УНИВЕРЗИТЕТ ОДБРАНЕ У БЕОГРАДУ

ВОЈНА АКАДЕМИЈА

Јасмина Андрић

КРЕИРАЊЕ ТЕОРИЈСКОГ МОДЕЛА БЕЗБЕДНОСНЕ АНАЛИТИКЕ НА ПРИМЕРУ СУПРОТСТАВЉАЊА ТЕРОРИЗМУ

ДОКТОРСКА ДИСЕРТАЦИЈА

Ментор:
Пуковник
Ванр. проф. др Срђан Благојевић

Кандидат:
Докторанд
Јасмина Андрић

Београд, 2026

Планирајте оно што је тешко док је још лако, чините оно што је велико док је мало. Најтеже ствари на свету морају бити учињене док су још лаке, највеће ствари на свету морају бити учињене док су још мале.

Сун Цу

ЗАХВАЛНИЦА

Овим путем желим да изразим захвалност свима који су на било који начин допринели изради ове дисертације.

На првом месту, захваљујем се свом ментору, пуковнику и професору доктору Срђану Благојевићу, који ме је током израде овог рада стручно водио, усмеравао и несебично делио своје знање, нарочито у области методологије истраживања, чиме је значајно допринео квалитету и структури дисертације.

Искрено се захваљујем свом професору и пријатељу, генералу у пензији, професору доктору Божидару Форци на непрекидној подршци, драгоценим саветима и богатом искуству, који су ми значајно помогли у разумевању теме и обликовању истраживачког оквира. Његова спремност да у сваком тренутку подели знање и практичне увиде представља за мене посебно вредну подршку.

Захваљујем се и својим колегама Милошу Тишми и Николи Стојићу, који су својим знањем и ангажовањем омогућили израду примера базе података и пружили неопходну стручну ИТ подршку током истраживања. Такође, захваљујем се свим стручњацима који су се одазвали и учествовали у истраживању, својим увидима и искуством доприносећи релевантности и практичној вредности овог рада.

На крају, најдубљу захвалност дугујем својој породици, на разумевању, стрпљењу и подршци током целокупног процеса израде дисертације, као и драгим пријатељима који су ме бодрили и веровали у мене.

САДРЖАЈ

СПИСАК СЛИКА

СПИСАК ТАБЕЛА

СПИСАК ГРАФИКОНА

СПИСАК ПРИЛОГА

УВОД

Човеков живот и опстанак условљени су сазнањима како искуственим тако и научним. Путем чула и личног искуства добијамо сазнања о природним појавама и друштвеним догађајима. С друге стране, научним методама, кроз емпиријска и теоријска истраживања, стичемо систематизована знања из одређене области. У процесу стицања сазнања посебну улогу имају аналитика и аналитичке методе.

Уочавање одређених података, њихово груписање и изградња једне схватљиве целине је природан процес који човеку помаже у свакодневном животу. Тако можемо рећи да је аналитика својствена човеку и да је природни епитет човековог постојања. „Према изложеном, аналитика је делатност стицања (и употребе) истинитог, у одређене сврхе употребљивог сазнања систематски и континуирано, применом проверених, плодотворних, првенствено научних метода“ (Даниловић, Милосављевић, 2008: 7). За долажење до сазнања у аналитичким процедурама користе се, поред научних метода и оперативне и све друге методе сазнања.

Безбедност у савременим условима, и теоријски и практично, проширена је са иманентно војног подручја на друге секторе, као што су политички, економски, социјетални и еколошки. Модерне државе, без обзира на то да ли припадају или не одбрамбеним коалицијама и безбедносним интеграцијама, развијају сопствени (национални) систем безбедности. Управо је безбедносна аналитика она грана аналитике која данас има посебан значај за систем безбедности.

Прикупљање и обрада података у области безбедности често су кључни за очување виталних, националних интереса једне државе. Међутим, без обзира на њен значај безбедносна аналитика још увек није успостављена као посебна научна дисциплина и многи је сматрају више вештином него науком. О томе да ли је безбедносна аналитика струка или наука подељена су мишљења, те преовладава став да је то струка заснована на науци.

> „Анализа коју спроводе обавештајци, органи реда и предузећа заједнице никада неће постићи тачност и предвидљивост истинске науке, јер информације са којима аналитичари морају да раде су обично непотпуне, двосмислене и потенцијално варљиве. Аналитички

процес међутим, може имати користи од неких лекција из науке и прилагодити неке елементе научног резоновања“ (Heuer & Pherson, 2015: 186).

Без обрзира на научни оквир, безбедносна аналитка је данас неизоставни део сектора безбедности који функционише највише на оперативном нивоу. Министарства која припадају сектору безбедности и одбране запошљавају аналитичаре како би дошла до одговора на широк спектар питања везаних за националну безбедност. Тако аналитички сектори постоје, на пример, у Министарству унутрашњих послова и Министарству одбране и другим државним организацијама и институцијама.

Иако је безбедносна аналитика истраживана кроз различите сегменте обавештајног рада, војног и полицијског деловања као што је, на пример, полицијско-обавештајни модел, ипак ови сегменти нису обједињени нити довољно теоријски обрађени. Стога, јавила се потреба да се креира модел безбедносне аналитике општијег типа који би могао бити примењен у различитим секторима безбедности, а који су проширени са иманентно војног подручја. Како би се такав модел сликовитије представио, изабрали смо једну од највећих претњи безбедности савременог доба – тероризам.

Тероризам као динамичан облик политичког насиља из дана у дан поприма нове облике, као и методе и средства борбе. Да би савремена држава, али и међународна заједница, могла да се супротстави једној оваквој претњи, она се мора ослањати на прикупљање података и обавештајни рад. Овде се намеће питање да ли је данас довољно да се против једне овако сложене претње ослањамо на класичне обавештајне методе или је потребно обухватити шири аспект података, као што су културолошке разлике, друштвено-економски контекст, па све до еколошких аспеката који могу имати утицај на настанак и функционисање једног терористе или терористичке организације.

Тероризам је толико сложен феномен да, иако се доминантно односи на сферу политике, он ипак као флуидан облик политичког насиља може користити све дисиметрије и друштвене проблеме као повод, изговор или оправдање за терористичке акције. Да би савремене службе безбедности могле да се супротставе тероризму и да предвиде потенцијалне терористичке активности морају се ослањати на безбедносну аналитику која има стандардизоване процесе који се могу применити на широк спектар безбедносних изазова, ризика и претњи.

Управо теоријски модел безбедносне аналитике који желимо да представимо обједињује различите секторе безбедносног деловања и оно што је данас познато у теорији како бисмо креирали основу за обавештајни рад која може да има широку примену и која се даље може развијати, али и критиковати.

У научним истраживањима друштвених процеса, поготово оним која претендују да изнедре њихов модел, неопходно је критички приступити постојећем сазнању и уочавању оних подручја истраживане појаве (процеса) подложне промени. У том смислу, у првом делу дисертације анализираће се сам назив и процес „безбедносне аналитике“, преко њиховог теоријског одређења, с једне, и примене у пракси, с друге стране. Теорија и пракса су две стране једног истог проблема па нема добре праксе без коректно утврђене теорије, нити добре теорије без њене проверљивости у пракси.

1. ФОРМУЛАЦИЈА ПРОБЛЕМА ИСТРАЖИВАЊА

1.1 Основни хипотетички ставови о проблему истраживања

Једну од дефиниција аналитике дао је Славомир Милосављевић, који каже: „Аналитика је првенствено интелектуална, организована, систематска, циљна и сврсисходна делатност усмерена ка стицању релативно истинитих, релативно тачних и употребљивих сазнања о претежно актуелним збивањима у разним областима људског и друштвеног живота“ (Термиз и Милосављевић, 2008).

Посебно сложен и недовољно научно истражен облик аналитике јесте безбедносна аналитика. Ту одредбу аналитике, у ужем смислу, поједини аутори посматрају кроз рад обавештајних и безбедносних служби. Тако, Бајагић (2010) наводи да је:

> „Обавештајна активност, као један од три кључна канала информисања битан елемент националне моћи сваке савремене државе и њеног система безбедности, и да у најопштијем смислу подразумева целисходно, правовремено, планско, тајно и организовано прикупљање и обраду обавештајних информација које се кроз процес анализе, обраде и интеграције претварају у завршно обавештајно знање о датом проблему, појави или догађају и, у форми завршних обавештајних докумената, уступају крајњим корисницима“.

Такође, Стајић (2021) наводи да „обавештајна служба ствара услове да руководство земље (политичко, војно и др.) своју активност усмерава само ка поузданим, веродостојним и тачним подацима“.

Деловање обавештајних и безбедносних служби, у аналитичком смислу посматрано, одвија се у процесу који се назива обавештајни циклус. Према Форци и Аночићу (2018), „обавештајни циклус је структурисана, систематска серија операција које имају за циљ да се надлежни обавештајни органи упознају са расположивим информацијама, одлуче које од њих су битне за конкретну операцију, установе који подаци им недостају и наложе органима или агенцијама да их прибаве, а затим да процесуирају те податке у обавештајне информације, пре него што их доставе корисницима“. Обавештајни циклус, према различитим виђењима, има различите фазе (кораке), где се, најчешће, помињу четири: прикупљање података, аналитика, израда обавештајно-аналитичких дела и достављање (дисеминација) корисницима. Дакле, аналитика је само једна фаза (корак) обавештајног циклуса.

Аналитиком у свом раду користе се сви субјекти система националне безбедности. Тако, разликују се: дипломатска аналитика, аналитика управљачких органа, обавештајна аналитика (војска); аналитика у полицији: 1) криминалистичко-обавештајни рад (КОР), 2) криминалистичко-обавештајна аналитика (КОА), 3) криминалистичко-аналитичка делатност; 4) криминалистичка аналитика и 5) криминалистичко-обавештајни послови; 6) аналитика у корпорацијама (корпоративно-обавештајна аналитика) и друге. С обзиром на то да се све те аналитике баве истим послом, аналитиком безбедносних појава, логично, поставило се питање може ли се тај рад именовати једним именом – безбедносна аналитика.

Обавештајни циклус и његов део аналитика посебно се користе у супротстављању тероризму, као једне од највећих претњи безбедности 21. века, али уједно и изазова у економском, моралном и културном смислу. То је сложен феномен који има много појавних облика и који карактеришу динамичност и променљивост.

Један од домаћих, а признатих у свету експерата за тероризам и политичко насиље Драган Симеуновић дао је своју дефиницију савременог тероризма. Овај аутор наводи следеће:

> „Као вишедимензионални политички феномен савремени тероризам се може теоријски најопштије одредити као сложени облик организованог групног, и ређе индивидуалног или институционалног политичког насиља обележен застрашујућим брахијално-физичким и психолошким методама политичке борбе којима се обично у време политичких и економских криза, а ретко у условима остварене економске и политичке стабилности једног друштва, систематски покушавају остварити велики циљеви на начин непримерен датим условима, пре свега друштвеној ситуацији и историјским могућностима оних који га као политичку стратегију упражњавају“ (Симеуновић, 2002).

Уколико повежемо све наведене појмове – аналитику, прикупљање података и савремене претње безбедности, долазимо до заједничког појма – *безбедносна аналитика*, као реалтивно новог појма у теорији и пракси система националне безбедности Републике Србије. Тај појам више се појављује у практичном раду обавештајних и безбедносних служби него у теорији. Тако, безбедносна аналитика, као обједињени појам, у нашој теорији и пракси примарно се подразумева као практична делатност, а ређе као практична делатност заснована на науци. Стога, јавила се потреба да се безбедносној аналитици да теоријски оквир како би могао да се формира модел који би био примењив на супротстављању савременим претњама безбедности попут тероризма.

1.2 Значај истраживања

У складу са претходно наведеним, безбедносна аналитика јесте један од врло значајних и примарних задатака свих субјеката система безбедности усмерена ка правилној (пр)оцени стања и предузимању мера и активности ради постизања оптималног нивоа стања безбедности.

Иако још увек није конституисана као наука у пуном смислу, безбедносна аналитика као подврста аналитике има свој изузетан научно-друштвени значај. Безбедносна аналитика је одавно ушла у рад безбедносних и обавештајних служби, сектора и одељења. Међутим, њен пун потенцијал долази до изражаја у савременом контексту управо због динамичне флуктуације великог броја података. Такође, за сложене безбедносне појаве попут тероризма, које у себи садрже више простијих облика насиља, потребно је пратити трендове развоја у циљу предикције његових будућих кретања. Предиктивна функција безбедносне аналитике може да има изузетан значај у борби против сложених претњи безбедности попут тероризма.

Колики је значај безбедносне аналитике, а посебно постојања аналитичких база података за супротстављање тероризму говори и податак да се и научна заједница окреће формирању оваквих база. Тако је више универзитета и међународних института кроз пројекте или самостално креирало више база попут Академске база која припада Универзитету у Мериленду, Колеџ Парк (https://www.start.umd.edu/gtd/-Global Terrorism Database). Такође, у сврху борбе против тероризма формирана је база за претрагу података везаних за тероризам и

организовани криминал, у чијој су изради са колегама из Џорџ Маршал центра учествовали и факултети Универзитета у Београду (http://www.tocsearch.com – TOC database). У том смислу, битно је уважити улогу безбедносне аналитике у супротстављању савременом тероризму. Међутим, да бисмо разумели како се безбедносна аналитика и аналитичке базе могу користити у савладавању препрека у супротстављању тероризму, морамо прво разумети шта је безбедносна аналитика и устројити њен нов теоријски модел у овој области.

1.3 Научни значај истраживања

Научни значај овог истраживања се може посматрати као хеуристички резултат у смислу потенцијалног откривања новог теоријског модела безбедносне аналитике у борби против тероризма, али и као верификовани резултат кроз потврду постојећих сазнања у области борбе против тероризма и аналитичких процеса. Кључни допринос је у сазнавању новог теоријског модела безбедносне аналитике кроз његов опис и објашњење.

1.4 Друштвени значај истраживања

Друштвени значај овог истраживања огледаће се у унапређењу теорије и праксе у области спречавања и борбе против тероризма, што ће за последицу имати и унапређење рада система безбедности у овој области. Претпоставка је да ће нови понуђени модел безбедносне аналитике моћи да се примењује поред тероризма и на друге сродне облике политичког насиља од чега ће целокупно друштво имати користи.

1.5 Резултати претходних истраживања

Безбедносна аналитика као релативно нова научна дисциплина није довољно истражена у литератури. Мали је број аутора, посебно домаћих, који су се бавили овом специфичном врстом аналитике. Славомир Милосављевић и Џевад Термиз у свом делу *Аналитика* (Термиз и Милосављевић, 2008) дали су основни преглед аналитике као научне дисциплине уз осврт на безбедносну аналитку. Наслањајући се на ово дело Славомир Милосављевић и Нђо

Даниловић креирали су монографију *Основи безбедносне аналитике* (Даниловић и Милосављевић, 2008). Ови аутори, као пионири у Србији, дали су своје дефиниције аналитике и безбедносне аналитике и своје виђење аналитичког процеса које је умногоме засновано на пракси. Поред наведених аутора, безбедносном аналитиком бавили су се и професор Божидар Форца и бивши начелник Обавештајне управе Генералштаба Бранислав Аночић у скрипти *Безбедносна аналитика* (Форца и Аночић, 2018). Темама изазова, ризика и претњи, као и темом обавештајног рада, које су тесно везане за безбедносну аналитику, бавили су се професор Љубомир Стајић у делу *Основи система безбедности* (Стајић, 2013, 2021) и професор Младен Бајагић у *Методици обавештајног рада* (Бајагић, 2010).

С друге стране, тероризам је појам који је нашироко описан у литератури, али с обзиром на динамичност овог феномена недовољно прецизно оивичен. Домаћи, а светски признат експерт за ову област, професор Драган Симеуновић, бавио се тероризмом кроз више дела, као што су *Тероризам* (Симеуновић, 2002), *Политичко насиље* (Симеуновић, 1989) и друго. Такође, међу домаћим ауторима темом тероризма бавио се и професор Радослав Гаћиновић у монографијама *Тероризам* (Гаћиновић, 2005) и *Тероризам у политичкој и правној теорији* (Гаћиновић, 2010). Наведена дела су теоријска основа за домен безбедносне аналитике и бробе против тероризма, али такође треба напоменути и значај научних и полицијских интернационалних база података које се баве тероризмом.

