomsbury Intelligence and Security Institute \(BISI\)](https://bisi.org.uk)

усвојувањето на ВИ од страна на групата за производство на висококвалитетна пропагандна содржина, засилувајќи го нивното влијание и досег.⁶²

Дипфејковите исто така претставуваат една од поголемите закани. Тие можат да личат на одредени лица, предмети или настани и да изгледаат автентично. Дипфејковите стануваат сè пошироко распространети и сè потешки за разликување од автентична содржина, со што се олеснуваат незаконски и опасни активности. На пример, медиумска организација поврзана со Ал-Каеда ширела дезинформации и пропаганда што изгледало како да е создадена со помош на дипфејкови.⁶³

Корисноста на ВИ е воочена од терористичките организации така што таа може да се искористи за значително забрзување, подобрување и автоматизирање на процесот на погодување лозинки. Злонамерните актери би можеле да тренираат невронски мрежи со овие огромни онлајн бази на податоци за лозинки, што пак може да генерира посоефицирани варијации на лозинки отколку што луѓето би можеле да замислат. Овие невронски мрежи потоа би можеле да извршуваат повеќе обиди еден по друг додека не се утврди решение, со што се ублажува потребата од директно вклучување на хакер. Во една студија од 2017 година, истражувачите внеле десетици милиони протечени лозинки во невронска мрежа задолжена за генерирање нови лозинки. Овие лозинки потоа биле вкрстени со протечени лозинки од страници како што е LinkedIn, со цел да се измери колку успешна би била невронската мрежа во пробивањето на лозинките на корисниците. Студијата покажала дека тие биле во можност да пробијат 27% од лозинките во сетот LinkedIn. Последователна студија покажала дека вештачката интелигенција може да погоди лозинка со откривање кои лозинки се пишуваат врз основа на движењата на рамената анализирани за време на видео повици. Резултатите од студијата покажаа дека софтверот за вештачка интелигенција за кој станува збор имал алармантна

⁶² Shai Farber (2025), „AI-Enabled Terrorism: A Strategic Analysis of Emerging Threats and Countermeasures in Global Security“ стр. 330, Journal of Strategic Security 18, no. 3, Достапно на: [AI-Enabled Terrorism: A Strategic Analysis of Emerging Threats and Countermeasures in Global Security](#)

⁶³ Asha Hemrajani (2024), „The Use of AI in Terrorism“, стр. 2, RSIS Commentary, Достапно на: [The Use of AI in Terrorism.pdf](#)

стапка на точност од 75% до 93%.⁶⁴Ваквата технологија може да биде злоупотребена од страна на терористички организации не само за пробивање на лозинки на обични граѓани, туку и на административни службеници во која било државна институција или приватна фирма.

ВИ не само што претставува потенцијална алатка која може терористите да ја употребуваат, туку тековно ја користат уште од нејзината појава. Неоспорлив е нејзиниот потенцијал во здравството, образованието и општото секојдневие, но сепак нејзината злоупотреба од страна на терористичките и екстремистичките организации предизвикува сериозна загриженост. Клучно е што современите системи со ВИ се создадени со веќе интегрирани заштитни мерки што ги спречуваат терористите директно да употребуваат ВИ за да создаваат бомби или други видови оружје, но наместо тоа тие ја користат ВИ за измама, регрутирање на нови членови и ширење пропаганда. Од наведените области, најистакната злоупотреба се пропагандата и регрутирањето. Генеративните способности на ВИ им овозможуваат на екстремистите да произведуваат убедливи лажни видеа и слики, односно дипфејк. Овие материјали можат да се користат за радикализирање на нови потенцијални членови, следбеници и симпатизери, величење насилство и промовирање на нивните екстремистички, политички и религиозни доктрини. За разлика од традиционалната пропаганда, содржината генерирана од ВИ може да се произведува во голем обем, на повеќе јазици и со ниво на реализам што им отежнува на обичните корисници да одредат која содржина е реална, а која не. Ова им помага на овие организации да шират лажни наративи со толку забрзано темпо што владите и светските организации кои се борат против терористите, ќе се спротивставуваат со големи потешкотии.

⁶⁴ UNICRI, UNCCT (2021), „Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes“, Достапно на: [Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes | UNICRI :: United Nations Interregional Crime and Justice Research Institute](#)

4.6 Анализа на законот за безбедност на мрежни и информациски системи

Законите се тие кои не штитат од заканите во средината која не опкружува. Воедно, тие се границата која ние самите не смееме да ја пречекориме. На овој начин се воспоставува ред во општествената заедница. Заштитата е неопходна во физичкиот свет, но и во виртуелниот и тука постои дилемата колку ние сме заштитени од ВИ доколку се употребуваат од страна на терористички и/или криминални групи, и општо виртуелните закани. За понатамошно разјаснување на оваа проблематика се зема предвид Законот за безбедност на мрежни и информациски системи, кој Собранието на Република Македонија го донесе на седницата одржана на 27 јуни 2025 година.

Согласно член 1 од овој закон, се уредува кои органи се надлежни за оваа област, како се управува со големи или значајни сајбер инциденти, и кој ја сноси одговорноста. Законот предвидува формирање тимови за одговор на компјутерски инциденти, пропишува мерки за заштита и управување со ризик, и воведува обврска сите правни лица кои обезбедуваат критични услуги – како енергетика, транспорт, здравство или финансии – да известуваат за инциденти и да разменуваат информации. Дополнително, тој бара усвојување стратегија за сајбер безбедност и воспоставува надзор за да се осигура дека правилата навистина се спроведуваат. Целите на Законот, согласно член 2 се поврзани со изградба на капацитети за заштита на мрежните и информациски системи, да се намалат заканите кои можат да ја загрозат критичната инфраструктура, и да се обезбеди континуитет на основните услуги дури и во случај на напад или инцидент.

Законот за безбедност на мрежните и информациски системи има многу широк опфат и ги зема предвид: приватниот сектор како телекомуникациски компании, даватели на доверливи услуги, управувачи на домени, сопственици на критичка инфраструктура, приватни здравствени установи, и јавниот сектор со клучните институции (Влада, Собрание, министерства, судови, општини и нивни управни органи), и критичната инфраструктура (електрика, транспорт, здравство, водовод и канализација, производство и сл.). Накусо, законот ги опфаќа сите сектори и области, но со некои исклучоци, како што се органите за безбедност и

одбрана (Министерство за внатрешни работи, Агенција за национална безбедност, Агенција за разузнавање, Министерство за одбрана, Јавно обвинителство, Оперативно-техничка агенција и дирекција за класифицирани информации), Истото се однесува за Народната банка, но само во ситуации кога овие органи или нивните даватели на услуги обезбедуваат доверливи услуги (на пример, дигитална идентификација или електронски потпис). Во ваквите случаи законот важи и за нив.

Законот за безбедност на мрежните и информациски системи одредува два главни столба кои ја штитат државата од сајбер закани. Првиот е Министерството за дигитална трансформација, кој ја пишува стратегијата, предлага планови, дава упатства и протоколи, собира информации за инциденти и врши надзор над институциите. Министерството е и централна точка на контакт и воедно делува како специјален тим за одговор на компјутерски инциденти за органите на извршната власт. Вториот столб е Агенцијата за електронски комуникации преку MKD-CIRT, која е единица што реагира на напади и инциденти. Таа е задолжена за Собранието, судовите, регулаторните тела и сите компании од критичните области – енергетика, транспорт, здравство, банкарство, дигитална инфраструктура и други. MKD-CIRT се првите кои одговараат кога се пројавува некаков проблем, аномалија или закана.

Законот предвидува и широка соработка – Министерството мора да работи со домашни институции (како оние за безбедност, заштита на лични податоци, банкарски сектор, кризни управувања) и со меѓународни организации. Особено важна е врската со ЕУ и НАТО, преку ENISA и EU-CyCLONe, што ја става Македонија во европската и глобалната мрежа за сајбер безбедност.

Предвидени во Законот се санкции доколку не се постапува согласно насоките на истиот. Имено, компаниите и институциите што се дел од критичната инфраструктура мора да бидат одговорни – доколку не известат за напад, доколку не ги информираат граѓаните, или доколку не преземаат мерки, тогаш ќе се соочат со високи казни и забрана за работа.