Наведене базе представљају пример практичне примене безбедносне аналитике у спречавању тероризма. Неке од значајних база података су: Глобални индекс тероризма Института за економију и мир из Њујорка, База терористичких догађаја у Европи, академско-научна база која припада Универзитету у Бергену у Норвешкој, База глобалног тероризма, академска база која припада Универзитету у Мериленду, Колеџ Парк, затим Интерполова база о међународним бегунцима и осумњиченим терористима. Треба напоменути да је и Србија преко Београдског универзитета учествовала у изради TOC базе за претрагу терориста и терористичких организација.

Такође, за ово истраживање су значајни и стратешки документи: Стратегија националне безбедности Републике Србије (*Службени гласник РС*, бр. 94/2019) и Национална стратегија за спречавање и борбу против тероризма за период од 2017. до 2021. године (*Службени гласник РС*, бр. 94/2017).

2. ОДРЕЂЕЊЕ ПРЕДМЕТА ИСТРАЖИВАЊА

2.1 Теоријско одређење предмета истраживања

О предмету истраживања постоје научно позната и верификована, научно позната али неверификована сазнања, као искуствена сазнања из праксе.

2.2 Научно верификовано сазнање

Аналитика је вишедимензионална дисциплина и често се користи у истраживањима других научних дисциплина. Она је у бити истраживачка дисциплина која се ослања на емпиријска сазнања. У складу са наведеним, под аналитиком би се могао сматрати целокупан процес који претходи стицању сазнања. Како наводи Славомир Милосављевић, таква сазнања би требало да буду релативно истинита, релативно тачна и употребљива. Аналитика се може класификовати по више критеријума, па тако постоји више врста аналитике. Једна од свакако данас најзначајнијих, али недовољно истражених врста аналитике јесте безбедносна аналитика. Безбедносна аналитика је дисциплина у развоју која има широку примену у заштити националних вредности и остварењу националних интереса једне државе.

У одређењу појма безбедносне аналитике у литератури се често наводи да је то метода и/или вештина прикупљања података. Форца и Аночић (2018) дају нешто другачије одређење овог појма: „Безбедносна аналитика је посебна врста аналитике којом се применом делотворних метода стичу релативно истинита сазнања из различитих извора о безбедносним појавама, потребна за рад субјеката система безбедности“.

Различити аутори су у оквиру различитих класификација издвојили основне фазе обавештајног циклуса, чији је аналитика један део. Укрштањем различитих критеријума класификације, ове фазе се могу оквирно одредити на следећи начин:

- постављање (дефинисање) аналитичког задатка,
- прикупљање података,
- обрада прикупљених података и израда извештаја (одговора) на аналитички задатак и
- дисеминација (достава) одговора на аналитички задатак.

Овако уобличене фазе обавештајног циклуса представљају оквирни модел њеног рада, који се умногоме поклапа са обавештајним радом и обавештајном активношћу. Теоријски оквир обавештајне активности може се схватити као мултидисциплинаран, с обзиром на то да се у великој мери ослања на теоријска сазнања везана за политику, међународне односе и безбедност.

> „Иако општеприхваћена дефиниција обавештајне активности не постоји може се рећи да она у најопштијем смислу подразумева целисходно, правовремено, планско, тајно и организовано прикупљање и обраду обавештајних информација које се кроз процес анализе, обраде и интеграције претварају у завршно обавештајно знање о датом проблему, појави или догађају и, у форми завршних обавештајних докумената, уступају крајњим корисницима“ (Бајагић, 2015).

Обавештајни циклус ближе су дефинисали Форца и Аночић (2018) као:

> „Структурисану, систематску серију операција које имају за циљ да се надлежни обавештајни органи упознају са расположивим информацијама, одлуче које од њих су битне за конкретну операцију, установе који подаци им недостају и наложе органима или агенцијама да их прибаве, а затим да процесуирају те податке у обавештајне информације, пре него што их доставе корисницима“.

Обавештајне активности су значајан елемент супротстављања тероризму. Тероризам као феномен је изузетно сложен. Осим тога, карактеришу га динамичност, мноштво појавних облика и променљивост. Ово је један од разлога зашто је феномен тероризма тешко дефинисати. Међутим, оно око чега се велика већина аутора слаже јесте да је тероризам облик политичког насиља. Посебна пажња у литератури посвећује се савременом тероризму. Као вишедимензионални политички феномен, савремени тероризам се може теоријски најопштије одредити као „сложени облик огранизованог групног, и ређе индивидуалног или институционалног политичког насиља обележен застрашујућим брахијално-физичким и психолошким методама политичке борбе којима се обично у време политичких и економских криза, а ретко у условима остварене економске и политичке стабилности једног друштва, систематски покушавају остварити ‚велики циљеви’ на начин непримерен датим условима, пре свега друштвеној ситуацији и историјским могућностима оних који га као политичку стратегију упражњавају“, наводи Симеуновић (Симеуновић, 2002).

2.3 Научно евидентирано, али неверификовано сазнање

Безбедносна аналитика је врста анлитике која се највише везује за рад државних служби и органа у систему безбедности. Државни органи и њихови аналитички сектори највише се баве овом врстом аналитике јер је безбедност грађана и друштва у већој мери у надлежности државног у односу на приватни сектор. Тако ови органи имају овлашћења да прикупљају и обрађују осетљиве податке који су од виталног интереса за безбедност једне државе. Не само да имају овлашћења, већ имају и највећи интерес, с обзиром на природу посла који обављају. Због наведеног, али и због честог преклапања аналитичког и обавештајног рада, у литератури се не може пронаћи пуно података о томе како аналитичке службе функционишу.

Обавештајни циклус се састоји из више фаза које су одвојене, али се у пракси често преклапају. Такође, ова врста процеса је применљива на различитим нивоима, од стратегијског до тактичког, и прилагодљива је датим околностима и оперативним захтевима.

С друге стране, савремени тероризам поседује одређене карактеристике које су га учиниле толико сложеним да је супротстављање овом феномену обојено читавим дијапазоном препрека. Од двоструких стандарда по питању тога шта јесте тероризам и шта није, преко недовољне међународне сарадње до оскудних и попустљивих закона и распиривања екстремизма и националне нетрпељивости у појединим државама. Ове препреке данас стварају озбиљне проблеме у супротстављању савременом тероризму.

У научној литератури из области наука безбедности све више се обрађује значај обавештајног рада за превазилажење горепоменутих препрека. Међутим, још увек не постоје конкретна објашњења општег модела по ком би безбедносна аналитика могла да се примени на супротстављање тероризаму.

2.4 Емпиријско, искуствено сазнање о предмету истраживања

У вишедеценијском процесу рада обавештајних и безбедносних служби постоји богато искуство о томе како се у пракси примењује обавештајни циклус и шта садржи једна од његових фаза – аналитика. Међутим, искуствено је познато да сама примена процедуре аналитичког рада није довољна за оптималан приступ у аналитици безбедносних појава.

Наиме, често се у анализама рада обавештајно-безбедносних аналитичара примећује потреба за теоријски систематизованим знањима и, још више, познавањем научних метода у раду[1]. Тако, на пример, Истраживачки центар за одбрану и безбедност (ИЦОБ) из Београда последњих година организује бројне радионице обуке и семинаре за припаднике сектора безбедности и студенте наука безбедности. Искуства ИЦОБ-а показују да полазници радионица, углавном, познају процедуре рада аналитичара, али да се осећа недостатак теорије (знања), као и непознавање метода, стандарда и стандардизације у тој области.

Дакле, уочава се потреба да се научно неверификована сазнања, као и искуствено показани недостаци аналитичког рада, подвргну једном истраживачком поступку.

2.5 Операционално одређење предмета истраживања

Операционално одређење предмета истраживања састоји се из чиниоца садржаја предмета истраживања, као и временског, просторног и дисциплинарног одређења предмета истраживања.

ПРВИ ДЕО

КРИТИКА ПОСТОЈЕЋЕГ СТАЊА У ОБЛАСТИ БЕЗБЕДНОСНЕ АНАЛИТИКЕ

Сазнајно-методолошки је коректно да се приликом увођења нечег новог у било којој делатности крене од критике постојећег стања. Кад је у питању безбедносна аналитика, кренућемо од самог назива, да бисмо довели у везу појмове *обавештајна аналитика*, *криминалистичко-обавештајна аналитика*, *криминалистичка аналитика* како у домаћој тако

[1] Тако, на пример, након терористичких аката на објекте у Њујорку и Вашингтону, 11. 9. 2001. године, извршена је опсежна анализа рада америчких обавештајних служби, поготово ЦИА-е. Један од закључака том приликом био је да аналитичари не познају довољно научне методе потребне за свој рад, те је уследио задатак образовном систему САД да се посебно посвети овом питању (Шире у**: Michael W. Collier**, Ph.D: *A Pragmatic Approach to Developing Intelligence Analysts,* page 27, "Defence Intelligence Journal: 14-2", November, 2005).

и у страној теорији и пракси. Тај поступак ће резултовати сазнањима о могућности обједињавања свих врста аналитике у јединствен модел – безбедносна аналитика.

Основу критике постојећег стања чиниће: дефинисање аналитике, приступи обавештајном циклусу, место аналитике у обавештајном циклусу; процедуре рада аналитичара; методе и технике у раду аналитичара; излазни резултати (аналитичка дела); потребна својства аналитичара и присуство стандарда у аналитици.

У наведеном смислу, критици постојећег стања ће бити подвргнути: 1) обавештајна аналитика у Војсци, 2) криминалистичка аналитика у полицији и 3) теоријски модел Intelligence-led policing, као и његова примена у страним државама, ОЕБС и Европској унији.

Поред постојећих домаћих извора, приручника и других материјала, посебно ће се анализирати страни извори и практична искуства у примени Intelligence-led policing-a.

Ова глава је операционализована кроз четири поглавља:

1. Дефинисање аналитике,
2. Обавештајна аналитика,
3. Криминалистичка аналитика и
4. Intelligence-led policing и његова примена у страним државама, ОЕБС и ЕУ.

ДРУГИ ДЕО

ТЕОРИЈСКИ МОДЕЛ БЕЗБЕДНОСНЕ АНАЛИТИКЕ НА ПРИМЕРУ СУПРОТСТАВЉАЊА ТЕРОРИЗМУ

Теоријски модел безбедносне аналитике инспирисан је идејом да се постојеће врсте аналитике интегришу у један теоријски модел под називом безбедносна аналитика. Тај модел, такође, инспирисан је неким страним погледима по питању потребних знања аналитичара, познавања метода и техника у раду и примени стандарда. Ти мотиви иницирали су идеју да се суштина теоријског модела безбедносне аналитике, у ствари, своди на знање, које се у теорији и пракси именује као доктрина. Ова доктрина (знања) обухватаће: знања о секторима безбедности, знања о процедурама рада аналитичара и знања о стандардима у аналитици, као и формирање и коришћење база података. Свакако, све то, као студија случаја, обухватиће аналитику у супротстављању тероризму.

Безбедност, како смо истакли, поодавно је проширена са чисто војно-полицијског у политички, економски, социјетални (друштвени) и еколошки сектор. У конципирању општег теоријског модела безбедносне аналитике неопходно је истражити и дефинисати скуп

информација који детерминише наведене секторе, како би се исти ефикасно применио на супротстављање тероризму.

Процедуре у раду безбедносних аналитичара најквалитетније су описане у научној и стручној теорији. Међутим, увек постоји простор да се, са научно-теоријског аспекта посматрано, те процедуре унапреде, што треба открити и доказати у истраживању. Овом приликом наводимо само неке од приступа који ће се користити у истраживању: 1) процедуре аналитичког процеса (Heuer & Pherson, 2015), 2) Британски National Intelligence Model – NIM (NCPE, 2005), 3) Европски криминалистичко-обавештајни модел – ECIM (Justice and Home Affairs Ministers Informal, 2005) и 4) Европолов документ SOCTA (Европол, 2013).

Примена метода и техника у раду аналитичара јесте један од најзначајнијих проблема уочених у пракси. Искуства показују да се морају укрштати научни методи верификовани у теорији и методолошки приступи које је изнедрила пракса.

Стандард, у општем смислу, дефинише се као норма и критеријум. Стандард је поновљиви, усаглашени, договорени и документовани начин на који је потребно нешто радити. Стандарди садрже техничке спецификације или друге прецизне критеријуме дизајниране да се доследно користе као правило, смерница или дефиниција. Помажу у поједностављивању живота и повећању поузданости и ефикасности многих добара и услуга које користимо. У основи, стандардизација процеса описује успостављање скупа правила која регулишу начин на који људи у компанији треба да испуне одређени задатак или низ задатака. Најпознатији вид стандардизације су ISO стандарди. Стандардизација је оквир споразума кога се морају придржавати све стране у компанији како би осигурале да се сви процеси који су повезани са стварањем производа или учинком услуге одвијају у складу са постављеним смерницама.

Познати су стандарди у разним доменима сектора безбедносне аналитике, као и процедурама рада аналитичара. Овом приликом истичемо само неке које ћемо анализирати у раду: 1) ANACAPA модел у криминалистичкој аналитици (Kopal & Korkut, 2022), 2) Стандарди еколошког сектора безбедности (Publications Office of the European Union, 2014), 3) Стандарди социјалне безбедности (Heinz-Herbert, 2002); 4) Стандарди економске безбедности (United Nations Commission on Sustainable Development, 2001) и 5) наведени National Intelligence Model – NIM.

Базе података су незаобилазан елеменат у безбедносној аналитици и раду аналитичара, пре свега у условима коришћења савремене ИТ технологије у свим аспектима креирања, иновирања и коришћења база.

Карактеристике савременог тероризма указују на тенденције промена у смислу стратегије, тактике, терористичких аката, финансирања и опште логистике терористичких организација и појединачних терориста. Све те аспекте савременог тероризма потребно је истражити зарад стварања оптималног модела за супротстављање тој пошасти.

Стратешка опредељења у супротстављању тероризму јесу нормативни прописи које доносе државе зарад супротстављања овом облику политичког насиља. Дакле, потребно је истражити основне поставке стратешких опредељења у свету, као и у нашој земљи. Тероризам је, због динамичности и мноштва појавних облика, тешко дефинисати. Такође, његов међународни карактер и неусаглашеност правних система различитих држава отежавају његово дефинисање и воде у селективно и субјективно одношење према овом феномену у пракси. Ово је само једна од препрека у супротстављању тероризму. У истраживању је потребно доћи до сазнања које су то све објективне и препреке субјективне природе које утичу на то да сузбијање тероризма нема потребну ефикасност.

Постојећи обавештајни циклус у супротстављању тероризму, примарно, своди се на процедуре рада аналитичара. То је, свакако, у пракси заживело и даје одређени резултат. Међутим, потребно је аналитичким поступком подврћи критици тај циклус и доћи до сазнања потреба његовог унапређења (оптимизације).

Ова глава операционализована је у следећа поглавља:

1. Сектори безбедности,
2. Процедуре рада аналитичара,
3. Методе и технике у безбедносној аналитици;
4. Базе података,
5. Стандарди у безбедносној аналитици и
6. Примена теоријског модела безбедносне аналитике у супротстављању тероризму.

ТРЕЋИ ДЕО

РЕЗУЛТАТИ ИСТРАЖИВАЊА

Истраживање у било којој делатности, а поготово научно, има свој теоријски и емпиријски део.

У *теоријском делу* истраживања неопходно је извести основне закључке по свим сегментима предмета рада до којих долазимо увидом у научне радове, студије, практикуме и друге службене документе, а који се односе на 1) теоријски модел безбедносне аналитике и 2) аналитику у супротстављању тероризму.

Емпиријски део резултата истраживања односи се, пре свега, на коришћење оних истраживачких метода које дају одговоре на комплетан истраживачки поступак са аспекта примене теоријског дела у пракси. У том смислу, незаобилазна метода у приказу резултата истраживања јесте испитивање експерата и приказ њихових ставова о понуђеном теоријском моделу безбедносне аналитике.

Свакако, посебан део резултата истраживања јесте примена теоријског модела безбедносне аналитике у супротстављању тероризму, примарно заснована на савременим базама података.

Ова глава се операционализује у следеће делове:

1. Резултати теоријског дела истраживања,
2. Резултати емпиријског дела истраживања и
3. Провера теоријског модела безбедносне аналитике на примеру супротстављања тероризму.

2.6 Временско одређење предмета истраживања

Предмет овог истраживања има прошлу, садашњу и будућу димензију. Распадом биполарног света тероризам као претња безбедности постаје све сложенији, те предмет истраживања тежишно временски сеже у прошлост до краја Хладног рата. У садашњем времену тероризам представља у готово свим земљама света највећу претњу безбедности и с тим у вези је и предмет истраживања везан и за данашњицу. Међутим, предмет истраживања сеже и у будућност, с обзиром на то да ће се нови модел безбедносне аналитике за борбу и спречавање тероризма посебно у будућности користити, при чему будуће време није могуће стриктно одредити.

2.7 Просторно одређење предмета истраживања

Просторна димензија овог истраживања се односи на цео свет с обзиром на глобални карактер тероризма као претње, а у ужем смислу на Републику Србију, јер се истраживање базира првенствено на раду и за рад система безбедности Републике Србије.

2.8 Дисциплинарно одређење предмета истраживања

Предмет истраживања тежишно припада наукама безбедности. Међутим, с обзиром на то да поједини сегменти истраживања припадају и психологији, социологији, правним и организационим наукама, може се констатовати да предмет истраживања има интердисциплинарни карактер.

2.9 Појмовно-категоријални систем

Основни појмови који на нивоу појмовно-категоријалног система имају везу са предметом истраживања јесу:

- *Тероризам* је намерна употреба или претња употребом насиља против цивила или цивилних мета ради постизања политичких, идеолошких и религиозних циљева.
- *Супротстављање тероризму* јесте стратешко опредељење усмерено ка превенцији и сузбијању те пошасти.
- *Анализа* је основна и почетна и основна метода сазнања у оквиру посебних научних метода помоћу које се у процесу истраживања и сазнања уопште реализује рашчлањивање предмета сазнања на посебне и појединачне делове, односно чиниоце структуре, функције, веза и односа у одређеном простору и времену (Сакан,
- *Аналитика* је првенствено интелектуална, организована, систематска, циљна и сврсисходна делатност усмерена ка стицању релативно истинитих, релативно тачних и употребљивих сазнања о претежно актуелним збивањима у разним областима људског и друштвеног живота (Даниловић и Милосављевић, 2008).
- *Безбедносна аналитика* је посебна врста аналитике којом се применом делотворних метода стичу релативно истинита сазнања из различитих извора о безбедносним појавама, потребна за рад субјеката система безбедности (Форца и Аночић, 2018).
- *Модел* је сваки теоријски, појмовни или стварни или појединачни или реални предмету истраживања аналогни систем, помоћу кога се истражује известан предмет или систем (Шешић, 1974).
- *Теоријски модел*. У класификацији модела, између осталих, разликујемо практичне, идеалне и идеализоване моделе. *Теоријски модел* јесте идеализовани модел, који делом

чине саставни делови праксе, а делом норме, захтеви, упутства и потребна знања усмерена ка пракси (Миљевић, 2007).

- *Креирање теоријског модела безбедносне аналитике* подразумева изградњу и сталну доградњу знања/доктрине о секторима безбедности, процедурама рада аналитичара и стандардима у тој области.
- *Сектори безбедности* су подручја у којима се испољавају изазови, ризици и претње безбедности, а акцептирају се као: политички, војни, економски; социјетални и еколошки сектор.
- *Процедуре рада аналитичара* јесу начин (поступак) који се примењује у безбедносној аналитици, примарно усмерен на методе и технике у раду, као и израду и коришћење база података.
- *Стандарди у безбедносној аналитици* подразумевају техничке спецификације или друге прецизне критеријуме дизајниране да се доследно користе као правило, смерница или дефиниција.

3. ЦИЉЕВИ ИСТРАЖИВАЊА

Имајући у виду сложеност предмета истраживања, може се идентификовати више циљева истраживања.

3.1 Нучни циљеви истраживања

Како наводи Сакан (2006): „Чињеница да се откриће не планира истаживачким пројектом никако не значи да открићу не треба тежити. Напротив, пожељно је да се тај циљ реализује у сваком истраживању. Оно се реализује преко научног објашњења повезаности, узрочно-последичне зависности и законитости“ (стр. 464). Нучни циљ истраживања је научно објашњење са тежњом ка научном открићу новог теоријског модела безбедносне аналитике и његова класификација и типологизација, као и дескрипција примене тог модела у борби и спречавању тероризма.

3.2 Друштвени (практични) циљеви истраживања

Друштвени циљ истраживања примарно јесте могућност примене резултата у научној теорији и наставном процесу, као и практичном раду безбедносних аналитичара.

Такође, резултати истраживања могу се применити и у унапређењу методологије научних истраживања сличних појава.

4. ХИПОТЕЗЕ И НАЧИН ЊИХОВЕ ПРОВЕРЕ

4.1 Генерална (општа) хипотеза

Теоријски модел безбедносне аналитике садржи доктрину, то јест потребна знања о секторима безбедности, процедуре рада аналитичара и стандарде у тој области, што се може приказати на примеру супротстављања тероризму.

Начин провере: доказивањем посебних хипотеза.

4.2 Прва посебна хипотеза истраживања

1. Знања/доктрина о секторима безбедности су део теоријског модела безбедносне аналитике.

Начин провере: анализа литературе и нормативне регулативе и ставови експерата.

4.3 Друга посебна хипотеза истраживања

2. Процедуре рада аналитичара су део теоријског модела безбедносне аналитике.

Начин провере: анализа теоријских извора и ставови експерата о процедурама рада аналитичара.

4.4 Трећа посебна хипотеза истраживања

3. Стандарди су део теоријског модела безбедносне аналитике.

Начин провере: анализа постојећих стандарда у области безбедности и компарација са критеријумима које су идентификовали експерти.

4.5 Четврта посебна хипотеза истраживања

4. Теоријски модел безбедносне аналитике могуће је проверити на примеру супротстављања тероризму.

Начин провере: израда модела аналитике у супротстављању тероризму применом савремених база података.

5. МЕТОДЕ

5.1 Основне методе сазнања и мишљења

С обзиром на сложеност предмета истраживања у овом истраживању биће примењенеосновне методе истраживања са посебним акцентом на конкретизацији, којом ће устаљена пракса безбедносне аналитике у раду служби безбедности бити превреднована новим теоријским моделом безбедносне аналитике.

5.2 Општенаучне методе истраживања

Од општенаучних метода примарна ће бити метода моделовања како би се утврдио нови теоријски модел безбедносне аналитике. Такође, користиће се и хипотетичко-дедуктивна метода како би се у нови теоријски модел безбедносне аналитике укључила и сазнања на основу друштвеног и научног искуства.

5.3 Методе за прикупљање података

Поред анализе садржаја докумената и доступне литературе у области безбедносне аналитике, рада обавештајних служби и борбе против тероризма, у овом истраживању посебно ће се користи метода испитивања кроз технику интервјуа, која треба да да бољи увид

у устаљену праксу служби безбедности и фазе аналитичког процеса у сектору безбедности. Метода испитивања ће се применити преко технике усмереног интервјуа, којој ће се подвргнути експерти из домена безбедносне аналитике.

6. ОЧЕКИВАНИ РЕЗУЛТАТИ

Кључни резултат планираног истраживања је у сазнавању новог теоријског модела безбедносне аналитике кроз његов опис и објашњење, те приказ на примеру супротстављања тероризму. Очекује се да резултати истраживања унапреде не само теорију, већ и праксу.

Обавештајни циклус је показао одређене мањкавости и пропусте када је спречавање тероризма у питању (пример напада на Куле близнакиње у САД). Један од резултата оваквог истраживања био би и одговор на питање како предупредити такве пропусте кроз стандардизацију аналитичког процеса. Такође, у раду ће бити приказани начини за коришћење отворених база података и јавно доступних (ОСИНТ) података у аналитичком процесу, што у будућности даје могућност за олакшавање процеса прикупљања података.

Друштвени допринос овог истраживања огледаће се у унапређењу теорије и праксе у области спречавања и борбе против тероризма, што ће за последицу имати и унапређење рада система безбедности у овој области. Нови понуђени модел безбедносне аналитике моћи ће да се примењује поред тероризма и на друге сродне облике угрожавања безбедности, од чега ће целокупно друштво имати користи.

ПРВИ ДЕО: КРИТИКА ПОСТОЈЕЋЕГ СТАЊА

У првом, теоријском делу, истраживање је усмерено на утврђивање стања теоријске одређености безбедносне аналитике и одређење према њеној прихватљивој дефиницији, с једне, те анализи функционисања безбедносне аналитике у пракси, с друге стране.

1. ТЕОРИЈСКО ОДРЕЂЕЊЕ БЕЗБЕДНОСНЕ АНАЛИТИКЕ

„Мудрост почиње дефиницијом појмова“ (Сократ у: Heuer & Pherson, 2015). Појмови су основа знања и у свакој предметној области образују један појмовно--категоријални апарат потребан за његово једнозначно разумевање. Сложени појам (синтагма) „безбедносна аналитика“ чине два појма (термина) „безбедносна“ као атрибут изведен из појма „безбедност“ и „аналитика“. Основни појам у синтагми јесте „аналитика“, док га атрибут „безбедносна“ ближе одређује, у смислу подручја у ком се „аналитика“ употребљава. Сваки од појединачних појмова синтагме „безбедносна аналитика“ теоријски је дефинисан, што уноси у синтагму, дајући јој ново, теоријско значење.

1.1 Појам и развој аналитике

Од момента када се пробуди, док поново не заспи, човек несвесно и свесно обави мноштво аналитичких процеса, од свакодневних процена до озбиљних анализа. Дакле, аналитика је саставни део како свакодневног тако и научног живота човека. У смислу Њутнове изреке: *Оно што знамо је капљица, оно што не знамо је море,* можемо посматрати целокупно човеково битисање. Да бисмо опстали и развијали се, пред нама је императив нових сазнања.

До нових сазнања можемо доћи на различите начине. Неки од њих су лична или пак туђа искуства. За научна сазнања користи се све оно што нам је наука до сада дала кроз образовање и оно до чега сами долазимо путем теоријских и емпиријских истраживања. Међутим, иза сваког сазнања директно или индиректно стоје аналитички процеси. Аналитика нам је неопходна како бисмо на основу постојећих сазнања и података дошли до нових. Путем чула и личног искуства добијамо сазнања о природним појавама и

друштвеним догађајима, док научним методама, то јест кроз емпиријска и теоријска истраживања, стичемо систематизована знања из одређене области. У процесу стицања сазнања посебну улогу имају аналитика и аналитичке методе.

За долажење до сазнања у аналитичким процедурама користе се, поред научних метода, и оперативне и све друге методе сазнања. Према изложеном, *аналитика је делатност стицања (и употребе) релативно истинитог, у одређене сврхе употребљивог сазнања систематски и континуирано, применом проверених, плодотворних, првенствено научних метода* (Термиз и Милосављевић, 2008).

Етимолошки, *аналитика* је реч грчког порекла и везује се за термин *анализа.* На грчком ἀναλύω (analýo) значи разрешити, анализирати (Грчки речник, 2022). Када помињемо *анализу,* требало би поменути да су још стари Грци уочили да ће неку појаву једноставније објаснити уколико је расставе на саставне делове и потом објасне сваки део појединачно. На сличан начин Фројд је тумачио анализу, сматрајући је процесом "растварања" концепта, првобитних података, мисли на "крајње" или једноставније саставне делове. Аналитика се као појам јавља и у Кантовој филозофији, у Аристотеловој логици. За Аристотела, она је синоним за формалну логику, а код Канта за гносеологију. Затим Квајн прави разлику између аналитичких истина и правих логистичких истина (Хемлин, 2001). Такође, занимљив је податак да се у енглеском речнику као синоним речи *аналитика* (*analytics*) појављује синтагма *у детаље* (*in detail*), што говори о још једном својству аналитике. Заправо, назив аналитика не осликава у пуном смислу дисциплину на коју се односи нити сва њена обележја, али је устаљен и општеприхваћен па се као такав и задржао.

Као наука, аналитика се развила у много праваца, покривајући различите сегменте људског рада и живота. У том смислу постоји више класификација аналитике и праваца њеног изучавања, а једна од значајних је класификација према предмету изучавања. Тако Даниловић и Милосављевић (2008) наводе да се „аналитике, по критеријуму предмета, могу класификовати и према областима изучавања. Тако се јасно разликују: 1) политичка (политичко-правна) аналитика; 2) војна; 3) полицијска; 4) царинска; 5) аналитика цивилне заштите; 6)економска итд. Неке од аналитика су комбиноване, јер обухватају истовремено више области. Таква је, на пример, безбедносна аналитика. Она је нужно и политичка, и правна и економска, па чак и биолошко-медицинска“ (стр. 15).

Постоји уверење да се појмом „аналитика“ не баве много ни теорија ни пракса, у општем смислу, па ни у било којој људској делатности. Врло често, кад је пракса у питању, аналитика се повезује са анализом, па чак и тако назива, у зависности од тога о којој делатности је реч. Свакако, анализа јесте неодвојиви део аналитике, али не и њен језички супституит у смислу садржаја и обима појмова „анализа“ и „аналитика“.

Аналитика је уско повезана са анализом, што можемо видети и из етимологије речи аналитика. Међутим, оно где се најчешће греши јесте код изједначавања аналитике и анализе. С обзиром на то да се аналитика развила из анализе, али је истовремено шири појам од ње, њихов однос није једноставан. То свакако није оправдање за њихово изједначавање, јер се ради о два различита појма. Анализа је заправо једна од фаза аналитике и може се изједначити са обрадом података. Тако, на пример, можемо анализирати својим чулима какво је време напољу без потребе да у ту анализу укључимо више извора и без потребе да проверавамо истинитост добијених података,. док је аналитички процес шири и састоји се из више фаза.

Аналитика се развијала и надопуњавала паралелно са методологијом научног истраживања и методиком. Можемо рећи да је циљ сваке аналитике да се стекне што потпуније сазнање о предмету истраживања и у ту сврху користе се научне методе. Како наводи Сакан (2006), ,,дијалектичка аналитичко-синтетичка метода масовно се примењује и у војним наукама, нарочито у борбеним дејствима. Целина борбеног дејства се, на пример, не може схватити без схватања делова, и обрнуто“ (стр. 245).

Значајан за прављење дистинкције између појмова „анализа“ и „аналитика“ јесте и међусобни однос садржаја и обима појма. Кључни методолошки став гласи: „Обим и садржај појма су обрнуто пропорционални када се ради о појмовима исте врсте или рода. Ако је обим широк, садржај је узак и обрнуто“ (https://filozofijagsm.files.wordpress.com/2019/09/obim-i-sadrzaj-1.pdf).

Анализу можемо посматрати као 1) научну методу из реда основних посебних научних метода и 2) практичан поступак сагледавања – разлагања било које друштвене појаве или творевине. *Анализа као научна метода* јесте „посебна научна метода сазнања која се остварује мисаоним или стварним растављањем неке целине и тако стиче одређено сазнање“. (Сакан, 2006).

Како истичу Термиз и Милосављевић (2008), применом методе анализе, почев од најједноставније – анализе садржаја, до каузалне анализе, ми углавном можемо да сазнамо: који делови или једноставнији чиниоци чине целину; у каквим односима и како повезани морају бити ти чиниоци да би сачињавали целину; какав им временски и просторни поредак мора бити да би сачињавали целину; какве су улога и функција сваког појединачног чиниоца у целини; какво је место чинилаца у целини; постоји ли и каква је способност сваког посебног чиниоца као засебне целине и каква је и колика способност и тежња појединачног чиниоца да се повеже, интегрише, уклопи у друге целине.

Термиз и Милосављевић (2008) утврђују етапе спровођења анализе као: дефинисање предмета сазнања; избор и дефинисање целина које ће бити анализиране; дефинисање и избор извора сазнања о проучаваном предмету; избор врсте, типа и процедуре анализе који ће бити примењен и на крају, утврђивање резултата анализе и њихову смисаону и функционалну презентацију (Исто). На крају приказане опсервације анализе као научне методе, Термиз и Милосављевић (2008) закључују: „Полазне основе етапа анализе указују на чињеницу да анализа не омогућава довољно сазнања да би се могао сазнати и ваљано схватити један целовити процес или целовит део процеса, нити се само њоме може схватити једна друштвена појава, систем или низ појава. Очигледно, потребне су и друге методе!“ (Исто). *Анализа као практична делатност* нема и не мора *a priori,* да има искључиво научни карактер. На пример, анализа неког обављеног посла (екскурзија, пословање фирме у протеклој години, саобраћајни удес…) или анализа неког објекта (предмета) или уметничке творевине (анализа мобилног телефона као предмета, анализа песме). Дакле, анализа као практична делатност, примарно, сагледава шта се и како догодило, шта је и како речено, из чега се нешто састоји и слично.

Да би се нека појава, процес или систем схватили и разумели у потпуности, очевидно, поред анализе, потребне су и друге методе и поступци. То „разумевање у потпуности“, кад су друштвене појаве у питању, поред тога шта се, када и где догодило, захтева и сазнања по питањима: зашто се догодило, како се догодило, какве то последице може да има и како се припремити – реаговати у односу на могуће последице. Једном речју – потребна је „аналитика“.