Законот не е насочен кон заканите, нивната природа и како тие се прогонуваат и казнуваат, туку говори за тоа како институциите треба да се штитат себеси, како да функционираат и постапуваат во случај на сајбер инцидент и каде треба да се обратат. Во таа насока се забележува дека, иако со новодонесениот закон се додава нов слој на одбрана на институциите и механизми за реакција при појава на некоја од овие сајбер закани, нема конкретни нови закони кои зборуваат за казнување на сторители на вакви кривични дела и на ова поле има сериозни пропусти и недостатоци. За дополнително појаснување на оваа проблематика се повикувам на неколку одредби од Кривичниот законик на Македонија, и тоа:

- „**Тероризам“ Член 394-б:** „ Тој што ќе изврши едно или повеќе дела на убиство, телесно повредување, грабнување лица, уништување на јавните објекти, транспортни системи, објекти на инфраструктура, компјутерски системи и други објекти за општа употреба, грабнување авиони или други средства за јавен транспорт, производство, поседување, транспорт, трговија, набавка или примена со нуклеарно оружје, биолошки, хемиски оружја и други видови оружја и опасни материи, како и истражувања во насока на развој на биолошко и хемиско оружје, пуштање опасни радиоактивни, отровни и други опасни супстанции, или предизвикување пожар или експлозија, уништување постројки за снабдување со вода, енергија или други основни природни извори, со намера за загрозување на животот и телото и создавање чувство на несигурност или страв кај граѓаните, ќе се казни со затвор најмалку десет години, или со доживотен затвор. “ Во став (2) продолжува: „ Тој што сериозно ќе се закани со извршување на делото од ставот (1) на овој член непосредно или посредно, со употреба на електронски средства или на друг начин, со намера за загрозување на животот и телото и создавање чувство на несигурност или страв кај граѓаните, ќе се казни со затвор најмалку осум години.“ Овој член ги покрива заканите по компјутерските системи и кои било други ненаведени дејствија преземени со електронски средства чија намера е загрозување на животот и создавање чувство на страв кај граѓаните и може да се имплементира во контекст на сајбер закана, но земајќи ги предвид трендовите во светот и степенот на брзо развивање на технологиите, неопходно е надополнување на овој закон и споменување конкретно на сајбер заканите од терористичките организации

и поединци, или засебен член од Кривичниот законик посветен на ова дело, наспрема оставање простор за слободна интерпретација. Со други зборови, постои недостаток на конкретизација за сајбер заканите општо, а потоа и сајбер заканите предизвикани од терористи.

- **„Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем“ Член 394-г став 1:** „Тој што преку компјутерски систем во јавноста шири расистички и ксенофобичен пишан материјал, слика или друга репрезентација на идеја или теорија која помага, промовира или поттикнува омраза, дискриминација или насилство, против кое било лице или група, врз основа на раса, боја на кожа, национално или етничко потекло, како и верско уверување, ќе се казни со затвор од една до пет години.“;

- **„Оштетување и неовластено навлегување во компјутерски систем“ Член 251: (1)** Тој што неовластено ќе избрише, измени, оштети, прикрие или на друг начин ќе направи неупотреблив компјутерски податок или програма или уред за одржување на информатичкиот систем или ќе го оневозможи или отежне користењето на компјутерски систем, податокот или програмата, или на компјутерска комуникација, ќе се казни со парична казна, или со затвор до три години;**(2)** Со казната од став (1) ќе се казни и тој што неовластено ќе навлезе во туѓ компјутер или систем со намера за искористување на неговите податоци или програми заради прибавување противправна имотна или друга корист за себе, или за друг, или предизвикување имотна или друга штета, или заради пренесување на компјутерските податоци што не му се наменети и до кои неовластено дошол на неповикано лице;**(3)** Со казната од ставот (1) на овој член ќе се казни тој што неовластено ќе пресретне, со употреба на технички средства, преносна компјутерски податоци кој нема јавен карактер до, од, и внатре во одреден компјутерски систем, вклучувајќи и електромагнетни емисии од компјутерски систем кој поддржува такви компјутерски податоци;**(4)** Тој што делата од ставовите (1) (2) и (3) на овој член ќе ги стори спрема компјутерски систем, податоци или програми кои се заштитени со посебни мерки на заштита, или се користат во работењето на државни органи, јавни претпријатија или јавни установи, или во меѓународни комуникации, или како член на група создадена за

вршење такви дела, ќе се казни со затвор од една до пет години; **(5)**. Ако со делото од ставовите (1) (2) и (3) на овој член е прибавена поголема имотна корист или е предизвикана поголема штета, сторителот ќе се казни со затвор од шест месеци до пет години; **(6)**. Ако со делото од став 3 е прибавена поголема имотна корист, или е предизвикана поголема штета, сторителот ќе се казни со затвор од една до десет години; **(7)**. Тој што неовластено изработува, набавува, продава, држи или прави достапни на друг посебни направи, средства, компјутерска лозинка, код за пристап и сличен податок со кој целината, или дел од компјутерскиот систем се оспособува за пристап, компјутерски програми, или компјутерски податоци наменети, или погодни за извршување на делата од ставовите (1), (2) и (3) на овој член, ќе се казни со парична казна, или со затвор до една година; **(8)**. Обидот за делото од ставовите (1) и (2) е казнив; **(9)**. Ако делото од овој член го стори правно лице, ќе се казни со парична казна; **(10)**. Посебните направи, средства, компјутерски програми, или податоци наменети за извршување на делото ќе се одземат;

- **„Правење и внесување компјутерски вируси“ Член 251-а: (1)**. Тој што ќе направи, или ќе преземе од друг компјутерски вирус со намера за внесување во туѓ компјутер, или компјутерска мрежа, ќе се казни со парична казна, или со затвор до една година; **(2)**. Тој што со употреба на компјутерски вирус ќе предизвика штета во туѓ компјутер, систем, податок или програма, ќе се казни со затвор од шест месеци до три години; **(3)**. Ако со делото од став (2) е предизвикана поголема штета или, делото е сторено во состав на група создадена за вршење такво дело, сторителот ќе се казни со затвор од една до пет години; **(4)**. Обидот за делото од став (2) е казнив; **(5)**. Ако делото од овој член го стори правно лице, ќе се казни со парична казна;

- **„Компјутерска измама“ Член 251-б: (1)**. Тој што со намера за себе, или за друг да прибави противправна имотна корист со внесување во компјутер или информатички систем невистинити податоци, со невнесување на вистинити податоци, соменување, бришење или прикривање компјутерски податоци, со фалсификување на електронски потпис, или на друг начин ќе предизвика невистинит резултат при електронската обработка и преносот на податоците, ќе се казни со парична казна, или со затвор до три години; **(2)**. Ако сторителот прибавил

поголема имотна корист, ќе се казни со затвор од три месеци до пет години; **(3)**. Ако сторителот прибавил значителна имотна корист, ќе се казни со затвор од една до десет години; **(4)**. Тој што делото од став (1) ќе го стори само со намера да оштети друг, ќе се казни со парична казна, или со затвор до една година; **(5)**. Ако со делото од став (4) е предизвикана поголема штета, сторителот ќе се казни со затвор од три месеци до три години; **(6)**. Тој што неовластено изработува, набавува, продава, држи, или прави достапни на друг посебни направи, средства, компјутерски програми, или компјутерски податоци наменети за извршување на делото од став 1, ќе се казни со парична казна, или со затвор до една година; **(7)**. Обидот за делото од ставовите (1) и (4) е казнив; **(8)**. Ако делото од овој член го стори правно лице, ќе се казни со парична казна; **(9)**. Посебните направи, средства, компјутерски програми, или податоци наменети за извршување на делото ќе се одземат; **(10)**. За делото од став (4) гонењето се презема по приватна тужба.

Согласно погоренаведената анализа на законите од Кривичниот законик и новодонесениот Закон за безбедност на мрежни и информациски системи, се констатира дека во Македонија, заклучно со првата половина од 2026 година, нема закон кој конкретно е насочен кон вештачката интелигенција, нејзината употреба и примена во рамките на институции, како и кривични дела кои јасно и недвосмислено се изведени со помош на вештачка интелигенција, со акцент на терористички активности од каков било вид.

Покрај законските рамки и регулативи важно е да се акцентира дека сè уште нема проекти и активности кои одат во насока на подигнување на институционалната и општата свест за постоење профили на социјални мрежи кои се профилни слики и објави генерирани со помош на ВИ, дипфејкови, кои се употребуваат за реализација на измами, изнуда, лажно претставување, и во контекст на тероризмот, регрутација, врбување, манипулирање и др. Онлајн регрутација со помош на ВИ генерирани профили и пораки па сè до употреба на ВИ при осмислување идеологии и доктрини, планирање и координирање напади, па дури и реализацијз, претставуваат теми за кои мора да постојат обуки за лица вработени на раководни позиции и останати кадри, доколку Македонија и општо која било држава, сака да даде соодветен и навремен одговор на овие закани.

Законите само по себе не значат многу доколку немате обучен и образован тим кој може истите да ги спроведе и тука веќе не станува збор само за правосудниот систем, туку системот на државата како целина. Без оглед за каква закана станува збор, доколку државата сака да даде сеопфатен, навремен, точен, јасен и прецизен одговор, потребни се институционална координација, јасна хиерархиска поставеност, недвосмислени закони и навремени одговори. Во спротивно, тероризмот ќе биде секогаш чекор понапред.

4.7 Актот за ВИ на Европска Унија

Согласно 2026 година, постојат над 70 држави кои имаат поставено некакви регулативи, закони, подзаконски акти и акциони планови кои говорат за вештачката интелигенција, како треба да се регулира, класифицира, употребува и ограничува. Помеѓу нив се наоѓаат и државите-членки на Европската Унија кои пројавуваат голем интерес во доменот на вештачката интелигенција.

Регулативата за вештачка интелигенција на Европската Унија⁶⁵, формално усвоен на 13 јуни 2024 година, претставува прва, хоризонтална и сеопфатна законска рамка во светот за регулирање на вештачката интелигенција. Оваа регулатива е продукт на тригодишна работа која започнува со негово предложување на Европската комисија во април 2021 година и конечното усвојување на 13 јуни 2024 година. Карактеристично за него е тоа што Регулативата е хоризонтална по природа и важи и ќе се применува исто за секој систем на вештачка интелигенција ставен на пазарот или ставен во употреба во рамките на Унијата, без оглед на тоа дали давателот на услуги е со седиште во ЕУ, или во трета земја. Овој екстра територијален дострел гарантира дека секој субјект кој сака да пристапи до Европскиот пазар мора да се придржува до определени безбедносни и етички стандарди, кои се регулирани со оваа Регулатива. Со ова се зајакнува улогата

⁶⁵ EU(2024), „REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL“, Достапно на: [Regulation - EU - 2024/1689 - EN - EUR-Lex](#)

на ЕУ како организација чија примарна цел и основен темел е економијата и економскиот систем.

Централниот столб на Регулативата е пристапот базиран на ризик. Тоа значи дека степенот на регулирање се заснова на тоа колкав е ризикот од штета кој би се предизвикал доколку се случи некаков пропуст. Оние системи кои се со низок ризик остануваат во голема мера нерегулирани, додека оние кои се со висок степен на ризик ќе подлежат под построг надзор. На крајот се оние кои подлежат на неприфатлив ризик и истите, согласно член 26 се целосно забранети.

Согласно повеќепати споменатата дилема во доменот на профилирањето, поконкретно моралните и етичките проблематики, во рамките на Регулативата, член 31, јасно стои дека: „ Системите за вештачка интелигенција кои обезбедуваат социјално бодување на физички лица од страна на јавни или приватни актери може да доведат до дискриминаторски резултати и исклучување на одредени групи. Тие може да го прекршат правото на достоинство и недискриминација и вредностите на еднаквост и правда. Ваквите системи за вештачка интелигенција ги оценуваат или класифицираат физичките лица или нивните групи врз основа на повеќе точки на податоци поврзани со нивното социјално однесување во повеќе контексти или познати, заклучени или предвидени лични или карактеристики на личноста во одредени временски периоди. Социјалниот резултат добиен од таквите системи за вештачка интелигенција може да доведе до штетен или неповолен третман на физичките лица, или цели нивни групи во социјални контексти, кои не се поврзани со контекстот во кој податоците првично се генерирани или собрани или до штетен третман кој е непропорционален или неоправдан во однос на сериозноста на нивното социјално однесување. Затоа, системите за вештачка интелигенција кои вклучуваат такви неприфатливи практики на бодување и водат до такви штетни или неповолни резултати треба да бидат забранети. Таа забрана не треба да влијае на законските практики за евалуација на физичките лица кои се спроведуваат за одредена цел во согласност со законодавството на Унијата и националното право.“ Регулативата во овој поглед е многу јасна и го забранува и остро го осудува користењето на ВИ за поставување на претпоставки и ставови за дефинирани

„физички лица“ врз основа на минато однесување и показатели бидејќи тоа може да нанесе штета врз истите тие лица и може да доведе до погрешни резултати.

Понатаму во член 42: „Во согласност со презумпцијата на невиност, физичките лица во Унијата секогаш треба да се оценуваат според нивното вистинско однесување. Физичките лица никогаш не треба да се оценуваат според однесување предвидено од вештачка интелигенција, само врз основа на нивното профилирање, особини или карактеристики на личноста, како што се националност, место на раѓање, место на живеење, број на деца, ниво на долг, или вид автомобил, без основано сомнение дека тоа лице е вклучено во криминална активност, врз основа на објективни проверливи факти и без човечка проценка на истите. Затоа, проценките на ризик што се спроведуваат во однос на физички лица со цел да се процени веројатноста за нивно кривично дело, или да се предвиди појава на вистинско, или потенцијално кривично дело, само врз основа на нивно профилирање, или врз основа на проценка на нивните особини и карактеристики на личноста, треба да бидат забранети. Во секој случај, таа забрана не се однесува ниту допира до аналитика на ризик што не се базира на профилирање на поединци, или на особини и карактеристики на личноста на поединци, како што се системите за вештачка интелигенција кои користат аналитика на ризик за да ја проценат веројатноста за финансиска измама од страна на претпријатијата врз основа на сомнителни трансакции, или алатки за анализа на ризик за да ја предвидат веројатноста за локализација на наркотици, или недозволена стока од страна на царинските органи, на пример врз основа на позната рута на трговија.“ Ова е првиот член кој е директно насочен кон профилирањето со употреба на ВИ и кога смее, а кога не смее да се употребува. Односно, во областа на аналитиката и анализа на ризик, доколку профилите се засноваат на факти и фактичка состојба, веќе-сторени дела и објективно проверливи факти, употребата на ВИ во профилирањето е целосно дозволено. Во спротивно, кога ВИ наместо со факти, се служи со податоци, кои според Регулативата се ирелевантни и дискриминарни, како што се раса, пол, возраст, сексуална ориентација, социо-економски статус и слично, се забранети бидејќи при процесот на истражна постапка секое лице се презумпционира како

невино и која било одлука донесена врз основа на вакви дискриминаторни показатели се коси со таа претпоставка.

Понатаму, со цел дополнително да се избегне потенцијална дискриминација, во Регулативата се нагласува биометриското профилирање. Оттука во член 30: „Треба да се забранат системи за биометриска категоризација кои се базираат на биометриски податоци на физички лица, како што се лицето, или отпечатокот од прст на поединецот, за да се заклучат или констатираат политичките мислења, членството во синдикат, религиозните или филозофските верувања, расата, сексуалниот живот или сексуалната ориентација на поединецот. Таа забрана не треба да го опфаќа законското етикетирање, филтрирање или категоризација на биометриски збирки податоци стекнати во согласност со законодавството на Унијата или националното право, според биометриските податоци, како што е сортирање слики според бојата на косата или бојата на очите, кои на пример можат да се користат во областа на спроведувањето на законот“.