Нађо Даниловић, који је са Славољубом Милосављевићем утврдио дефиницију „аналитике“ коју смо навели у уводу, у каснијим радовима је еволуирао. Наиме,

Даниловић не пориче дефиницију аналитике коју је дао с Милосављевићем, као и дефиницију коју су дали Термиз и Милосављевић, али истиче:

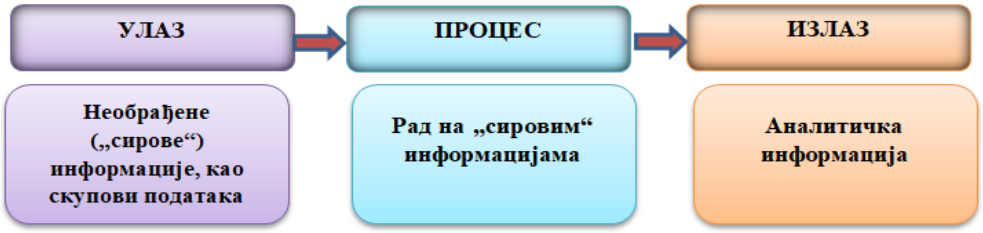
> „Назив ‚аналитика' не обухвата у целини њену делатност нити сва битна обележја битних одредаба и њене манифестације као друштвене појаве. Напротив, назив ‚аналитика' исказује само почетну фазу и полазни метод сазнања – анализу, која служи у почетку сазнавања, заједно са аналогијом и, разумљиво, другим аналитичким методама. У том смислу, назив ‚аналитика' је једностран, али зато што је уобичајен, остајемо и даље при његовој употреби. Аналитичка сазнања (сазнања до којих се долази процедурама аналитике) стичу се коришћењем свих основних метода сазнања, општенаучних метода и првенствено применом оперативне методе ‚анализа садржаја докумената'. Дакле, назив ‚аналитика' прихватамо искључиво као номиналан, а не као суштински и свеобухватан" (Даниловић, Манојловић, 2024: 15).

У складу с наведеним, Даниловић и Манојловић (2024) уместо речи „аналитика", користе синтагму „аналитички процес", за који кажу да је: „повезано деловање субјеката аналитичке делатности у циљу произвођења последица у чијој основи је коначно аналитичко дело (студија, збирка, извештај, информација, уметничка творевина и слично) у основи повезано" (стр. 16).

На основу претходне опште представе садржаја и обима појма може се закључити да је „аналитика" (аналитички процес) сложен истраживачки процес, који користи више научних метода. У том смислу, условно, „аналитика" је *родни појам* за „анализу", као појам на нивоу *врсте*.

У претходном ставу употребили смо реч „условно" кад је у питању однос „аналитике" и „анализе". Зашто? Зато што аналитика у себи садржи и методолошки и методски приступ односно, аналитика, поред недвосмислене потребе за коришћењем научних метода, у истраживачком поступку (процесу) користи и методе и поступке који се не сматрају научним. Коришћење научних и ненаучних метода и поступака саставни је део истраживачког рада, али и сваке организоване људске делатности. Стога, аналитика је свеприсутна у животу и раду људи и њихових заједница и организованих облика деловања.

Основни предмет аналитике јесте *информација*. Информација, у општем смислу посматрано, јесте скуп повезаних података или (са)знање о нечему (некоме). Аналитика је процес рада на (са) информацијама, који од скупа улазних података и информација, применом разних метода и методолошких поступака, као излаз даје нову информацију – (са)знање (Слика 1).



Слика 1. *Аналитика као процес рада на информацијама*

Извор: *Обрада ауторке дисертације*

Аналитички процеси, у суштини, базирају се на научним истраживањима, те је и аналитичка делатност у својој бити истраживачка. Уједно, аналитика је вишедимензионална дисциплина, што значи да се примењује у више других научних дисциплина којима се помаже у истраживањима. Логично је да се од аналитике захтева да понуди истинита сазнања, што пред аналитичаре увек ставља једну недоумицу – *шта је истина*? У трагању за одоговором на наведено питање морали бисмо да уђемо у сферу науке, филозофије, религије и уметности, што свакако није примарни циљ истраживања. Једноставно, без анализе појма „истина“ у наведеним областима, закључујемо да *апсолутна истина не постоји*. У том смислу, сва сазнања која нуди аналитика, ма колико појавно изгледало да у потпуности одговарају објективној стварности, именујемо као *релативно истинита сазнања*. То, свакако, не значи да се од аналитичара не захтева да у свом раду не теже максимално могућим (проверљивим) информацијама – сазнањима.

У складу с наведеним, може се сматрати коректном дефиниција аналитике коју су дали Даниловић и Милосављевић, а која је наведена у претходном тексту.

Из наведене дефиниције требало би да уочимо *функцију* и одредимо је према *врстама* аналитике.

Функција аналитике, у појмовном смислу, може да се посматра са два аспекта, – 1) као мисија (сврха и циљ) и 2) као скуп послова и активности. На овом месту примарно нас интересује мисија (сврха и циљ) аналитике, а о пословима и активностима говорићемо у питању о процедурама у безбедносној аналитици.

Из дефиниције аналитике коју су дали Даниловић и Милосављевић можемо да кажемо да је циљ – сврха (функција) аналитике да **за некога** прибави релативно истинита

сазнања **о нечему (о некоме)**. У наведеном смислу, аналитика има за циљ (сврху) да информише о нечему (некоме), или – *информативну функцију (дескрипција)*. Та информативна функција, кад су друштвене појаве у питању, најчешће има карактер *ex post facto*, односно информише шта, када и где се нешто догодило или се догађа. Међутим, с обзиром на то да је аналитика сврховита делатност, одговори на питања шта, где и када нису довољни за укупну спознају о некој појави. Стога, постоји потреба да се прибаве сазнања о томе зашто се нешто догодило (догађа), али и што више информација о томе како ће се то дешавати убудуће и шта, у вези с тим, треба чинити. Дакле, долазимо до тога да аналитика некога инструише, као и да прогнозира будућност анализиране појаве, де даје препоруке како се понашати. У складу с наведеним, долазимо до основних функција аналитике као мисије, које се могу именовати као: *дескрипција, дијагностика, прескрипција* и *предикција* (Слика 2). Те функције аналитике, као мисију, можемо једним именом назвати – *оперативна аналитика.*

Слика 2. *Функције аналитике*

Извор: *Обрада ауторке дисертације*

Дескриптивна, то јест информациона функција аналитике примарно се бави доласком до истинитих података о томе шта се догодило или се догађа, те извештавањем о томе и складиштењем података/информација. *Дијагностичка* функција аналитике, примарно се бави доласком до истинитих података о томе зашто се нешто догодило/догађа, анализирајући понашање у некој делатности и утврђивањем кореалација међу појавама и учесницима. *Прескриптивна* функција аналитике примарно се бави будућим стањем, односно предвиђањем будућих појава у односној делатности, у чему се ослања на дескрипцију и дијагностику, али користећи разне методе тежи ка прибављању додатних података и информација за закључивање.

Није ретко да аналитика поред својих основних функција које се огледају у долажењу до потребних сазнања има и предиктивну функцију. Често је неопходно, након анализе постојећег стања у некој области и извођења закључака, предвидети како ће се нека појава кретати у будућности. Ова врста аналитике назива се *предиктивна аналитика*. *Предиктивна аналитика* (predictive analytics) иначе представља скуп напредних алата и техника које се користе у анализи великих серија прошлих и садашњих података како би се предвидели будући догађаји на бази идентификованих образаца понашања (Лазаревић, 2015). *Предиктивна* функција аналитике, примарно, бави се предлагањем шта и зашто нешто треба радити у одређеној делатности, како би се моделовале и оптимизирале одлуке за будуће стање и функционисање предметне делатности.

На крају, посебна функција оперативне аналитике, као њен неизоставни организациони део, јесте *евиденциона аналитика*. Сама реч каже, ради се о евидентирању (записивању и памћењу у базама података) огромног броја информација до којих дође оперативна аналитика.

Посебна функција аналитике, која се може одвојено посматрати од наведених, јесте *научно-истраживачка*. Њена посебност, пре свега, огледа се у томе што није везана за конкретан проблем са аспекта оперативних потреба аналитичких органа, већ се, с примарно научних потреба, бави аналитиком појава у одређеној делатности на различитим нивоима општости. Свакако, научно-истраживачка аналитика користи резултате оперативне аналитике, као што се и њени резултати могу користити у оперативном раду аналитичара.

Данас се аналитика користи широко и у природним и у друштвеним наукама. Често се везује и за информационе технологије, где се ослања на примену статистике, компјутерског програмирања и операционих истраживања која се квантитативно обрађују. Заправо, аналитички процеси који се одвијају уз употребу одређених софтвера су популарни када је потребно обрадити велику количину података (тзв. Big Data). Велики број података може представљати проблем за многе фирме које раде кроз трансакциони систем онлајн и као негативан резултат се добијају велике количине података у веома кратком временском интервалу (Naone, 2010). Тада софтвери преузимају улогу аналитичара и у том контексту помиње се и напредна аналитика. Затим,

аналитика се примењује у пословању и индустрији у истаживању тржишта. Аналитиком тржишта проучавају се атрактивност и динамика посебног тржишта у посебној индустрији. Кроз ово се анализирају детаљно предности, слабости, могућности, као и претње једне компаније које у датом тренутку могу да се идентификују. На крају, уз помоћ анализе и адекватне пословне стратегије, компанија ће дефинисати проблеме и спречити исте (Dilerupand & Stoi, 2006).

На овом нивоу анализе може се констатовати да постоји онолико врста аналитике колико и подручја људске и друштвене делатности. Све наведене врсте аналитике имају додира са једном од најзначајнијих грана аналитике, а то је безбедносна аналитика. С обзиром на глобалне промене које су се дешавале од Другог светског рата па до данас, безбедносни подаци, њихова обрада и извођење закључака и предикција на основу њих постали су изузетно важни.

1.2 Безбедност

Други појам у синтагми „безбедносна аналитика“ који треба ближе одредити јесте „безбедност“, јер је из тог појма изведен атрибут „безбедносна“. Да бисмо прецизније утврдили шта је и шта све обухвата безбедносна аналитика, неопходан је шири захват појма „безбедност“. У складу с предметом истраживања, посебну пажњу заслужују два аспекта безбедности, а то су 1) системски приступ безбедности и 2) системи безбедности.

1.2.1 Системски приступ безбедности

Од изворног (грчки и латински језик) значења, реч „безбедност“ се у бројним језицима на сличан начин поима, а најчешће као одсуство опасности (беде, страха…). Међутим, реч „безбедност“ се изузетно широко користи у бројним људским и друштвеним делатностима те је, с тим у вези, попримила шира теоријска и практична значења. Отуда, у теоријским радовима се уобичајено истиче да појам безбедност нема једнозначно утврђену дефиницију.

Одсуство опасности (претње) професор Бери Бузан (Barry Buzan) је узимао за своје опште одређење безбедности, истичући да је то 1) „тежња ка слободи од претњи“ (Buzan, 1991: 18) или 2) „одсуство претњи по референтни објекат безбедности“ (Buzan, 1983). Управо други став Бузана о безбедности узећемо као опредељујући у промишљању

безбедности у овом питању. Наиме, постављају се два питања – 1) које су то претње безбедности и 2) ко (шта) је референтни објект безбедности.

Кад су у питању *претње безбедности*, Бери Бузан сам, а касније са својим сарадницима из Копенхашке школе безбедности[2], заслужан је за тзв. проширење појма безбедност. Наиме, дуго је основна претња безбедности долазила из војне сфере (сектора) и поимана је као рат. Бузан и сарадници су развили теорију о *секторима безбедности*, у којој су утврдили и друге области које угрожавају безбедност људских заједница осим војне, као што су: политичка, економска, социјетална (друштвена) и еколошка (Buzan, Waever and De Wilde, 1998). Претеча секторском приступу безбедности, који су развили истраживачи Копенхашке школе безбедности, јесу рани радови професора Бузана о *областима утицаја на безбедност људских заједница* (Buzan, 1983), Табела 1.

Табела 1. *Области утицаја на безбедност људских заједница*

Политичка	Усредсређује се на организацију стабилности држава, система владања и најбољих идеологија које им дају легитимитет
Војна	Међународно деловање офанзивних и дефанзивних потенцијала државе и тога како поједине државе опажају намере оних других. Истраживање војне безбедности је подскуп студија безбедности – СТРАТЕШКЕ СТУДИЈЕ
Економска	Односи се на приступ ресурсима, финансијама и тржиштима неопходним за одржавање прихватљивог нивоа благостања и моћи државе
Социјетална	Усредсређена на одржавање и развој традиционалних образаца језика, културе и религијског и националног идентитета и обичаја
Еколошка	Тиче се очувања локалне и планетарне биосфере као суштинског потпорног система од којег зависе сви други људски подухвати

Извор: *Buzan, 1983 (обрада ауторке дисертације)*

С друге стране, кад је *референтни обејкт безбедности* у питању, а посебном заслугом Велшке школе безбедности[3], дошло је и до тзв. продубљења појма безбедност са нивоа државе: наниже – ка појединцу и навише – ка глобалној безбедности. У том смислу, референтни објект безбедности јесте човек појединац, друштво, држава,

[2] Копенхашка школа безбедности формирана је у оквиру Института за истраживање мира – COPRI у Копенхагену (Данска) 1985. године. У оквиру научних програма њене три основне идеје по којима је запамћена у теорији јесу: 1) Теорија секуритизације, 2) Теорија сектора безбедности и 3) Теорија регионалних безбедносних комплекса. (Види: Форца, Б., *Савремене теорије безбедности*, Факултет за пословне студије и право, Београд, 2022.).

[3] Професор Кен Бут је заједно са својим сарадником Ричардом Вин-Џоунсом, на Универзитету Аберистwит основао постдипломски студијски програм назван Критичке студије безбедности, који је претеча тзв. Велшке школе безбедности. Критички осврт на безбедност негира државоцентрични приступ безбедности и продубљујући појам безбедност, примарно се окреће другим референтним објектима, као што су појединац и друштвене групе, односно глобално (Види: Ејдус, Ф., *Међународна безбедност, теорије, сектори и нивои*, „Службени гласник“, Београд, 2012.).

међународни поредак и све на планети Земљи (биодиверзитет, животна средина). У складу с наведеним, у научној теорији је дошло до развоја *концепата безбедности*, који се примарно акцептирају као: 1) људска безбедност, национална (безбедност државе) безбедност, међународна безбедност и глобална безбедност, кад је референтни објект, односно нивои безбедности у питању и 2) политичка, економска, војна, социјетална и еколошка безбедност, кад су у питању сектори (равни), односно извори претњи безбедности (Форца, 2022).

Сагледавајући наведене концепте безбедности обједињено могу се генерализовати два савремена теоријска приступа безбедности: *државоцентрични* и *друштвеноцентрични*. У теорији конвергирају ставови да, због улоге државе у међународним односима, државоцентрични приступ безбедности јесте доминантан и да датира од настанка модерних држава у Европи из 16. и 17. века, посебно од Вестфалског мира[4] (1648).

1.2.1.1 Државоцентрични приступ безбедности

Држава је, Конвенцијом из Монтевидеа (1933), дефинисана на следећи начин: „Држава као субјект међународног права мора поседовати следеће квалификације: 1) перманентно становништво, 2) утврђену територију, 3) владу и 4) капацитете да уђе у односе са другим државама“ (Форца, 2021). Тако, држава с наведеним ентитетима постаје референтни објект безбедности, а кључна опасност долази од друге државе (држава) и, пре свега, испољава се као војна претња. Два светска рата у 20. веку постала су плодно тло за два приступа државоцентричној безбедности.

Прво, развијена је теорија истраживачког правца – *реализам*, која у фокус међународних односа ставља државу, а у достизању безбедности фаворизује њену моћ, пре свега војну (Шире у: Вилијамс, 2012). С друге стране, трају покушаји да се успостави систем колективне међународне безбедности, који ће предупредити рат, као облик решавања спорова међу државама. Тако су настале међународне владине организације – Лига (Друштво) народа и Организација уједињених нација. Лига народа је била кратког

[4] Дана 24. октобра 1648. године у Минстеру и Оснабрику је закључен Вестфалски мировни споразум, који је означавао крај тридесетогодишњег рата. У европској историји се тај рат поима као граница између феудалног друштва и настанка модерног доба. Био је то последњи рат који је вођен „под заставом вере“ (католичке) (Види: Дугин, А., *Вестфалският мир,* доступоно на https://pogled.info/svetoven/aleksandar-dugin-vestfalskiyat-mir.135488, 14. 1. 2024).