Воглавно, Унијата е доста внимателна кога станува збор за профилирањето со помош на ВИ и општата употреба на ВИ и како треба да се употребува и регулира со цел да се избегнат негативните аспекти, односно дискриминацијата. Меѓутоа, во Регулативата е исто така, покрај биометриското профилирање кое се заснова на физички карактеристики, се споменува емоционално профилирање кое се базира на физички показатели, наведено во член 18: „Поимот „систем за препознавање емоции“ наведен во оваа Регулатива треба да се дефинира како систем на вештачка интелигенција со цел идентификување, или заклучување на емоции, или намери на физички лица врз основа на нивните биометриски податоци. Поимот се однесува на емоции, или намери како што се среќа, тага, лутина, изненадување, гадење, срам, возбуда, срам, презир, задоволство и забава. Не вклучува физички состојби, како што се болка или замор, вклучувајќи на пример, системи кои се користат за откривање на состојбата на замор кај професионални пилоти, или возачи со цел спречување несреќи. Ова исто така не вклучува само откривање на лесно очигледни изрази, гестови или движења, освен ако не се користат за идентификување, или заклучување емоции. Тие изрази можат да бидат основни изрази на лицето, како што се мрштење или насмевка, или гестови како што се движење на рацете, рацете

или главата, или карактеристики на гласот на една личност, како што е подигнат тон на гласот, или шепотење.“ Ваквите системи за детекција на емоција може да бидат корисни во полициското работење и поконкретно во контекст на профилирањето на тероризмот, но би можеле и да бидат многу злоупотребувани доколку нема граница за нивна употреба. Попрецизно, во членот 44 е наведено токму тоа: „Постојат сериозни загрижености во врска со научната основа на системите на вештачка интелигенција кои имаат цел да идентификуваат, или заклучат емоции, особено затоа што изразувањето на емоциите значително варира низ културите и ситуациите, па дури и во рамките на една индивидуа. Меѓу клучните недостатоци на ваквите системи се ограничената сигурност, недостатокот на специфичност и ограничената генерализација. Затоа, системите со вештачка интелигенција кои идентификуваат, или заклучуваат емоции, или намери на физички лица врз основа на нивните биометриски податоци може да доведат до дискриминаторски резултати и можат да бидат нарушувачки за правата и слободите на засегнатите лица. Со оглед на нерамнотежата на моќ во контекст на работата или образованието, во комбинација со наметливата природа на овие системи, ваквите системи би можеле да доведат до штетен, или неповолен третман на одредени физички лица, или цели нивни групи. Затоа, пласирањето на пазарот, пуштањето во употреба, или употребата на системи со вештачка интелигенција наменети за откривање на емоционалната состојба на поединци во ситуации поврзани со работното место и образованието, треба да биде забрането. Таа забрана не треба да ги опфаќа системите со вештачка интелигенција пласирани на пазарот строго од медицински, или безбедносни причини, како што се системите наменети за терапевтска употреба“.

Регулативата на Европската Унија, која претставува камен-темелник за употребата на вештачката интелигенција, претставува една од најсеопфатните регулативи кои се досега донесени. Во неа се истакнати предностите и недостатоците на оваа технологија, како таа може да придонесе за побрзо работење, детекција и реакција, но истовремено не се обидува да ги прекрие негативните аспекти како дискриминацијата и моралните и етичките дилеми. Наместо тоа, таа ги нагласува и овозможила отворање дискусија за истите и наоѓа решенија за нив.

Преку ограничување на степенот на надзор, граѓаните се чувствуваат побезбедно и послободно, а при тоа на ВИ ѝ е овозможено да ја извршува нејзината функција, т.е. обработка на обемен збир податоци за краток временски период со голем процент на прецизност.

Исто така, Регулативата става акцент и на профилирањето како метод и како може ВИ да биде од корист, без при тоа да генерализира и да се почитува претпоставката за невиност и недискриминација врз основа на биометриски карактеристики и да се носат претпоставки кои можат да ги нарушат честа, и угледот на граѓанинот.

Поради сето ова, оваа Регулатива е одличен пример за тоа како Македонија може да создаде систем кој ја користи ВИ како алатка, без притоа да наштети врз правосудниот, социјалниот, и економскиот систем на државата.

4.8 Предности и недостатоци од користење на ВИ во профилирање на тероризмот

Интеграцијата на вештачката интелигенција (ВИ) во борбата против тероризмот и профилирањето на тероризмот претставува една од најзначајните промени во областа на безбедност. Додека се справуваме со сложеноста на ерата на дигитализацијата, сликата на глобалната безбедност е неповратно изменета поради способноста на машините да анализираат многубројни податоци, идентификувајќи обиди за радикализација што би останале невидливи за човечкото око. Оваа технолошка еволуција не е само квантитативно подобрување на брзината на анализа на податоци, туку и квалитативна трансформација во начинот на кој државата ги перцепира и предвидува заканите. Сепак, оваа моќ доаѓа со длабок сет од етички, социјални и правни дилеми. Движењето кон алгоритамско профилирање е меч со две острици што ветува побезбеден свет, а истовремено ги загрозува основните принципи на приватноста, еднаквоста и претпоставката дека сите се невини се додека не се докаже спротивното.

Примарниот аргумент во корист на профилирањето на тероризмот со употреба на ВИ лежи во неговиот невиден капацитет за синтеза на податоци. Во современата ера, дигиталниот отпечаток⁶⁶ на поединецот е огромен, опфаќајќи финансиски трансакции, патни евиденции, интеракции на социјалните медиуми, па дури и метаподатоци од шифрирани комуникации. За човечките аналитичари, самиот обем на овие информации е огромен, што доведува до застој во истражната постапка или случајно изоставување на критични информации. Системите за вештачка интелигенција, особено оние што користат длабоко учење и невронски мрежи, се со неспоредливи резултати во овој домен. Тие се способни да идентификуваат нелинеарни шеми - суптилни шеми на однесување кои, кога се гледаат изолирано, изгледаат бенигни, но кога се анализираат подетално, укажуваат на голема веројатност за мобилизација и радикализација.

Понатаму, профилирањето со вештачка интелигенција нуди предност при следење во реално време. За разлика од човечките капацитети кои подложат на замор, глад, пристрасност и сл. ВИ работи континуирано без потреба од пауза од која било причина, освен секако во ситуации кога ќе има застој од некои технички причини како немање мрежно поврзување и дефекти. Покрај обработка и анализа на податоци онлајн, важно е и биометриско профилирање во реално време. Овие системи не бараат само лица врз основа на слика и отпечаток од прст, тие се способни и да анализираат одење, мали промени во изразот на лицето и аномалии во однесувањето што укажуваат на стрес, напнатост или обиди за прикривање и потиснување агресија. Брзината на овие системи и степенот на прецизност го прави профилирањето да биде алатка која се користи пред да настане штетата, а не по неа. Ова придонесува за повисок степен на безбедност и сигурност на индивидуално и светско ниво.

Вештачката интелигенција се истакнува во анализата на терористички групи, анализа на нивни минати напади, предвидување на идни активности, локации, лица и сл. Меѓутоа, ВИ е доста корисна алатка и за анализа на терористички мрежи на макро ниво. Феноменот волк-самотник кој доминираше

⁶⁶ Единствена, уникатна трага од податоци што ја оставате зад себе додека сте на интернет.

како една од поголемите закани кога стануваше збор за теорирзмот, иако е сè уште присутен, делумно се заменува со индивидуи кои дигитално се радикализираат преку форуми кои се онлајн, на веб-страни и социјални медиуми. Тие можат да дејствуваат сами, но да се во комуникација со истомисленици и на овој начин се создаваат ќелии кои се меѓуповрзани, можеби се консултираат, но не дејствуваат заедно туку претендираат одделно и се особено тешки за следење и поради тоа потребни се голем број експерти и човечки капацитети, и финансии. Употребата на ВИ овозможува поефикасна распределба на ограничените безбедносни ресурси. Во ерата на стеснување на буџетите, економска криза и глобална нестабилност, разузнавачките агенции не можат да бидат насекаде одеднаш. Моделите на вештачка интелигенција можат да генерираат мапа на потенцијална екстремистичка активност врз основа на геополитички промени, економски показатели и ширење на специфични екстремистички наративи. Ова гарантира дека се применува највисоко ниво на контрола таму каде што ризикот е објективно највисок, потенцијално намалувајќи го целокупниот надзор врз пошироката јавност. Сепак, транзицијата од човечко кон алгоритамско профилирање полна е со значајни ризици, од кои најзначајна е алгоритамската пристрасност. Системите со вештачка интелигенција не се по природа неутрални. Тие се одраз на податоците што се користат за нивна обука. Ако податоците за борба против тероризмот се пристрасни кон определени групи и лица, кон специфични етнички, религиозни или географски и демографски податоци, вештачката интелигенција ќе учи и ќе ги засили тие предрасуди. Во пракса, ова може да доведе до ситуација каде што одредени заедници се непропорционално означени како високо ризични не поради нивните постапки, туку затоа што делат карактеристики со поранешни престапници. Ова создава свет каде што невини поединци се наоѓаат под постојан надзор, подложени на бесправно основана контрола, или дури им се одбиваат услуги врз основа на проценка што не можат ниту да ја видат, ниту да ја оспорат. Кога човечки аналитичар носи одлука за профилирање, постои синџир на команда и образложение кое може да се ревидира. Спротивно на тоа, моделите кои се темелат на ВИ честопати доаѓаат до заклучоци без разјаснување како дошле до крајниот продукт кои тие го приложуваат. Овој недостаток на објаснување го прави речиси невозможно лицето кое е обвинето да ја докаже својата невиност, или