даха и распала се пред Други светски рат. Организацију уједињених нација након Другог светског рата, примарно, створиле су велике силе, које ће у скоро осам деценија постојања те организације имати пресудну улогу у њеном успеху и неуспеху да се постигну и одржавају међународни мир и безбедност.

Пола века након Другог светског рата велике силе (САД и СССР) и њихови блокови (НАТО и ВУ) држали су свет у страху од новог великог рата. Иако се велики рат међу силама није догодио, свет је био оптерећен бројним регионалним и локалним сукобима, у којима су директно или индиректно учествовале велике силе. А онда се све мало смирило, јер је једна од страна (СССР и ВУ) изгубила тзв. Хладни рат, што је искористила друга страна (САД) у намери да загосподари светом. Привидни мир је трајао кратко, до 2022. године, када је Русија војно напала Украјину. Свет је поново на ивици великог рата.

Зашто је то тако?

Безбедност државе супституисана је појмом *национална безбедност*. Формално-логички посматране ентитете државе – територија (призната), становништво и власт, „заменили“ су појмови *националне вредности, интереси* и *циљеви*. Тако, појам безбедности добио је једно тзв. објективно-субјективно гледиште, које је својевремено Волферс (Arnold Oscar Wolfers, 1952) исказао ставом: „…безбедност мери објективно одсуство претњи усвојеним вредностима, а у субјективном погледу значи одсуство страха да ће те вредности бити нападнуте*“*. Иако је Волферс употребио општи појам *вредности,* тај појам се с временом изгубио у међународним односима, а потиснуо га је појам филозофије прагматизма – (национални) *интереси* (и *циљеви*). Иако се појам „интереси“, најчешће, сматра вишим нивоом општости од појма „циљеви“, међу тим појмовима не постоји експлицитно јасна разлика, при чему се они понекад поистовећују, а чак се негде циљеви сматрају оштијим од интереса (Форца, 2022).

Тријада (националне) *вредности, интереси* и *циљеви* унела је збрку у теоријску расправу студија безбедности и, поготово, неред у пракси међународних односа. Тако, готово парадоксално звучи да све земље на сличан начин утврђују националне вредности, док се кључне разлике појављују у артикулисању и, поготово, у начину остваривања националних интереса и реализацији националних циљева. Национални интереси (и циљеви) постали су праоснова/праузрок свих сукоба у међународним односима, поготово међу великим силама (Вишњић, 1995). Та чињеница утицала је на то да се у теорији делом

ревидира Волферсов став о безбедности. Тако, полазећи од става да су националне вредности и интереси потребе државе које проистичу и из њеног места и улоге у међународним односима, национална безбедност се поима као: „Способност државе да самостално или у сарадњи са другим државама или организацијама заштити виталне вредности и интересе друштва од спољних и унутрашњих облика угрожавања и да тиме обезбеди опште услове за несметан политички, економски, социјални и културни развој друштва и благостање својих грађана“ (Стајић и Гаћиновић, 2007: 57).

Да је државоцентрични приступ безбедности доминантан у теорији и пракси после Другог светског рата, указује и дефиниција безбедности коју су дале Уједињене нације у својој студији из 1986. године, у којој се за безбедност каже да је то: „Стање у коме државе сматрају да нема опасности од војног напада, политичког притиска или економске присиле, тако да могу слободно да се развијају и напредују“ (Стајић, 2013).

1.2.1.2 Друштвеноцентрични приступ безбедности

Много тога се променило у промишљању безбедности након Хладног рата, пре свега у глобалном смислу, односно на нивоу који ниједна држава није сама у могућности да реши. Такву ситуацију (глобални проблем) Софија Дах (Zofia Dach) појашњава на основу четири параметра: „1) глобални проблем има ‚целосветски карактер', он се тиче свих народа и држава; 2) угрожава целокупно ‚међународно друштво'; 3) њихова актуелност захтева хитна решења; 4) захтевају ангажман међународне заједнице и ‚међународног друштва'. Државе појединачно нису способне да их саме реше“ (Dach', 2009: 13). Практичан пример ставова које износи Дахова налазимо у стратешком документу Немачке (*Бела књига*) с почетка овог века (2006), где стоји:

> „Велики број нових безбедносних ризика и изазова који утичу на нашу безбедност чак и на великим удаљеностима, прате процес глобализације, транснационалног карактера су и тичу се недржавних актера. Сиромаштво, неразвијеност, лоше образовање, недостатак ресурса, природне катастрофе, уништавање животне средине, болести, неједнакост и кршење људских права, само су неки од фактора који пружају плодно тле за илегалне миграције и како секуларни, тако и религијски екстремизам. На такав начин, ови ризици и изазови могу постати узрок нестабилности, и у свом најрадикалнијем облику, створити пут за међународни тероризам. У све тешње повезаном свету, ови ризици не само да имају утицај на непосредно окружење, већ утичу на различите начине и на безбедност међународне заједнице у целини. Кључне претње су: тероризам, пролиферација оружја, регионални конфликти, енергетска безбедност, миграције, епидемије и пандемије“ (Bundesministerium der Verteidigung, 2006: 18-20).

Померање фокуса безбедности са државе и војне претње као основне, у теоријском смислу посматрано, почело је наведеним тзв. проширењем и продубљењем самог појма безбедност, за који су заслужне Копенхашка и Велшка школа безбедности.

Теорију секуритизације започео је професор Копенхашке школе Оле Вивер (Weaver**,** 1989) и наставио је са сарадницима - Беријем Бузаном и Јапом де Вилдеом. Основно питање теорије наведених аутора било је: *Зашто се неке појаве третирају као безбедносне претње, а друге не"*.[5] Теорија секуритизације безбедност смешта у домен политике, односно политичког дискурса, у коме: „секуритизујући чинилац одређује неку појединy ствар или чиниоца као ‘‚егзистенцијалну претњу’ појединoм референтном објекту, а тај потез се прихвата од стране релевантне публике" (Вилијамс, 2012: 120). Секуритизујући чинилац су политичке елите, а публика је јавност (народ). Тако, Оле Вивер (1995) је концептуализовао безбедност „као дискурс којим политичке елите идентификију претње и од друштва захтевају легитимитет за примену специјалних мера како би се бориле против тих претњи". За Вивера је безбедност „говорни чин", „који формулише одређени политички проблем као посебно значајан за опстанак заједнице и тако га премешта ван поља утврђених правила игре. Тако, безбедносно питање (претња), практично, може да постане све и свашта „(Ејдус, 2012: 107).

Потпунији увид у дилему – *шта се све може сматрати безбедносним питањем* (претње), добијамо ако анализирамо шта су поједини аналитичари и међународне организације сврстали у *концепт људске безбедности*. Фен Ослер Хамсон, позивајући се на бројне ауторе и званичну ОУН, тврди да постоје три различите концепције *људске безбедности* које обликују теоријске расправе:

> „**Прва**, која се може означити као *природна права/владавина закона*, која има упориште у основној либералној претпоставци о основним индивидуалним правима на живот, слободу и тежњу ка срећи, и у обавези међународне заједнице је да заштити и унапређује та права. **Друго** гледиште о људској безбедности је *хуманитарно*. То гледиште, на пример, прожима међународна настојања да се продуби и оснажи међународно право, нарочито у погледу геноцида и ратних злочина и да се униште оружја која су посебно штетна по цивиле и

[5] Према подацима Светске здравствене организације, у 91% смртних случајева у свету, узрок смрти је болест, док колективно насиље представља узрок смрти тек у 0,4% случајева. Осим тога, према подацима Светске банке, од сиромаштва премине шест милиона људи годишње, од цигарета три милиона, а од ХИВ вируса дневно оболи 14.000 људи. Ипак, у одбрану и безбедност, а посебно у светску борбу против тероризма, улаже се далеко више средстава него у решавање наведених проблема. **Ејдус, Ф.,** (2012), оп. цит., стр. 106.

неборце. **Треће** гледиште, које надопуњује претходна два, јесте најшире и у себе уноси *социјални елеменат*, а разматрају се: глобална економија, силе глобализације, здравље, животна средина, у смислу легитимне забринутости због утицаја на безбедност појединца“ (Вилијамс, 2012: 306).

У извештају УНДП из 1994, експерти Уједињених нација дају једну седмодимензионалну матрицу изазова људској безбедности независно од простора и система у коме живе:

1. *Економска безбедност* суочава се са претњама назапослености, несигурности радног места, лошим условима на послу, неједнакостима у погледу прихода, инфлацијом, слабо развијеном мрежом социјалног осигурања и бескућништвом.
2. *Безбедност у погледу хране* остварује се решавањем проблема који се односе на физички и економски приступ храни. Људи гладују не зато што хране нема, него зато јер не могу да је приуште.
3. *Здравствена безбедност* бави се претњама по живот и здравље људи изазваним инфективним и паразитским болестима, ХИВ-ом и другим вирусима, болестима изазваним загађеним ваздухом или водом, као и неадекватним приступом здравственим службама.
4. *Еколошка безбедност* спречава деградацију локалних и глобалних екосистема, несташицу воде, поплаве и друге природне катастрофе, нерационално крчење шума, као и загађивање воде, ваздуха и земљишта.
5. *Лична безбедност* бави се сузбијањем претњи које могу имати неколико облика: тортура од стране државе (физичко насиље), претње од других држава (рат), претње од друге групе људи (етничке тензије), претње од појединаца или криминалних група (криминал или улично насиље), претње усмерене ка женама (силовање и насиље у породици), претње усмерене ка деци (злостављање) и претње усмерене ка себи самом (самоубиство, употреба дрога).
6. *Безбедност заједнице* суочава се са етничким тензијама и насилним сукобима.
7. *Политичка безбедност* представља један од најважнијих аспеката људске безбедности и подразумева живот у таквом друштву које поштује основна људска права и не спроводи државну репресију (УНДП, 1994: 24-33).

У складу с претхотдно наведена два аспекта поимања људске безбедности, поједини аутори тај приступ именују као *хуманитаран* („нови хуманизам“) и као алтернативу државној и националној безбедности, сматрајући да појединац и друштвене групе јесу прави референтни објект безбедности посматран кроз седам димензија које су утврдиле УН (УНДП). У том смислу, за државну, националну и глобалну безбедност се каже да су неоправдано преовладавајуће, јер:

„Под изговором постизања и очувања националне и државне безбедности, заташкавају се афере и малверзације кључних политичких фигура у једном друштву; заштиту и поштовање људских права (како се, поједностављено, гледа на људску безбедност), промовишу највеће светске силе, чиме правдају властити интервенционизам у деловима света који за њих имају стратегијску важност; идеју регионалне, а нарочито, глобалне безбедности, најчешће заговарају они којима постојећа констелација међународних односа, одговара, те се из петних жила боре против оних који би да тај статус кво поремете и тако даље“ (Стојановић, 2012).

Одвојена анализа државоцентричног и друштвеноцентричног приступа безбедности оправдана је с теоријског аспекта посматрано. Међутим, чињеница је да нема ниједног питања безбедности којим се не баве државе, односно које се без улоге државе може решити. Безброј је потврда наведеног става у пракси, а наводимо неке актуелне примере:

1) *Пандемија вируса корона* захватила је цео свет. Кључну улогу у њеном сузбијању одиграле су државе, не занемарујући Светску здравствену организацију, као ни фирме које су произвеле вакцине[6].
2) *Глобално загревање атмосфере* јесте претња коју производе државе, односно њихова индустрија. Без обзира на светску организацију која то питање разматра, смањење загревања атмофере могу да реше једино државе својим одлукама и њиховом реализацијом у пракси[7].
3) *Војна претња* и даље остаје као једна од најтежих по људске животе и материјалну и нематеријалну имовину. Војне претње, примарно, долазе од држава и, у условима нефункционисања Савете безбедности УН, ратне сукобе преговорима могу да реше само државе. Пример рата у Украјини од фебруара 2022. је најбоља потврда наведеном[8].
4) *Тероризам* је глобална претња безбедности која не познаје државне границе. Међутим, значајније ангажовање држава света и ОУН у борби против тероризма почиње тек након терористичких напада на Њујорк и Вашингтон 11. 9. 2001. године. Приступи држава света у борби против тероризма су врло различити, али је чињеница да једино заједничко деловање држава може дати резултат[9].
5) *Организовани криминал*, посебно нерегуларна трговина људима, оружјем, наркотицима, јесте претња безбедности која не познаје државне границе. У борби

[6] На дан 19. 11. 2022. године, у свету је од вируса корона било заражено око 626 милиона особа, од чега је преко 6,5 милиона преминуло. И поред великих губитака (1%), највећу заслугу за сузбијање пандемије имају државе и њихови здравствени системи. Иако пандемија није потпуно обустављена, ипак је значајно умањено њено дејство. Доступно на: https://covid19.rs/ (5. 1. 2024).

[7] Од 1992. године (Оквирна конвенција УН о промени климе) трају напори ОУН да се смање ефекти „стаклене баште“ који настају загревањем атмосфере. Ти напори су појачани Кјото споразумом (Јапан) из 1997, који је ступио на снагу 2005. године. Такође, 2015. године у Паризу државе су се сагласиле о смањењу емитовања штетних гасова у атмосферу. Међутим, стање се није побољшало, напротив. Основни разлог за то јесте чињеница да су највеће силе и највећи загађивачи атмосфере. Доступно на: https://ekoblog.info/globalno-zagrevanje-konvencije/; 5. 1. 2024.

[8] Русија је 24. 2. 2022. године извршила агресију на Украјину. Савет безбедности је блокиран, а резолуције које доноси Генерална скупштина УН немају обавезујући карактер и не производе правно дејство. Оружани сукоб Русије и Украјине претворио се у сведимензионални сукоб Русије и западних земаља, које предводе САД. Размере и могући исход сукоба је тешко предвидети, али је сигурно да без међудржавних преговора нема решења.

[9] Терористичке организације примарно се формирају у муслиманским државама, а њихова дејства, осим у непосредном окружењу, усмерена су на развијене државе, пре свега ЕУ. Према налазима Европола за 2020. и 2019. годину, број терористичких аката у земљама ЕУ, иако је у благом паду, увек је преко 100. Доступно на: https://www.ips.ac.rs/wp-content/uploads/2020/10/PR-65-1.pdf, 5. 1. 2024.

против те пошасти, једино заједничко деловање држава на међународном плану и државе понаособ, на унутрашњем плану, може дати позитиван резултат[10].

6) *Масовне миграције* су постале једна од највећих претњи безбедности савременог света[11]. Чињеница је да ниједна држава сама не може да реши тај проблем. Да је то тако, показала је и мигрантска криза која је захватила ЕУ од 2015. године, подривајући темеље њеног опстанка[12]. Стога, чињеница је да само сарадња међу државама може дати позитиван резултат, јер нема тог механизма у међународним односима који би државе могао да замени.

У складу с наведеним, обједињени приступ безбедности примарно подразумева националну безбедност, која обухвата и безбедност појединца и друштва с једне, и уважава успостављени систем међународне (заједничке и/или глобалне) безбедности, с друге стране. Тако посматрана, национална безбедност има *унутрашњу и спољну компоненту,* које се испољавају јединствено и недељиво као *интегрална безбедност* (Стајић, 2021).

1.2.1.3 Спољна компонента безбедности

Од постанка државе, њена спољна безбедност је била примарна, а испољавала се у одбрани територијалног интегритета и суверености. Дакле, референтни објект безбедности је држава (границе и сувереност) и њена равноправност чланства у

[10] *Организовани криминал* је пошаст савременог света која не познаје границе, урушава привреду сваке земље, а на глобалном плану представља један од највећих безбедносних проблема. Посебно негативан утицај на безбедност имају ирегуларна трговина оружјем, наркотицима и људима. Финансијска добит у домену организованог криминала мери се стотинама и хиљадама милијарди долара. Тако, на пример, за 2022. годину се истиче податак да се само од трговине људима стиче добит од преко 152 милијарде долара на годишњем нивоу. Доступно на: https://www.rts.rs/page/stories/sr/story/125/drustvo/4801536/trgovina-ljudima.html; 5. 1. 2024. Кад је трговина дрогом у питању, у 2020. години је само у ј/и Европи заплењено између 60 и 65 тона дроге у вредности од око милијарду долара, а то је само мали део светске трговине. Доступно на: https://globalinitiative.net/wp-content/uploads/2022/01/IFFs2-BCMS.pdf, 5. 1. 2024. Трговина оружјем је један од најуноснијих бизниса, поготово за најразвијеније државе света, који се мери стотинама милијарди долара. У 2021. години америчке компаније су остариле 51% укупне светске трговине оружјем, а европске (кумулативно) 27%, Кина 18%, а Русија свега 4%. Међутим, трговина оружјем има и свој ирегуларни ток, у коме предњаче државе, утицајне фирме и појединци. У том смислу, врло је опасна спрега илегалне трговине оружјем и тероризма.

[11] Према подацима УНХЦР, на крају 2021. године у свету је 89,3 милиона присилно расељених лица. При томе, преко 27 милиона су избеглице, а око 53 милиона интерно расељена лица. Доступно на: https://www.unhcr.org/rs/; 5. 1. 2024.

[12] Притисак миграната са ратом захваћених подручја Блиског истока и Африке, који је посебно евидентан од 2015. године, довео је до дијаметралних погледа земаља чланица ЕУ до те мере да је проузроковао мигрантску кризу, која је уздрмала и саме темеље Уније. Мигрантска криза је делимично спласнула појавом пандемије вируса корона, али је значајно појачана ратом у Украјини од 2022. године, као и најавом новог таласа избеглица са подручја Блиског истока и Африке.

међународној заједници, а основна претња – војна претња друге државе или групе држава. Временом, како се развијала свест о проширеном аспекту безбедности, спољна безбедност државе је све више попримала атрибуте који нису само војни, а долазили су из сфере политике, економије, социјеталне и еколошке равни. Тако, директна војна претња, у комбинацији са другим облицима (претњама) угрожавања, у савременим условима добија један израз који се именује као *хибридне претње* (деловање, ратовање).

Сматра се да је синтагму *хибридни рат* први употребио Томас Мокатис (Thomas R. Mockaitis) у чланку *Британске противпобуњеничке мере у пост-империјалној ери* (British Counterinsurgency in the Post-Imperial Era). Чланак је објављен 1995. године (Latawski, 2011). Интензивно коришћење термина *хибридне претње* и *хибридно ратовање* започело је у протеклој деценији, приликом покушаја да се објасни стратегија Хезболаха током рата у Либану 2006. године. Коришћење термина нарочито је интензивирано након сукоба у Украјини и присаједињења Крима Руској Федерацији 2014. године. Значајну улогу у успостављању теорије хибридних претњи и хибридног ратовања имао је Френк Хофман (Frank Hoffman). У једној од првих публикација која се бави проблематиком хибридног ратовања, под називом *Сукоби у 21.веку: успон хибридних ратова* (Conflict in the 21st century: the rise of hybrid wars), Хофман (2007) истиче да „хибридне претње обухватају пун опсег различитих начина ратовања, укључујући конвенционалне способности, нерегуларне тактике и формације, терористичке активности са неселективним насиљем и криминал. Хибридне ратове могу водити државе, али и недржавни актери. Те мултимодалне активности могу да извршавају посебне јединице или чак једна јединица, али су оперативно и тактички усмерене и координисане у оквиру основног борбеног простора ради постизања синергијских ефеката у физичкој и психолошкој димензији сукоба. Ефекти се могу остваривати на свим нивоима рата“.

Дакле, спољна безбедност је заснована на држави као чланици међународне заједнице, као креатору и субјекту међународних односа. Чињеница је да поједине државе чланице међународне заједнице, инсистирајући на постизању апсолутног права и користи за себе и наступајући са позиције силе, нарушавају иста таква права других држава, чиме је непосредно и посредно угрожена њихова безбедност. Нажалост, много је примера у савременим међународним односима који указују на примену силе великих сила, чиме је

драстично угрожавана безбедност других самосталних и независних држава. Агресија НАТО на бившу СР Југославију (1999) је типичан пример за наведено.

1.2.1.4 Унутрашња компонента безбедности

У теорији постоји мноштво приступа унутрашњој компонети безбедности, као неодвојивом делу националне безбедности (интегралне безбедности државе). Стајић (2013) широко захвата синтагму унутрашња безбедност државе као јединке и каже:

> „Унутршња безбедност штити унутрашњи суверенитет државе од свих антидруштвених појава, односно од свих појава којима се угрожава државно уређење. С обзиром на то да су саставни делови уставног уређења државе управо елементи друштвеног уређења, често се унутрашња безбедност поистовећује са заштитом економске, политичке, правне и социјалне сигурности грађана, тј. са заштитом уставног и правног поретка“ ().

У неким својим каснијим радовима Стајић је еволуирао у погледу схватања организације и функција унутрашње безбедности. Тако, полазећи од одређења функција унутрашње безбедности како их поима Саша Мијалковић (2010), каже:

> „У складу са тим, систем унутрашње безбедности је систем субјеката који се старају о заштити државног уређења, унутрашњег јавног поретка и безбедности људи од различитих облика оружаног и неоружаног угрожавања које настаје унутар државе (оружана побуна, тероризам, природне непогоде, техничко-технолошки акциденти и сл.), али и од невојних претњи које долазе споља (прекогранични криминал, заразне болести итд.). Чине га више подсистема: *сектор унутрашњих послова, правосуђе, безбедносно-обавештајни систем, инспекције, царина, субјекти приватне безбедности*“ (Стајић и сар., 2017: 1335).

По питању унутрашње безбедности, врло је занимљиво становиште ЕУ као заједнице 27 држава чланица. Тај аспект безбедности прецизиран је 2010. године у документу *Стратегија унутрашње безбедности*, која покрива следећих пет области – „1) Сузбијање међународних криминалних мрежа, 2) Превенција тероризма и одговор на радикализацију и регрутовање, 3) Повећање безбедности грађана и приватног сектора у сајбер простору, 4) Повећање безбедности кроз управљање границама и 5) Ефикасно управљање ванредним ситуацијама, и пружа стратешке смернице за акцију која би гарантовала унутрашњу безбедност и у наредном периоду“ (Европски покрет у Србији, 2011). Анализирајући наведену стратегију ЕУ, Кујић (2018) пише:

„Тако су формулисане мере у хоризонталној и вертикалној димензији, где **у прве** спадају правосудна и демократска контрола активности, проактиван приступ који се темељи на

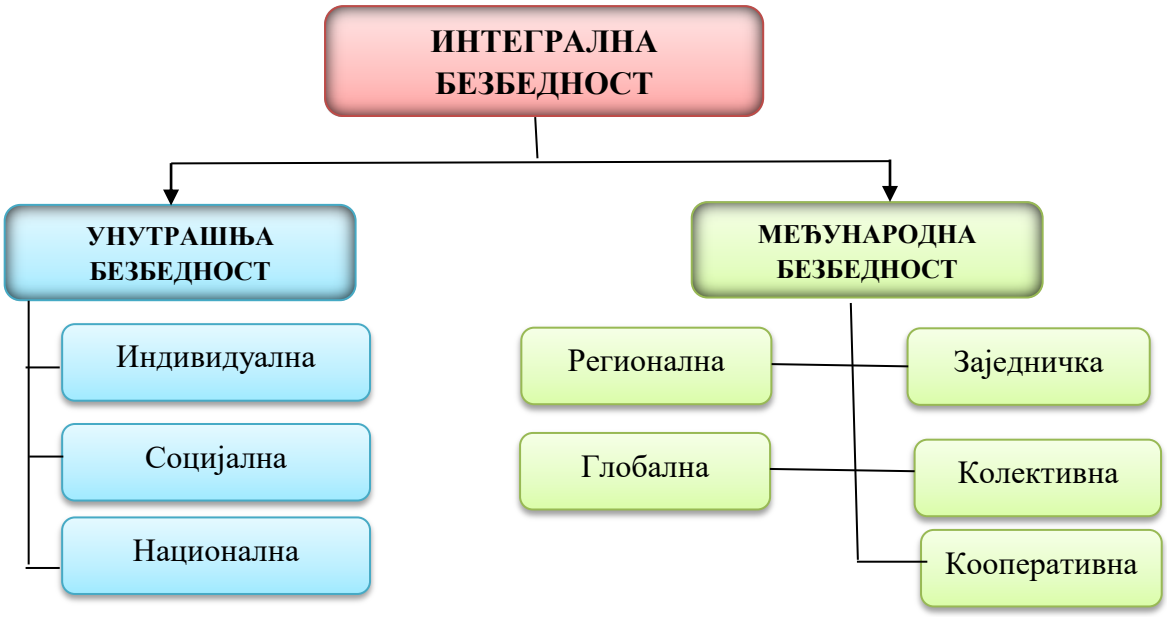
информацијама, правосудна сарадња у кривичним стварима, интегрисано управљање границом и настојање да путем иновација и информација из различитих области друштвеног живота буде пружен адекватан одговор на будуће безбедносне изазове, док **у друге** спадају различити нивои који се креирају путем међународне, регионалне и националне сарадње, спречавање тероризма и регрутовања терориста кроз креирање Европске мреже за надзор радикализације и помоћ цивилном друштву у борби против терористичке пропаганде, унапређење безбедности граница“ (стр. 132).Унутрашња безбедност (Homeland Security) у САД је питање које је посебно добило на значају након терористичких напада Ал-Каиде на објекте у Њујорку и Вашингтону 11. 9. 2001. године. Тако, у склопу опсежних реформи у систему безбедности, 2002. године је формирано *Министарство унутрашње безбедности (Department of Homeland Security – DHS)*, у чијој агенди стоји:

> „Заједно смо посвећени немилосрдној отпорности, настојећи да спречимо будуће нападе на Сједињене Државе и наше савезнике, одлучно реагујући на природне катастрофе и катастрофе које је изазвао човек, и унапређујући амерички просперитет и економску безбедност дуго у будућности“. Шест је основних мисија Министарства: „Борба против тероризма и претњи унутрашњој безбедности, Сигурне америчке границе, Безбедан сајбер простор и критична инфраструктура, Очувати и одржавати просперитет и економску сигурност нације, Ојачати спремност и отпорност и Ојачати радну снагу Министарства“ (ал-).

1.2.1.5 Интегрална безбедност

Одвојена анализа спољне и унутрашње безбедности државе оправдана је с теоријског аспекта посматрано и има одраза на аспекте организовања система безбедности. Међутим, чињеница је да је код бројних облика (претњи) угрожавања безбедности врло тешко правити разлику да ли су спољни или унутрашњи. С друге стране, систем безбедности државе је јединствен, а његови подсистеми се могу ближе везати за поједине компоненте безбедности. У складу с наведеним, говоримо о *интегралној безбедности државе*. Позивајући се на ставове Стајића и Гаћиновића, Ђукић (2017) за интегралну безбедност каже (Слика 3):

> „Интегрална безбедност се дефинише као свеукупна или целовита безбедност. Представља сублимат унутрашње и међународне безбедности, али не као прости збир тих двеју безбедности, већ као нова вредност која се штити. Не можемо говорити о било каквој, па ни унутрашњој ни међународној безбедности ако је било који елемент тих безбедности значајније угрожен. Као свеобухватна, интегрална безбедност је једна и јединствена и са тог становишта је недељива. Њена подела на унутрашњу и међународну је условна више из педагошких и практичних разлога због лакшег објашњења и учења. Пошто се савремене државе, данас, нападају на свим пољима (породица, вера, власт, уставно уређење, спољна политика, економија, систем безбедности итд.) онда и држава мора свим својим снагама да се супротставља тим нападима. Интегрални напад тражи интегралну одбрану“ (стр. 110).



Слика 3. *Класификација безбедности*

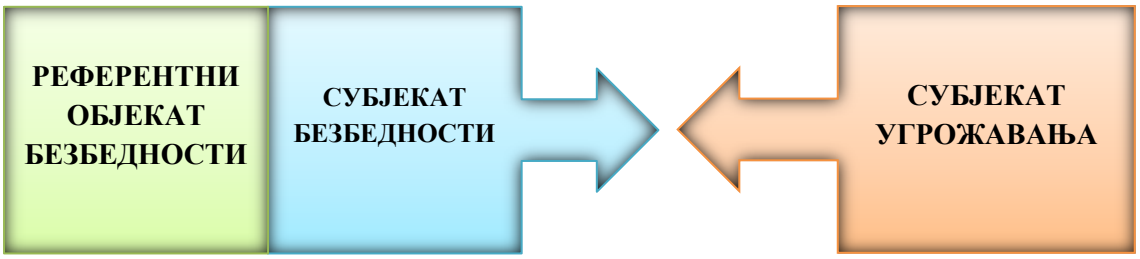
Извор: *Стајић, 2013 (у Ђукић, 2017: 110)*

Захватајући шири аспект институционализације безбедности кроз историју, Гаћиновић (2007, 2020) истиче да је формирањем Организације уједињених нација (1945) успостављена интегрална безбедност у правом смислу речи и пише:

> „Интегрална (лат. integralia) целина, који сачињава целину, потпун, целокупан, целовит. Интегрална безбедност, тј. свеукупна или целовита безбедност је одбрана од свих облика оружаног и неоружаног угрожавања и остварења потпуне и свестране безбедности на свим нивоима и у свим садржајима живота и деловања човека и друштва“

Могли бисмо да наводимо још теоријских извора који захватају појам интегрална безбедност и добили бисмо сличан резултат, а то је да тај аспект безбедности подразумева 1) одсуство свих облика (претњи) угрожавања које потичу од човека и природе и 2) да примарно захвата државу (национална безбедност), укључујући појединца, друштвене групе и друштво, као и њену везу са спољном (међународном) безбедношћу, која може да има карактер колективне, заједничке или кооперативне безбедности.

Анализом теоријских одређења (државоцентрични и друштвеноцентрични приступ) безбедности, као и њиховим ближим одређењем на нивоу државе (унутрашња, спољна и интегрална безбедност), може се успоставити системски приступ безбедности (Слика 4).



Слика 4. *Системски приступ безбедности*

Извор: *Форца, 2021: 43*

Анализом ставова страних аутора, кад је безбедност у питању, Филип Ејдус је успоставио тзв. граматику безбедности, која обухвата: „*опасност* (оно што угрожава), *референтни објект безбедности* (оно што је угрожено), *субјект безбедности* (онај који штити) и *средства*, односно *мере безбедности* (начин на који се штити)“ (Ејдус, 2012: 36. „Системски приступ безбедности (Слика 4) утврђује се у релацији три кључна питања: КО (шта) угрожава (безбедност) – КО се супротставља угрожавању и – КО (шта) се брани/штити од угрожавања? Прво КО (шта) угрожава (безбедност) јесте **субјект угрожавања**; друго КО се супротставља угрожавању јесте– **субјект безбедности** и треће КО (шта) се брани/штити од угрожавања јесте **референтни објект безбедности**. Субјект угрожавања и субјект безбедности имају своје начине, методе и средства деловања. Референтни објект безбедности има различиту „специфичну тежину“, односно значај за субјекта безбедности (нпр. немају исту „тежину“ – значај одбрана државе од оружаног угрожавања или заштита јавног реда и мира током фудбалске утакмице)“ (Форца, 2021: 43).

1.2.2 Систем безбедности

Из претходног текста може се закључити да је безбедност врло широко распрострањен појам. Отуда, било каква анализа тог појма, у вези са било којим референтним објектом или обликом (претњом) угрожавања, не може да буде лаичка и стихијна, већ стручна, планска и организована. У том смислу, том активношћу могу да се баве једино организационе целине које именујемо као *систем безбедности.*

Синтагму *систем безбедности* чине два појма, и то „систем“ и „безбедност“. У теорији постоји безброј дефиниција наведених појмова и њихово навођење и анализа

сваког понаособ није наш циљ. Наш циљ јесте да из оба појма узмемо њихову суштину и спојимо је у синтагму. Суштина појма „безбедност“ јесте одсуство претњи по референтни објект. Шта је суштина појма „систем“? Од прве дефиниције система коју је дао Лудвиг фон Берталанфи да је то скуп елемената који се налазе у интеракцији, познато је много одређења тог појма. Нас интересују организациони (друштвени) системи, које чине људи и средства. Суштина организационог система (организације као система) јесте да је то скуп људи и средстава формиран ради задовољења заједничке сврхе (циља). Формално-логички посматрано, прелиминарно, систем безбедности можемо одредити као *организован скуп људи и средстава којима је заједнички циљ (сврха постојања) превенција и/или елиминисање облика (претњи) угрожавања референтног објекта* (Форца, 2021).