државата да обезбеди правно оправдување за својата интервенција. На овој начин се поткопува демократскиот темел на една држава и правата и законите се ставаат под знак прашалник само затоа што вештачката интелигенција се изјаснила дека определено лице е виновно или не, без давање појаснување за тоа како дошла програмата до таков заклучок.

За вештачката интелигенција да биде ефикасна, ѝ е потребен постојан прилив на податоци со висока точност. Ова исто така значи дека на државата и е потребно да изведува поголем степен на надзор над своите граѓани и нивните приватни животи. Ова го нагласува парадоксалното прашање кое постојано се јавува во безбедноста, а кое гласи: Колку сме ние подготвени да отстапиме од нашата приватност за да бидеме побезбедни, и дали таа безбедност вреди доволно за да направиме толкава отстапка? Во потрагата по апсолутна безбедност, државата може да ги уништи токму слободите што се стреми да ги заштити. Психолошкото влијание на живеењето под лупа не може да се потцени. Може да доведе до момент каде што поединците избегнуваат да дискутираат за чувствителни политички теми, да посетуваат одредени веб-страници, или да се дружат со определени групи од страв да не бидат обележани од алгоритам. Овој ефект врз слободата на говор и здружување може полека да го уништи општеството кое оригинално се стремевме да го заштитиме.

Понатаму постои ризикот од лажни позитиви. Ниеден алгоритам не е 100% точен. Дури и стапката на точност од 99%, кога се применува на население од милиони, резултира со тоа што илјадници невини луѓе се погрешно категоризирани како потенцијални терористи. Човечката цена од овие грешки е огромна, почнувајќи од психолошки трауми па се до кривична постапка. Но, постои и аргументот дека, исто како што таква грешка може да направи човек, така може и еден автоматизиран систем, односно системот е онолку добар и прецизен колку што се луѓето кои го создале, и податоците од кои системот учи. Не може и не треба да се очекува максимална прецизност од систем создаден од несовршени луѓе, но може да се очекува побрза обработка на податоци и поголема прецизност во споредба со она кое го имаме сега.

Низа предности може да се наведат за ВИ и тие се повеќепати споменати во ова истражување. Како примарна предност е брзината на процесирање на податоци во однос на брзината на човек и колкав временски период е потребен за добивање на готов производ во вид на конкретна информација од едниот и другиот извор. Наредно во процесот е анализа на тој финален податок, дали е тој точен и релевантен и дали е навремено добиен, или не. Согласно овие критериуми, ВИ се покажува како супериорна, способна да обработи милиони податоци за дел од секунда, намален процент на грешка при обработка, и брзина која овозможува побрза реакција на релевантни институции во споредна со обработка на податоци од страна на еден цел тим од струни лица, а камо ли еден човек. Сепак брзината, безбедноста и сигурноста доаѓаат со своја цена и човечкиот фактор е оној кој ќе го има финалниот збор за тоа колку од својата приватност е подготвен да жртвува за низата поволности кои ги нуди вештачката интелигенција. Недостатоците се токму она кое државите и луѓето треба да бидат подготвени да ги прифатат во доза која е во текот со нивните морални и етички вредности. Имено, ВИ со цел да ги обработи податоците и да направи добри профили, треба да обработи лични податоци на луѓето кои тие сами ги објавуваат на своите социјални мрежи и општо онлајн, но и приватни податоци, пораки и слично. Ова е еден од најголемите недостатоци бидејќи се пројавува етичка дилема—колку од нашите податоци сме подготвени да ги дадеме во замена за поголема сигурност. Во безбедноста постои правило дека доколку сакаме да сме побезбедни, треба да отстапиме дел од нашата слобода и приватност, но апсолутна безбедност би можело да постои во свет каде што сите се под постојан мониторинг и идеално не излегуваат од своите домови па дури и тогаш под знак прашалник е дали ќе се дојде до апсолутна безбедност. Поради овие етички причини, мора државите при постепената, и во никој случај не смее да е оддеднаш, имплементација на ВИ во своите системи, без оглед од која област, мора да внимаваат колку од слободата и приватноста на своите граѓани ја заменуваат за зголемено ниво на безбедност и сигурност.

Како друг вид недостаток се истакнува постоењето предрасуди во самите системи. ВИ учи од луѓето и колку повеќе тие се користат, толку повеќе учат и прибираат знаење. Така, доколку ВИ учи од податоци создадени од луѓе, а кои по

природа сме полни со предрасуди, така и самата технологија ќе поприми дел од тоа. Доколку овие технологии попримат од пристрасни податоци, може да се појават значителни грешки во анализите на податоци и резултатите од истите.

Табела 3: Табеларно претставување на предностите и недостатоците на профилирањето.

	Предности	Недостатоци
Процесирање	Обработува многу податоци и идентификува шеми.	Се јавува празнина каде причината зад етикетата на „закана“ е скриена.
Време	Работи 24/7 без потреба од пауза.	Висока фреквенција на лажно позитивни резултати кога се применува кај голема популација.
Пристрасност	Може да е целосно непристрасен доколку податоците се такви.	Таргерира маргинализирани групи.
Анализа	Ефикасно ги мапира децентрализираните ќелии и лидерство на организации.	Поттикнува постојан надзор во име на повеќе податоци.
Менаџирање ресурси	Ефикасен во работењето.	Преобремен надзор создава страв и несигурност.
Контрадикторност	Делува превентивно наспрема реактивно.	Терористи користат ВИ за да влијаат на податоци и ги „оштетуваат“.
Одговорност	Обезбедува податоци за донесување на безбедносни одлуки.	Го нарушува носењето на одлуки, елиминирајќи дискусии.

Еден од најголемите технолошки подвизи во современата човекова историја е вештачката интелигенција, но истата таа технологија може да ни помогне во борбата против тероризмот и зголемување на степенот на нашата безбедност. Но, и покрај сето ова, треба да сме свесни за ризиците и недостатоците кои доаѓаат со оваа

технологија, односно обработката на лични податоци и неговата спротивставеност со правото на приватност и обработката на податоци засновани на предрасуди кои може да донесат погрешни резултати.

5. ЗАКЛУЧОК

Во рамките на овој труд беше поставена основна хипотеза заедно со низа од помошни хипотези. Согласно наводите на ова истражување се констатира дека **употребата на вештачката интелигенција значително го зголемува капацитетот за профилирање и превенција на терористички активности**. ВИ не само што го олеснува обемот на работа на лицата задолжени за таа работа, туку и ја извршува за многу краток временски период и дава прецизни резултати.