У ранијем тексту је описано како се имеунују референтни објекти безбедности, као и да по том питању нема потпуне сагласности у теорији. То са своје стране намеће и питање да ли за сваки референтни објект (треба да) постоји посебан систем безбедности? Без дубљег познавања теорије, одговор на наведено питање је негативан. Наиме, из досадашње анализе појма безбедност намећу се два одговора – 1) безбедност појединца, друштвених група и државе као целине, требало би да јамчи држава, за шта се формира систем националне безбедности и 2) безбедност успостављеног међународног правног поретка требало би да јамчи УН, као систем колективне међународне безбедности.

Између државе (национална безбедност) и УН (колективна међународна безбедност), појављују се аспекти *заједничке* и *кооперативне* безбедности.

Заједничка безбедност и одбрана, као изворни термин, појављује се у Европској унији, у Лисабонском уговору 2007/2009 (Заједничка безбедносна и одбрамбена политика – ЗБОП, као део Заједничке спољне и безбедносне политике – ЗСБП). У Министарству спољних послова Републике Србије на ЗБОП ЕУ се гледа на следећи начин:

> „Заједничка безбедносна и одбрамбена политика Европске уније – ЗБОП (*Common Security and Defence Policy – CSDP*) је део Заједничке спољне и безбедносне политике ЕУ – ЗСБП (*Common Foreign and Security Policy – CFSP*) и успостављена је у циљу афирмације улоге ЕУ као важног глобалног фактора, са препознатљивом спољном политиком и цивилно-војним ресурсима за управљање кризама, превенцију конфликата и одржавање међународног мира и безбедности. ЗБОП је интегрални део свеобухватног приступа ЕУ управљању кризама који, поред цивилних и војних капацитета, укључује и политичке, дипломатске, правне, развојне, трговинске и економске инструменте. Овако широк спектар инструмената и средстава неопходних за ефикасно управљање кризама ставља ЕУ у јединствену позицију у односу на остале међународне актере“ (www.mog.gov.rs).

Дакле, ЗБОП у оквиру ЕУ јесте шири од националне, а ужи од глобалне међународне (колективне) безбедности. Кад кажемо да је ЗБОП ужи од колективне међународне безбедности, пре свега мислимо на однос надлежности ЕУ и УН (Савет безбедности). Посебна карактеристика ЗБОП ЕУ јесте право држава чланица да се о појединим њеним аспектима саме опредељују. Типичан пример јесте Данска, која не учествује у мировним мисијама и операцијама ЕУ, противи се заједничкој одбрани Уније и сматра да је НАТО довољан гарант безбедности. Такође, специфичан и сопствени став према заједничкој одбрани Уније има Ирска, а делом и Аустрија, Малта и Кипар, као војно неутралне државе (Форца и сар., 2023).

Израз „заједничка безбедност“, осим наведеног и формализованог у ЕУ, срећемо у бројним облицима читавог дијапазона супротстављања претњама безбедности разних друштвених субјеката, као што су удружења, организације и корпорације. Тај аспект заједничке безбедности може да буде уско усмерен на одређену претњу или на шири скуп претњи, као што је, на пример, корпоративна безбедност. Принципијелно, ради се о заштити људи, имовине и пословања од разних облика угрожавања.

Синтагма *кооперативна безбедност* је нови термин који изражава везу колективне безбедности и општег приступа безбедности. Ради се о „широком приступу, мултидисциплинарног опсега, који фаворизује уверавање у односу на одвраћање; укључивање пре него искључивање; невојна решења у односу на војна; подразумева да су државе првенствени чиниоци система безбедности, али прихвата да недржавни чиниоци могу имати важну улогу; не захтева формално стварање безбедносних установа, али их не искључује и не искључује вредност дијалога на мултилатералној основи“ (Metodi-i-oblici-bezbednosnog-organizovanja-i-delovanja-beleške.pdf).

Системи безбедности захватају продубљену вертикалу и проширену хоризонталу поимања безбедности. Развијају се на националном и међународном нивоу, обухватајући најшири аспект сектора безбедности или се образују у конкретном сектору (еколошка безбедност, на пример).

Као што је национална безбедност у фокусу теорије и праксе, тако су и системи националне безбедности примарни у теоријском разматрању и практичном поступању. Системи националне безбедности су типични организациони (друштвени) системи, који су примарно дефинисани циљевима, функцијама, структуром (организацијом) и начелима

(принципима) функционисања, што је ближе уређено законима и подзаконским актима. Ти системи се налазе у различитим (чврстим или лабавим) формама интеракције са међународним системима заједничке и колективне безбедности и одбране (Форца, 2021).

С обзиром на то да се национална безбедност чврсто везује за националне вредности, интересе и циљеве, то се и општи циљ система националне безбедности, најчешће, утврђује као одбрана и заштита национаних вредности, интереса и циљева од свих облика угрожавања. Сваки систем националне безбедности спроводи политику националне безбедности коју је утврдила држава. У том смислу, безбедносна политика полази од националних вредности и утврђује националне интересе који се остварују реализацијом националних (стратешких) циљева. Тако, посебни циљеви система националне безбедности утврђују се у оквиру врсте и броја детерминисаних националних интереса (Форца, 2022).

С методолошког аспекта посматрано, при пројектовању било ког система, прво му се утврде функције, па структура (организација). Функције система националне безбедности различито се дефинишу у теорији и пракси. Најчешће, функцијама система националне безбедности приступа се са аспекта њихове мисије. Тако, као функције се утврђују превенција и репресија или правовремено откривање и спречавање деловања свих облика угрожавања вредности и интереса (Стајић, 2013). Такав приступ функцијама система националне безбедности не упућује на његову структуру (организацију). Стога, функцијама система националне безбедности мора се приступити као скупу послова и активности које обављају субјекти система. У том смислу, као функције система националне безбедности могу се утврдити основна и посебне функције. Основна функција јесте безбедност државе и грађана. Посебне функције система националне безбедности могу се идентификовати као: управљање (сваким организационим системом се управља); одбрана; заштита; безбедносно-обавештајна функција; санкционисање; функција приватне и корпоративне безбедности; контрола и надзор и функција компатибилних активности других субјеката значајних за националну безбедност (Форца, 2022).

Различит је приступ структури (организацији) система националне безбедности. У теоријском смислу, помињу се конвенционални, неконвенционални и суплементарни субјекти система (Кековић, 2011; Стајић, 2013). У конкретном смислу (званична документа) и најчешће, структура система националне безбедности дефинише се кроз

управљачки и извршни део. Управљачки део система националне безбедности чине највиши органи власти, као што су парламент, председник државе и влада. У извршном делу система разликују се подсистеми који реализују поједине функције, као што су: систем одбране; систем унутрашње безбедности; безбедносно-обавештајни систем; правосудни систем; систем контроле и надзора; систем приватне и корпоративне безбедности и подсистем других субјеката значајних за националну безбедност (Стратегија националне безбедности, 2019).

Узимајући у обзир наведено за систем националне безбедности, покажимо на конкретним примерима како се у појединим државама тај систем дефинише.

Табела 2. *Дефиниције система националне безбедности у званичним документима*

ИЗВОР	ДЕФИНИЦИЈА СИСТЕМА НАЦИОНАЛНЕ БЕЗБЕДНОСТИ
СТРАТЕГИЯ национальной безопасности Российской Федерации, 2021: т. 5.	**Систем обезбеђења националне безбедности –** Свеукупност успешне државне политике у сфери обезбеђења националне безбедности органа политичке власти и свих потребних и механизама који су им на располагању.
Закон о суставу домовинске сигурности Р. Хрватске, чл. 3: т. 1 (2017)	**Сустав домовинске сигурности** значи сустав који чине ресурси унутрашњих послова, обране, сигурносно-обавештајног сустава, цивилне заштите, ватрогаства, службе ванских послова те других тијела која организирано и координирано обављају послове и задаће препознавања, процјене, смањивања и/или уклањања сигурносних ризика од важности за националну сигурност Републике Хрватске.
Стратегија националне безбједности Црне Горе (2008)	**Систем националне безбједности** чини функционално јединство свих елемената државе ради обезбјеђења заштите националних интереса и вриједности Црне Горе.
Resolucijo o strategiji nacionalne varnosti Republike Slovenije (2019)	**Обезбеђење националне сигурности** Републике Словеније заснива се на функционисању система одбране, система унутрашње безбедности и система заштите од природних и других несрећа као подсистема система националне безбедности, али и на спољним политичким, економским, информационим и другим активностима које директно утичу на националну безбедност. Ови (под) системи ће и даље бити унапређени, а посебно ће бити интегрисани у кохерентну целину како би се повећала ефикасност целокупног система националне сигурности.
Стратегија националне безбедности Републике Србије (2019)	**Систем националне безбедности** представља нормативно, структурно и функционално уређену целину чијом се делатношћу обезбеђује заштита и остваривање националних интереса Републике Србије.

Извор: *Обрада ауторке дисертације*

Највећи број дефиниција система националне безбедности, експлицитно или имплицитно, везује се за његову структуру (организацију), наводећи и општи циљ тог система. Увидом у ширу литературу (теорија и службена документа), дефинисање система националне безбедности, принципијелно, регулисано је на два начина. Први, систем

националне безбедности уређен је посебним законом (САД, Русија, Хрватска, Словенија, Црна Гора…). Други, ставови о систему националне безбедности садржани су у документима изван закона, као што је (најчешће) стратегија националне безбедности (Република Србија) (Шире у: Форца, 2022). Без обзира на то да ли је уређен законом или другим документом, у структури система националне безбедности, најчешће, наводе се: систем одбране (војска), систем унутрашње безбедности (полиција), обавештајно-безбедносне службе и цивилна заштита (служба заштите и спасавања). Међутим, полазећи од општег одређења да систем чине управљачки и извршни део, потребно је мало детаљније анализирати његову структуру, што ћемо учинити на примеру Републике Србије.

У *Стратегији националне безбедности Републике Србије* из 2019. године, управљачки и извршни део система националне безбедности уређени су на следећи начин:

- *Управљачки део*: Народна скупштина, председник Републике, Влада и Савет за националну безбедност;
- *Извршни део:* Систем одбране, Систем унутрашње безбедности; Безбедносно-обавештајни систем и Други субјекти значајни за националну безбедност (Стратегија националне безбедности, 2019).

Наведена општа структура система националне безбедности само делом указује на конкретне елементе (субјекте) појединих делова те структуре. Тако, прецизно су утврђени субјекти управљачког дела (подсистема), као и безбедносно-обавештајног подсистема (БИА, ВБА и ВОА). С друге стране, уопштено су утврђени остали подсистеми, што се види из одређења у стратегији:

- *Систем одбране* је део система националне безбедности који представља јединствену целину, нормативно, структурно и функционално уређену, чији је циљ остваривање одбрамбених интереса Републике Србије.
- *Систем унутрашње безбедности* је део система националне безбедности намењен за обављање послова којима се обезбеђује безбедност грађана и имовине, пружа подршка владавини права, обезбеђују Уставом и законом утврђена људска и мањинска права и слободе, спроводе превентивне и оперативне мере и извршавају задаци заштите и спасавања људи и добара од последица елементарних непогода и других несрећа, укључујући и мере опоравка од тих последица. Поред надлежних органа државне управе, послове унутрашње безбедности обављају и правна лица, предузетници и физичка лица која врше послове приватног обезбеђења у складу са законом.
- *Други субјекти значајни за националну безбедност* јесу органи државне управе и институције надлежне за спољне послове, правосуђе, здравство, демографију, људска и мањинска права, економију, образовање и научну делатност, привреду, енергетику, телекомуникације, саобраћај и транспорт, инфраструктуру, заштиту животне средине, културу, затим органи аутономних покрајина и јединица локалне самоуправе, организације

цивилног друштва, медији, правна лица и грађани који доприносе остваривању циљева националне безбедности (Стратегија националне безбедности, 2019).

Дакле, да бисмо утврдили ко чини структуру појединог подсистема система националне безбедности није довољно ово што је наведено у Стратегији националне безбедности,односно неопходно је анализирати законе и друге прописе којима се уређују субјекти тих подсистема. Тако, на пример, ако анализирамо *Закон о одбрани*, уочићемо да су субјекти система одбране: „грађани, државни органи, органи аутономних покрајина, органи јединица локалне самоуправе, привредна друштва, друга правна лица, предузетници и Војска Србије“ (Закон о одбрани, 2018: ч. 4, т. 6). Међутим, у нас не постоји закон о унутрашњој безбедности, тако да је врло тешко операционализовати систем унутрашње безбедности наведен у стратегији. Такође, сви наведени субјекти система одбране (Закон о одбрани) јесу и субјекти и система унутрашње безбедности (Стратегија), а, изузев Војске, појављују се и као други субјекти значајни за националну безбедност.

На шта нам указује сложеност детерминисања субјеката система националне безбедности и његових подсистема? Прво, да се поједини субјекти система појављују у скоро свим подсистемима. Друго, сваки подсистем система националне безбедности мора да има кључног носиоца (субјект) и остале учеснике. Тако, сасвим је логично да је кључни субјект система одбране Војска, а да остали субјекти имају своје место и улогу у одбрани земље. Такође, кључни субјект система унутрашње безбедности јесте полиција. Тако, до конкретне улоге и задатака појединих субјеката система националне безбедности (и његових подсистема) заправо ми долазимо тек анализом прописа о сваком субјекту понаособ.

Детаљнији захват структуре система националне безбедности био нам је неопходан због разлога обраде наредног питања (појма) – *безбедносна аналитика*. Наиме, на основу теоријске анализе појма аналитика и у складу са чињеницом да се аналитика појављује у свим друштвеним делатностима, логично је да у систему националне безбедности, као посебна делатност и организација управљачког дела, функционише – *безбедносна аналитика.*

1.3 Безбедносна аналитика

Аналитика (аналитички процес) се, како смо видели, примењује у широком спектру научних дисциплина, од лингвистичких до хемијско-биолошких области. Међутим, у области безбедности примена аналитике се битно разликује од осталих дисциплина. Делокруг послова на које се она односи често се своди на стручно-оперативни, док је научно-истраживачки рад секундаран. Стога се безбедносна аналитика често посматра као вештина. Расправе на рачун безбедносне аналитике са темом да ли је она струка или наука, углавном завршавају са ставом да је то струка заснована на науци (Форца и Аночић, 2018).

1.3.1 Појам безбедносна аналитика

Дефиниција синтагме *безбедносна аналитика* (енг. Security Analytics) ретко се среће и у теорији и у пракси безбедности. Или, прецизније, среће се под разним другим називима и више подразумева да се ради о врстама безбедносне аналитике. Тако, као преовладавајуће, срећемо синтагме: обавештајна аналитика (у војсци и службама безбедности), криминалистичка аналитика и криминалистичко-обавештајна аналитика (у полицији).

Даниловић и Милосављевић (2008) у свом делу *Основе безбедносне аналитике* не дефинишу појам „безбедносна аналитика“ експлицитно, већ наводе да је то аналитика у систему безбедности, те истичу: „можемо говорити да се у елементима (подсистемима) система безбедности примењују два круга аналитичког рада. Први круг чини *оперативна аналитика,* а други *истраживачка аналитика*, коју неки аутори оправдано називају оперативно-интервентна и истраживачко-инструктивна аналитика“ (Даниловић, Манојловић, 2024:). Под оперативном (оперативно-интервентном) аналитиком подразумевамо интелектуалне радње које, у склопу редовних оперативних послова, обављају припадници система безбедности. Док за истраживачку (истраживачко-инструктивна) аналитику кажу да је то „стручна делатност која се ослања на примену одређених научних метода, техника, инструмената и процедура“ (Исто).

У каснијој разради претходно наведених врста аналитике Даниловић и Милосављевић истичу да се код бројних аутора безбедносна аналитика убраја у групу тзв. специјалних аналитика. Тако, позивајући се на ставове Новака Милошевића, Саше

Михајловића и Љубомира Стајића, кажу да специјалну аналитику можемо схватити као широки процес рада аналитичара и аналитичких служби у органима државне власти, организован кроз разне пригодне облике и усмерен својим радом, циљевима и сврхама на деловање према другим државама и сопственој земљи (Даниловић и Милосављевић, 2008:). Такође, Даниловић и Милосављевић наводе да: „под оперативном (оперативно-интервентном) аналитиком подразумевамо интелектуалне радње које, у склопу редовних оперативних послова, обављају припадници система безбедности“ (Исто).

Драган Ђурђевић, слично као и Даниловић и Милосављевић, безбедносну аналитику сврстава у групу тзв. специјалних аналитика, које припадају уском кругу државних органа власти (дипломатија, војска, полиција, обавештајно-безбедносне службе), класификујући је истоветно на оперативну, евиденциону и истраживачку (Ђурђевић и Милић, 2020).