Помошните хипотези имаа цел да дадат појаснување по однос на определени прашања за вештачката интелигенција и нејзината примена, па така првата говореше за тоа дека **вештачката интелигенција овозможува побрзо и поефикасно детектирање на екстремистички содржини на социјалните медиуми и онлајн платформите**. Оваа теза се докажува како точна. ВИ е и повеќе од способна да анализира содржини на социјални медиуми како Фејсбук, Инстаграм, Јутуб, Портали и сл. и тоа го прави за многу краток период, што придонесува за поефикасно работење. Хипотезата дека **предиктивните модели базирани на вештачка интелигенција можат да идентификуваат ризични поединци, или групи пред да се случи терористички акт**, исто така се воспоставува како точна бидејќи овие модели се опремени со програми за анализа на лица, глас, и биометриски показатели како отпечатоци од прсти кои подоцна ги поврзуваат со базите на податоци на државите, и доколку се појави сомнително лице при процесот на анализа, веднаш ги вклучува алармите за постапување доколку се јави таква потреба. Покрај ова, доколку лицата не биле идентификувани во веќе постоечките системи како „ризични“, системот може да детектира некоја неправилност и да сигнализира дека тоа лице треба да биде

обележано како лице од висок ризик. Како надоврзување на оваа помошна хипотеза е следната, според која **Алгоритмите за обработка на големи податоци (big data) помагаат во препознавање на поврзаности меѓу радикализирани индивидуи и терористички мрежи.** Станува збор за анализа на голем обем податоци кои можат да послужат при анализа на индивидуи, кои се нивните активности, дали се стремат кон радикализација, дали сакаат да бидат дел од некоја мрежа, и доколку одговорот е да, во која поконкретно, и дали во моментот веќе се во контакт со некоја терористичка мрежа.

Употребата на ВИ не е секогаш стопроцентно точна и тоа воглавно зависи од податоците кои ги обработува и колку се тие пристрасни кон нешто или некого. Така, хипотезата дека **системите базирани на ВИ честопати се подложни на алгоритамска пристрасност што може да резултира со лажно позитивни идентификации** е целосно потврдена, односно алгоритмите можат да бидат целосно пристрасни доколку им се даваат такви податоци, а доколку тоа е соодветно регулирано, пристрасноста би била сведена на минимум. Како надоврзување на ова е и следната хипотеза дека **недостатокот од транспарентност во алгоритамските процеси го намалува јавниот надзор и може да доведе до злоупотреба на овластувањата.** Злоупотребата на ваквите системи може да биде голема и многу опасна бидејќи станува збор за надзор на милиони онлајн профили и активности кои се покосуваат со основните права за приватност. Поради ова неопходно е да се најде баланс помеѓу степенот на надзор потребен за одржување на безбедноста на граѓаните, притоа без да се остави преголем простор за терористите слободно да дејствуваат онлајн, а и во физичкиот свет. Поради ова беа поставени и последните две помошни хипотези за тоа дека **ефикасната примена на вештачка интелигенција бара постојана човечка контрола, правна регулатива и етички надзор и успешното интегрирање на ВИ во борбата против тероризмот зависи од интероперабилноста меѓу националните и меѓународните безбедносни институции.** Во двата случаи, се воспоставува дека хипотезите се точни.

Профилирање се темели на науките за однесувањето на луѓето, како што е бихејвиоралната теорија, кои функционираат под претпоставката дека постапките

на една личност, особено за време на извршувањето на кривично дело се директен одраз на нивната психологија, социјална состојба и карактеристики на личноста.

Историски гледано, овој пристап е создаден како реактивна мерка, чија основна функција била да детектира сериски престапници, односно лица кои го повторуваат делото повеќекратно. Тоа може да бидат сериски убијци, луѓе кои извршуваат кражба и тешка кражба, и во контекст на овој труд, екстремисти, симпатизери на терористички групи, следбеници и терористи кои извршуваат напади. Со испитување на трагите кои може да се протолкуваат како еден вид „потпис“ на сторителот, кои се оставени на местото на злосторството, истражителите би можеле да ја заклучат веројатната возраст на престапникот, каде би можело да живее, брачен статус, телесна градба, начин на размислување и каде наредно би дејствувал.

Овој конвенционален модел е заснован на хипотезата за конзистентност, која претпоставува дека однесувањето на престапникот останува стабилно низ различни инциденти. Иако се покажало ефикасно за локализирана криминална активност, порастот на глобалните закани бара понапреден, проактивен развој на овие методи.

Кога профилирањето преминало во сферата на борбата против тероризмот, неговата цел се пренасочила од идентификување на сторителот по настанот кон предвидување и спречување на катастрофален настан кој би предизвикал непоправлива штета. Профилирањето на тероризмот е уникатно комплексно бидејќи се обидува да го мапира патот кон радикализација - процес кој е нелинеарен и многу идиосинкратичен. За разлика од традиционалното криминално профилирање, кое се занимава со специфични модели на однесување поврзани со опишани злосторства, профилирањето на терористите често ја таргетира предоперативната фаза. Ова вклучува идентификување лица кои можеби се движат кон насилан екстремизам пред да се случи какво било кривично дело. Предизвикот за безбедносните институции е при анализата на онлајн профили, да направат разлика помеѓу легитимно политичко несогласување и разлика во ставови помеѓу поединци и религиозно изразување и вистинските индикатори за

мобилизација кон насилство. Оваа промена на профилирањето од алатка која се користи пред настанокот на насилни напади наместо отпосле поместувајќи го во алатка за управување со ризици, каде преку анализа се доаѓа до екстремистите пред тие да дојдат до нас.

Во процесот на развој на профилирањето општо, а потоа и во доменот на тероризмот, се јавиле повеќе видови профили кои може да се изработат за да се добие појасна слика за потенцијалните закани со кои се соочува една држава или организација. Како такви се психолошкото профилирање кое е најприсутно во кој процес доколку станува збор за реактивно профилирање се анализираат дејствијата на една личност, или терористичка организација и се прави профил на сторителот/ите и се гради слика за тоа за кого станува збор и на тој начин да се трага по тие лица или, доколку станува збор за проактивност, се анализираат профили на социјалните мрежи и општо онлајн светот и врз основа на податоците собрани од лица кои при нивните активности се вклучило црвеното светло за некакво абнормално однесување, се известуваат надлежни органи кои понатамошно ќе ја проследат ситуацијата. Покрај психолошкото, тука е и географското профилирање кое исто така може да се примени пред или по напад, со цел да се утврди каде сака да дејствува определено лице пред воопшто да извршило некогаш напад или врз основа на минати напади, каде следно ќе се упати. Биометриското профилирање е исто така едно од клучните видови на профилирање кое се темели на отпечатоци од прсти, ДНК анализа преку биолошки материјали како коса, крв и сл. Вообичаено е сите овие видови профили да се употребуваат заедно за да се добие една целосна слика за заканата која претстои.

Сепак, со развојот на технологијата и брзината со која светот оди напред, се јавува потребата институциите да бидат во чекор со истото. Доколку има терористи кои употребуваат напредна и софистицирана технологија при извршување напади, тогаш доколку сакаме да дадеме соодветен одговор на тоа, треба да се развиеме и ние. Токму во текот на тој развој се појвува една нова алатка наречена Вештачка интелигенција.

Вештачката интелигенција (ВИ) е најголемиот технолошки подвиг во последната деценија. Наоѓа широка примена во сите можни области, па така и во профилирањето на тероризмот и нејзината помош е и повеќе од добредојдена, особено во процесот на обработка и анализа на бројни податоци. Нејзината брзина е од клучно значење бидејќи на тој начин ќе се намали обемот на работа на човечките капацитети. Така, тие би имале повеќе време да се посветат на други проблематики кои не може да се решат исклучиво со помош на ВИ. Овие системи внесуваат хетерогени податоци, вклучувајќи финансиски трансакции, биометриски податоци, метаподатоци од социјалните медиуми за да генерираат „оценка на ризик“ за поединци. Со користење невронски мрежи, овие системи можат да учат од огромни бази на податоци од историјат на терористичка активност па сè до актуелни активности денес за да предвидат кои современи однесувања најмногу ги отсликуваат индикаторите на претходните напаѓачи.

Системите за профилирање на тероризмот се од голема важност, поради што наоѓаат широка примена во земјите како што се Соединетите Американски Држави, земјите-членки на Европската Унија и Израел. Нивните системи овозможуваат анализа на податоци со неверојатна брзина и прецизност и се водечки во светот. Употребуваат енормни бази на податоци, анализираат голем број лица, какви термини употребуваат при говор на социјалните мрежи, какви слики објавуваат и со какви луѓе комуницираат. Во тој поглед, Македонија, иако нема воспоставено систем за профилирање на тероризмот кој користи вештачка интелигенција, сепак покажува иницијативност и оди во права насока со носење нови законски регулативи и системи како „Везилка“.

Едукацијата за тоа што сè може да направи ВИ е клучна во процесот на заштита на институциите, приватниот сектор и граѓаните. Процесот на едукација треба да ги вклучува сите генерации бидејќи во пракса се покажува дека постарите генерации кои имаат потешкотии во владеење на технологиите се најлесна мета за разни измами поради тоа што не се свесни за степенот на напредок на ВИ, дипфејкови и разни видови измами. Ефикасноста на самиот образовен процес треба да се стави под лупа бидејќи голем дел од обуките се реализираат со теорија

без значителни подобрувања во пракса поради недостаток на практично тестирање и општо реализација на реални и суштински обуки.

Сепак, покрај сите предности и поволности, важно е да се напомене дека ВИ доаѓа и со низа недостатоци, од кои главна е етичката димензија. Правото на приватност и не подлегнување под етнички и/или расни стереотипи се нешта на кои сите се надеваме, но исто како што луѓето имаат предрасуди, и оваа технологија може да биде програмирана научена да функционира на истиот тој принцип на предрасуди. Поради ова може да се појавуваат низа грешки кои може да ги чинат безбедносните системи финансиски, па дури и со човечки животи. Од овие причини, државите треба да вложат ресурси како во развивање на вакви системи, така и во нивното проучување и анализа.

КОРИСТЕНА ЛИТЕРАТУРА

КНИГИ

1. Alex P. Schmid (2023), „Defining Terrorism“, In ICCT Report, достапно на: [Schmidt - Defining Terrorism 1.pdf](#)
2. Algorithmic Bias Initiative (2021). Artificial Intelligence and Counterterrorism: Towards Responsible Use. Center for a New American Security (CNAS).
3. Arie W. Kruglanski* and Shira Fishman (2009), „Psychological Factors in Terrorism and Counterterrorism: Individual, Group, and Organizational Levels of Analysis“, University of Maryland, Достапно на: [sipr 1009 LR \(umd.edu\)](#)
4. Asha Hemrajani (2024), „The Use of AI in Terrorism“, RSIS Commentary, Достапно на: [The Use of AI in Terrorism.pdf](#)
5. Asmir Butkovic (2019), „GeoCrime - Geographic profiling software“ стр. 1-2, Academia.edu (online), Достапно на: [\(1\) GeoCrime - Geographic profiling software | Asmir Butkovic - Academia.edu](#)
6. Council of the European Union, (2002), „Draft Council Recommendation on the development of terrorist profiles“, Doc. 11858/3/02 REV 3, достапно на: [Microsoft Word - 11858-r3en2.doc \(europa.eu\)](#)
7. Daftary, F. (1994), „The Assassin Legends: Myths of the Isma'ilis. I.B. Tauris“, Достапно на: [TheAssassin Legends. Myths of the Isma'ilis.By Farhad Daftary.pp. VIII, 213, front.London,I. B. Tauris,1994.,£39.50. | Journal of the Royal Asiatic Society | Cambridge Core](#)
8. David Charles Rapoport (2004), „The four waves of modern terror: International dimensions and consequences“, researchgate.net (online), Достапно на: [\(PDF\) The four waves of modern terror: International dimensions and consequences](#)
9. Krisztina Huszti-Orbán, Fionnuala Ní Aoláin (2020), „Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?“, Human Rights Center, University of Minnesota, ohchr.org (online), Достапно на: [biometricsreport.pdf \(ohchr.org\)](#)

10. EU(2024), „ REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL“, Достапно на: [Regulation - EU - 2024/1689 - EN - EUR-Lex](#)
11. Farhan Hyder Sahito, Wolfgang Slany, Safdar Zaman, Irfan Hyder Sahito and Rana Shahzad Qaiser (2013), „Terrorist profiling as a Counterinsurgency Strategy: Applying the Concept to Law Enforcement“, стр. 282, issr journals (online), Достапно на: [IJIAS-13-211-34.pdf \(issr-journals.org\)](#)
12. Frederick J. Hacker (1976), „ Crusaders, criminals, crazies : terror and terrorism in our time “, Достапно на: [Crusaders, criminals, crazies : terror and terrorism in our time : Hacker, Frederick J : Free Download, Borrow, and Streaming : Internet Archive](#)
13. Gambetta D, Hertog S. (2016), „Engineers of Jihad: The Curious Connection Between Violent Extremism and Education“, Princeton, Princeton University Press.
14. GIFCT Red Team Working Group (2023), „Considerations of the Impacts of Generative AI on Online Terrorism and Extremism“, Global Internet Forum to Counter Terrorism, достапно на: [Considerations of the Impacts of Generative AI on .pdf](#)
15. Horsley, R. A. (1979). The Sicarii: Ancient Jewish "Terrorists". *The Journal of Religion*, Достапно на: [The Sicarii: Ancient Jewish "Terrorists" on JSTOR](#)
16. Iliyan Kuzmanov (2024), „AI and Psychological Profiling for Violence Risk Assessment: Enhancing Accuracy and Addressing Ethical Challenges“, достапно на: [\(PDF\) AI and Psychological Profiling for Violence Risk Assessment: Enhancing Accuracy and Addressing Ethical Challenges](#)
17. Iskren Ivanov (2016), „Lone Wolf Terrorism: Nature, History and Motivation“, Academia (online), достапно на: [Lone Wolf Terrorism Nature History and M.pdf](#)
18. Iliyan Kuzmanov. (2024). AI and Psychological Profiling for Violence Risk Assessment: Enhancing Accuracy and Addressing Ethical Challenges, Volume 2, Issue 12. Достапно на: chrome-extension:// efaidnbnmnnnibpcajpcglefindmkaj/<https://tjier.org/jnrid/papers/JNRID2412032.pdf>.

19. Jerrold M. Post, (2007), „The Mind Of The Terrorist“, Достапно на: [The Mind of the Terrorist: The Psychology of Terrorism from the IRA to al-Qaeda](#)
20. Musiani, F., & Pohle, J. (2021). *Algorithmic profiling in counterterrorism: Between efficiency and fundamental rights*. Internet Policy Review, 10(2). <https://doi.org/10.14763/2021.2.1562>
21. Ramón Spaaij (2012), „*Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention*“, SpringerBriefs in Criminology.
22. Reuben Vaisman-Tzachor (2007), „Profiling Terrorists“, Journal of Police Crisis Negotiations, researchgate (online), Достапно на: [\(PDF\) Profiling Terrorists \(researchgate.net\)](#)
23. Serena Bianchi, Marina Mancuso, Caterina Paternoster, George Kalpakis, Theodora Tsikrika, Stefanos Vrochidis, Denitsa Kozhuharova, Bernhard Jaeger (2023), „Artificial Intelligence to Counter Cyber-Terrorism“, Достапно на: [ALLIES Artificial-Intelligence-to-Counter-Cyber-Terrorism CyberCon-2023-02.pdf](#)
24. Shai Farber (2025), „AI-Enabled Terrorism: A Strategic Analysis of Emerging Threats and Countermeasures in Global Security“ стр. 330, Journal of Strategic Security 18, no. 3, Достапно на: [AI-Enabled Terrorism: A Strategic Analysis of Emerging Threats and Countermeasures in Global Security](#)
25. Stavros Makris (2018), „Geographic Profiling Locating The Serial Murderers“ стр. 4-8, Достапно на: [FULLTEXT01.pdf \(diva-portal.org\)](#)
26. Tucker, P. (2020). *AI Can Help Counter Terrorism—But It Can Also Help Terrorists*. *Defense One*, достапно на: <https://www.defenseone.com/technology /2020/06/ai-can-help-counter-terrorism-it-can-also-help-terrorists/166020>
27. U.S. Department of Justice, FBI, Behavioral Analysis Unit (2019), „A study of Lone Offender Terrorism in the United States (1972-2015)“, Достапно на: [lone-offender-terrorism-report-111319 \(1\).pdf](#)
28. UNICRI, UNCCT (2021), „Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes“, Достапно на: [Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes | UNICRI :: United Nations Interregional Crime and Justice Research Institute](#)

29. United Nations Office of Counter-Terrorism (2021), „Countering Terrorism Online with Artificial Intelligence“, Достапно на: [Countering Terrorism Online with Artificial Intelligence | UNICRI: United Nations Interregional Crime and Justice Research Institute](#)
30. Zuev, D., & Bratchford, G. (2019). *Profiling Terrorism: Law, Policy, and Artificial Intelligence. Law, Technology and Humans*, 1(1), 67–82.
31. Кривичен закон на Р.Македонија
32. Тања Милошевска (2018), „Глобален тероризам“, Скопје-Филозофски факултет, Универзитет „св. Кирил и Методиј“.
33. Тања Милошевска (2024), „Потенцијална експлоатација на генеративна вештачка интелигенција од терористи и насилни екстремисти“, *Годишен зборник*, Филозофски факултет, достапно на: <https://journals.ukim.mk/index.php/godzbo/article/download/2780/2396/>

Веб-страни

1. Abigail Darwish (2024); „Tactical AI: How Israel is fortifying its National Security Capabilities“; [bisi.org.uk](https://www.bisi.org.uk) (online); Достапно на: [Tactical AI: How Israel is fortifying its National Security Capabilities – Bloomsbury Intelligence and Security Institute \(BISI\)](#)
2. All About Forensic Psychology (2022), „Geographic Profiling“, All About Forensic Psychology (online), Достапно на: [Geographic Profiling \(all-about-forensic-psychology.com\)](https://www.all-about-forensic-psychology.com) (21.04.2024)
3. Amanda Moen (2021), „A Brief History of Biometrics“, bioconnect (online), Достапно на: [A Brief History of Biometrics | BioConnect](#)
4. Amber Pariona (2017), „What Is Lone Wolf Terrorism“, WorldAtlas (online), достапно на: <https://www.worldatlas.com/articles/what-is-lone-wolf-terrorism.html>
5. Ayoadé Onireti (2024), „Cyber-Terrorism: An Appraisal of the Dimensions of the New Face of Terrorism in a Post-9/11 Period“, достапно на: [Cyber-Terrorism: An Appraisal of the Dimensions of the New Face of Terrorism in a Post-9/11 Period | IntechOpen](#)

6. California Learning Resource Network Team (2024), „How do You analyze a case study?“, CLRN (online), достапно на: [How do You analyze a case study? - California Learning Resource Network](#)
7. Cambridge University Press (2024), „Profiling“, Cambridge English Dictionary, Достапно на: [PROFILING | definition in the Cambridge English Dictionary](#) (17.04.2024)
8. Criminal Justice Academic Writing Service (2024), „Profiling in Terrorism Cases“, iResearch.net (online), Достапно на: [Profiling in Terrorism Cases - Criminal Justice - iResearchNet](#)
9. DeLani R. Bartlette (2019), „The Mad Bomber and the Birth of Criminal Profiling“, Medium (online), Достапно на: [The Mad Bomber and the Birth of Criminal Profiling | by DeLani R. Bartlette | New York Voice | Medium](#)
10. Edwin Bakker, Jeanine de Roy van Zuijdewijn (2022), „Definition and nature of terrorism“, Amsterdam University Press, достапно на: [Definition and nature of terrorism \(Chapter 1\) - Terrorism and Counterterrorism Studies](#)
11. Europol (2026), „EU Internet Referral Unit - EU IRU“, Europol.europe.eu (online), Достапно на: [EU Internet Referral Unit - EU IRU - Monitoring terrorism and violent extremism online | Europol](#)
12. FBI (2026), „Terrorism“, Достапно на: [Terrorism — FBI](#)
13. JRank (2024), „Criminal Profiling, Origins, Procedures, Controversies, Resources“, jrank.org (online), Достапно на: [Criminal Profiling, Origins, Procedures, Controversies, Resources \(jrank.org\)](#)
14. Katie Worth (2016), „Lone Wolf Attacks Are Becoming More Common — And More Deadly“, PBS (online), Достапно на: [Lone Wolf Attacks Are Becoming More Common -- And More Deadly | FRONTLINE | PBS | Official Site | Documentary Series](#)
15. Kendra Cherry (2024), „Behavior Analysis in Psychology“, Very Well Mind (online), Достапно на: [Behavior Analysis in Psychology: How It's Used \(verywellmind.com\)](#) (24.04.2024)

16. Meloy, J. R., Hoffmann, J., Guldimann, A., & James, D. (2012), „The role of warning behaviors in threat assessment: An exploration and suggested typology“ стр. 265-266, n Wiley
17. Merriam-Webster (2024), „Profiling“, Merriam-Webster, Достапно на: [Profiling Definition & Meaning - Merriam-Webster](#)
18. Merriam-Webster (2024), „The History of the Word 'Terrorism'“, Merriam-Webster, Достапно на: [The History of the Word 'Terrorism' | Merriam-Webster](#)
19. Ministry of Economy and Industry, Foreign Trade Administration (2024), „View Larger Image AI-Powered Border Management: The Israeli Innovation Driving Global Security and Humanitarian Solutions“, itrade.gov.il (online), Достапно на: [AI-Powered Border Management: The Israeli Innovation Driving Global Security and Humanitarian Solutions - India - Israel Trade & Economic Office, Embassy of Israel](#)
20. Nasir Ahmed Ganaie (2025), „The role of artificial intelligence in radicalisation, recruitment and terrorist propaganda: deconstructing violent extremism and reimagining counterterrorism in contemporary digital ecosystems“, frontiersin.org (online), Достапно на: [Frontiers | The role of artificial intelligence in radicalisation, recruitment and terrorist propaganda: deconstructing violent extremism and reimagining counterterrorism in contemporary digital ecosystems](#)
21. National Institute of Standards and Technology (2024), „Biometrics“, Computer Security Research Center (online), Достапно на: [Biometrics - Glossary | CSRC \(nist.gov\)](#)
22. NATO (2023), „Deep Dive Recap: Counter Terrorism and the Gender Perspective“, NATO (online), Достапно на: [NATO - News: Deep Dive Recap: Counter Terrorism and the Gender Perspective, 28-Mar.-2023](#)
23. Online Library (online), Достапно на: [The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology \(drreidmeloy.com\)](#)
24. Open Access Government (2016), „Using biometrics to fight crime“, Open Access Government (online), Достапно на: [Using biometrics to fight crime | Open Access Government](#)
25. Oxford (2026), „Terrorism noun-definition, pictures, pronunciation and usage notes“, OxfordLearnersDictionaries.com (online), Достапно на: [terrorism noun - Definition,](#)

[pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com](#)

26. Oxford University Press (2024), „Profiling“, Oxford English Dictionary, Достапно на: [profiling - Quick search results | Oxford English Dictionary \(oed.com\)](#)
27. Reid Meloy (2016), „Perspective: Identifying Warning Behaviors of the Individual Terrorist“, FBI Law Enforcement Bulletin (online), Достапно на: [Perspective: Identifying Warning Behaviors of the Individual Terrorist – LEB \(fbi.gov\)](#)
28. Riya Kumari (2020), „What is an Algorithm? Types, Applications, and Characteristics“, Analytics Steps (online), достапно на: [What is an Algorithm? Types, Applications, and Characteristics | Analytics Steps](#)
29. Saul Mcleod (2023), „Offender Profiling In Psychology“, Simple Psychology (online), Достапно на: [Offender Profiling In Psychology \[Criminal Profiling\] \(simplypsychology.org\)](#)
30. Stanford University (2011), „Machine Learning“, достапно на: [Machine Learning - Stanford University](#)
31. Toronto Metropolitan University (TMU) <https://www.torontomu.ca> Dibbyo Saha Computer Science, A Brief Introduction to Artificial Intelligence
32. United States Court of Appeals for the Second Circuit (2020), „United States of America v. Sinmyah Amera Ceasar“, Justia (online), Достапно на: [United States v. Ceasar, No. 19-2881 \(2d Cir. 2021\) :: Justia](#)
33. Дигитален речник на македонски јазик (2025), „Радикализација“, достапно на: [радикализација - резултати од пребарување | Дигитален речник на македонскиот јазик](#)
34. Дејан Соколоски (2025), „ВЕЗИЛКА: Од македонски LLM до паметно земјоделство – Како националната AI Factory Antenna ќе ја трансформира Македонија“, Достапно на: [ВЕЗИЛКА: Од македонски LLM до паметно земјоделство – Како националната AI Factory Antenna ќе ја трансформира Македонија * IT.mk](#)