Форца и Аночић су ретки аутори који у свом делу експлицитно дефинишу појам „безбедносна аналитика“ на следећи начин: „Безбедносна аналитика је посебна врста аналитике, која се испољава као интелектуална, организована, систематска, циљна и сврсисходна делатност усмерена ка стицању релативно истинитих и употребљивих сазнања о безбедносним појавама, неопходним за рад субјеката система безбедности“ (Форца и Аниочић, 2018).

Бранислав Милосављевић у својој докторској дисертацији под насловом *Безбедносна процена као чинилац стратегије националне безбедности Републике Србије* (Милосављевић, 2019) имплицитно, безбедносну аналитику поима као *безбедносна процена*. До тог закључка долазимо на основу следећих ставова из његове дисертације:

- „Безбедносна процена представља предвиђање даљег развоја безбедносног стања, појава и догађаја, представља мисаону активност која има за циљ да се на основу анализе предвиде могући развој и тенденције развоја безбедносних ситуација у будућности“.
- “У ужем смислу, процена се посматра као аналитички поступак који се одвија у неколико фаза и обухвата иницијалну фазу, прикупљање, селекцију и класификацију података, аналитичко-синтетичку обраду података, формулисање закључака процене и верификацију процене”.
- „Безбедносна процена је и ‘скуп закључака настао применом изабраних метода и техника ради добијања података, показатеља и сазнања о свим видовима безбедносне угрожености људских, материјалних и природних ресурса’“.
- „Безбедносна процена представља процес утврђивања постојећег стања на темељу поузданих информација у циљу предвиђања будућег тока деловања и припреме варијанте

решења за доношење одлуке. До процене се долази анализом информација и података и међусобним повезивањем информација о појавама и догађајима“ (Милосављевић, 2019:

Како је наведено, уместо синтагме „безбедносна аналитика“ у теорији и пракси сусрећу се појмови „обавештајна аналитика“, „криминалистичка аналитика“, „криминалистичко-обавештајна аналитика“ и други. Наведимо само неке од дефиниција које срећемо у литератури:

- „Обавештајна аналитика (Intelligence) је специјализовани облик *знања, активности и организације*. Као *знање*, обавештајне информације упознају лидере, јединствено им помажући у просуђивању и доношењу одлука. Као *активност*, то је начин на који су прикупљени подаци и информације, утврђена њихова релевантност за проблем, протумачене како би се утврдили вероватни исходи и дистрибуиране појединцима и организацијама које их могу искористити, иначе познатији као ‚потрошачи обавештајних информација'. Обавештајна *организација* руководи и управља овим активностима како би се такво знање створило што ефикасније“ (Moore, 2007).
- У Приручнику „Полицијско-обавештајни модел“ МУП-а Србије стоји: „Криминалистичка анализа (не користи се термин аналитика, прим. аут.) је процесно и методолошки најкомплекснија функција криминалистичко-обавештајних послова, којом се прикупљени и обрађени подаци и информације обједињавају, структурирају, процењују и тумаче, на основу чега се изводе релевантни закључци и дају препоруке неопходне за доношење одлука за предузимање оперативно-полицијских активности“ (МУП Србије, 2016:).
- У документима МУП-а Хрватске, криминалистичко-обавештајна аналитика је дефинисана на следећи начин: „Криминалистичко-обавештајна аналитика је делатност прикупљања, обједињавања, прегледавања и анализирања података у свези криминалних активности те изналажења кључних значајки тих криминалних активности“ (Краљ, 2019: 52).

Несумњиво, све наведене дефиниције односе се на аналитику у систему безбедности, са напоменом да не дају експлицитну дефиницију безбедносне аналитике, изузев става Форце и Аночића, већ њених појединих врста.

У анализи праксе безбедносне аналитике, у даљем тексту, као студију случаја навешћемо пример Обавештајне заједнице САД. Учинићемо то ради потврђивања сазнања да безбедносна аналитика не може више да се ослони само на обавештајну (војска) или криминалистичку (полиција) аналитику, него је потребна синергија разних врста аналитике, па и специјализованих цивилних агенција. У том смислу, у САД постоје бројне специјализоване агенције које се баве аналитиком, па и аналитиком у систему националне безбедности. Ради утврђивања шта под безбедносном аналитиком подразумевају, навешћемо као примере само две агенције – Си-Ен-Ен (CNN) и Ен-Си-Ај (NSI). Наведене агенције спроводе аналитику у свим секторима безбедности (политички, војни, економски,

социјални, еколошки), али и, комерцијално, за корпоративне и друге потребе. Под безбедносном аналитиком, имплицитно, подразумевају:

- *Си-Ен-Ен:* Коришћење иновативних метода у анализи података и предлагању оптималних решења за заштиту здружених снага, односно подршка локалних и државних институција у заштити националне безбедности (https://www.cna.org/).
- *Ен-Си-Ај:* Примена различитих аналитичких метода заснованих на мултидисциплинарним друштвеним и наукама о одлучивању, које помажу да поузданије и предвидљивије разумеју људе и њихово понашање у критичним и сложеним проблемима (https://www.nsiteam.com/).

У складу са наведеним, у дефинисању појма „безбедносна аналитика“ користићемо правила дефинисања, раније наведену дефиницију „аналитике“ (Термиз и Милосављевић, 2008; Даниловић и Милосављевић, 2008) и изнете ставове о безбедности. Основно правило дефинисања гласи „виши род и специфична разлика“ (genius proximum – specifica diferentia). Дакле, сваки појам при дефинисању, као *врсту*, везујемо за виши *род*, а онда наводимо *специфичну разлику* тог појма као врсте на вишем роду, од других врста појомова које виши род обухвата. Друго, дефинисати неки појам значи одредити се према његовим најбитнијим карактеристикама, односно утврдити садржај појма (Форца и Аночић, 2018).

Повезујући наведено и друга правила дефинисања, као и полазну дефиницију „аналитике“ (Даниловић и Милосављевић,2008; Термиз и Милосављевић,2008,), као и уважавају дефиницију безбедносне аналитике коју су дали Форца и Аночић, за утврђивање појма „безбедносна аналитика“ користимо следеће премисе:

- *Безбедносна аналитика* је посебна *врста* аналитике као *родног* појма, на шта упућује реч „безбедносна“.
- Све врсте аналитике на родном појму *аналитика* имају нешто заједничко за све врсте (род као целину) и своје специфичности (specifica diferentia) по којима се *безбедносна аналитика* од њих разликује.
- Оно што је заједничко за све врсте аналитике (род као целину) јесте да је то интелектуална, организована, систематска и сврсисходна делатност усмерена на стицање релативно истинитих и употребљивих сазнања о актуелним збивањима у свом домену.
- Специфична разлика безбедносне аналитике од других врста аналитике на родном појму аналитика јесте што се испољава у сфери безбедности као друштвеној делатности.
- Безбедност као област друштвеног живота од других области разликујемо по томе што се бави: 1) појавама које угрожавају безбедност - *субјект угрожавања*, 2) *субјектом безбедности*, односно системом који се супротставља угрожавању и 3) *референтним објектом безбедности*, односно оним што се брани/штити. Дакле, тиме се не бави ниједна друга врста аналитике (види: Слика 4).

- Производ безбедносне аналитике су информације (знања) до којих долазе безбедносни аналитичари (организација), а које користе субјекти безбедности зарад заштите референтног објекта безбедности.

У складу с наведеним, номинална дефиниција појма (синтагме) *безбедносна аналитика* гласи: **Безбедносна аналитика је посебна врста аналитике која се испољава као интелектуална, организована, систематска, циљна и сврсисходна делатност усмерена ка стицању релативно истинитих и употребљивих сазнања о субјекту угрожавања, неопходним за рад субјекта безбедности у заштити референтног објекта безбедности.**

Из наведене дефиниције уочавамо да је предмет безбедносне аналитике – знање, односно информације. Али, не било које информације, већ информације о безбедности. Да бисмо оивичили појам „безбедност“, системски смо утврдили да га чине субјект угрожавања, субјект безбедности и референтни објект безбедности. У том смислу, предмет безбедносне аналитике јесте безбедност, у најширем и у најужем смислу схватања тог појма или – од глобалне безбедности до појединца. Такође, нису у питању било које информације о безбедности, него информације о угрожавању безбедности (субјект угрожавања) до којих се дошло *у процесу њихове обраде*. Тако прикупљена знања користе субјекти безбедности (систем безбедности) за свој рад, односно у заштити референтног објекта безбедности. У складу с наведеним, пре преласка на практичан део, а полазећи од става да је аналитика „знање, активност и организација“ (Moore, 2007:), неопходно је у потребном и општетеоријском обиму анализирати безбедносну аналитику као процес и организацију.

1.3.2 Безбедносна аналитика као процес и организација

Уочили смо Муров став о обавештајној аналитици као знању, активности и организацији. Такође, у претходном тексту смо више пута истакли да су предмет безбедносне аналитике у најширем смислу речи – информација, или процес над сировим подацима и инаформацијама (улаз) и производ – аналитичка информација (излаз). Тако схваћен процес безбедносне аналитике у себи садржи неколико елемената тог процеса: 1) структуру самог процеса (кораке или фазе), 2) методе и технике које се користе; 3) стандарде у раду и 4) аналитичаре који се тим процесом баве. Зато се и каже да је аналитика и *организовање* и *организација.*

На овом нивоу анализе даћемо само теоријска одређења наведених елемената процеса безбедносне аналитике, а због њихове разноликости у пракси, приказаћемо их у другом питању.

Фазе (кораци) безбедносне аналитике јесу релативно засебни делови аналитике, којима се од сирових података и информација добија аналитички производ – нова информација (знање).

Метод је пут (начин) доласка до истине. У безбедносној аналитици, евидентно, постоји неслагање око тога да ли је то научна или практична делатност, то јест да ли се примењују научне или ненаучне (практичне) методе или обоје. Преовладава став да је безбедносна аналитика практична делатност заснована на науци. У том смислу, у безбедносној аналитици се примењују и научне и ненаучне (практичне) методе и технике.

Стандарди у безбедносној аналитици подразумевају техничке спецификације или друге прецизне критеријуме дизајниране да се доследно користе као правило, смерница или дефиниција. У теорији и пракси постоје бројни стандарди, који су изван војне и полицијске сфере, као што су: Стандарди еколошке безбедности, Стандарди економске безбедности, Стандарди социјалне безбедности и други .

На крају, врло значајна за процес безбедносне аналитике јесте њена *организација,* односно *аналитичари*. У општем смислу посматрано, безбедносном аналитиком се баве сви субјекти система безбедности. Међутим, у ужем смислу, том аналитиком се баве за то оспособљене особе и тимови, једним називом именовани као *безбедносни аналитичари*.

Савремене државе теже да дођу до података о тајним плановима, намерама и активностима других држава, а да истовремено сакрију сопствене податке. У том процесу значајну улогу имају обавештајне службе и аналитички сектор. Тако Стајић (2008) наводи да „обавештајна служба ствара услове да руководство земље (политичко, војно и др.) своју активност усмерава само ка поузданим, веродостојним и тачним подацима“ (). Међутим, овде треба напоменути да постоји значајна разлика између податка и информације, посебно у безбедносном сектору.

Податак представља сирову, необрађену чињеницу која није стављена у одговарајући контекст. Да би податак постао информација, он мора да прође кроз процес обраде, а управо овај процес је суштина аналитике. Мандић наводи: „анализом и обрадом постојећег сазнања – података и његовом употребом податак добија нову квалитативну

вредност и постаје информација. Обрада података од стране корисника је процес који га претвара у информацију“ (Мандић, 2012: 279). Да би дошле до кључних података за очување националне безбедности, ове службе довијају се на различите начине, а аналитичари који се баве обрадом прикупљених података морају имати посебне вештине.

Дакле, потребно је разликовати три појма, а то су: податак, информација и знање.

Подаци су необрађена и неинтерпретирана запажања и мерења. Примери укључују карактеристике криминалних активности које се лако квантификују, као што су извештаји о злочинима и друге статистике о злочинима, базе података о преступницима и полицијски задаци.

Информације су подаци стављени у контекст и оснажени значењем, што им даје већу релевантност и сврху. **Знање** је информација којој су дати тумачење и разумевање. Када особа дода своју мудрост информацијама, оне постају знање. **Обавештајни подаци** су подаци, информације и знање који су процењени, анализирани и представљени у формату за доношење одлука у сврхе оријентисане на акцију (OSCE, 2017: 16).

Слика 5. *Шематски приказ односа податка, информације и знања*

Извор: *Обрада ауторке дисертације*

Упркос многим дефиницијама које су до сада објављене, најједноставније и најјасније је рећи да је: „*податак + обрада = информација*”. Наведена формула појашњава разлику између прикупљених података и добијене информације, где кључну улогу представља анализа односно обрада података. Тако, у документима САД, стоји: „Да би настала криминалистичко-обавештајна информација, неопходно је прикупљене податке

проценити, обрадити и анализирати“ (U.S. Department of Justice Office of Justice Programs, 2005).

Све аналитичке службе (организација) се успостављају са конкретним циљем и имају своју команду или управу којој одговарају. Примарни задатак ових служби јесте да раде по налогу и интересу својих оснивача (нпр. државе, министарства и слично). Тако је, на пример, задатак аналитичких сектора, управа и служби у МУП-у да допринесу остварењу функције тог министарства. У том смислу безбедносне аналитичке службе су, за разлику од науке, пристрасне према свом оснивачу.

Да безбедносне аналитичке службе зависе од делатности организације којој припадају, указали су и Даниловић и Милосављевић, наводећи следеће: „Ова посебна врста аналитике односи се на узак круг државних органа власти: дипломатија, војска, полиција, обавештајно-безбедносне службе, цивилна заштита у којима је организована аналитичка служба и аналитички рад. Код свих ових државних органа, аналитички процеси детерминисани су њиховом делатношћу“ (Даниловић и Милосављевић, 2008: 13).

Безбедносна аналитика је скопчана са политиком и од ње у великој мери зависна. С обзиром на то да свака политичка гарнитура бира руководства министарстава, а да она даље успостављају аналитичке секторе, управе и службе, јасно је да се политика и аналитика не могу одвојити. Такође, безбедносна аналитика није одвојена од међународних односа и геополитике. Тако да она може бити усмерена ка унутра и ка споља.

2. ФУНКЦИОНИСАЊЕ БЕЗБЕДНОСНЕ АНАЛИТИКЕ У ПРАКСИ

Овако како је у претходном питању теоријски утврђена безбедносна аналитика у нашој пракси функционише сепаратно. Прецизније, у оквиру општег појма *безбедносна аналитика,* у пракси се најчешће испољавају две врсте 1) безбедносна аналитика у војсци (оружаним снагама), именована као *обавештајна аналитика* и 2) безбедносна аналитика изван војске, односно у полицији, службама безбедности и другим секторима који се баве безбедносном проблематиком, именована као *криминалистичка* (криминалистичко-обавештајна) *аналитика* (*анализа).* С друге стране, иако се користи општи назив „безбедносна аналитика“, акценат је на термину „обавештајна“ (intelligence). У теорији се

сматра да је управо превод енглеске речи *intelligence* узрок свих спорења око назива аналитике. „На пример, синтагма *Business Intelligence* дуго је превођена као ‚пословна интелигенција', док се, временом, није усталио одгварајући и исправан назив – *пословно-обавештајна делатност*" (Краљ, 2019: 4).

У складу с претходно наведеним, кључни проблем јесте реч *intelligence*, за коју у српском и језицима региона нема адекватног превода. Стога, буквалан превод *intelligence* јесте – „обавештајно". Међутим, и у енглеском језику за тај термин постоји више значења, од којих истичемо нека:

- *Dictionary.com* реч *intelligence* тумачи као „информације о непријатељу или потенцијалном непријатељу; процењени закључци из таквих информација; организација или агенција која се бави прикупљањем таквих информација" (http://mup.rs/wps/portal/sr/direkcija-policije/ojdpp/uprava+kriminalisticke+policije/szka).
- Речник *Oxford English Dictinory* дефинише *intelligence* на следеће начине: „**а**. знања о догађајима која се саопштавају или добијају једна од друге; информације, вести, специјалне информације о војној вредности... **б.** део информација или вести... **ц.** добијање информација; агенција за добијање тајних података; тајна служба... **д.** одсек државне организације или војне или поморске службе чији је циљ добити информације" (посебно помоћу тајних служби или система шпијуна) (https://en.oxforddictionaries.com/definition/intelligence).
- Према тумачењу *Geneva Centre for Democratic Control of Armed Forces – DCAF,* обавештајна делатност односи се на начин на који држава поима своје стратегијско окружење, а који је заснован на прикупљању и анализи података прикупљених од тајних и јавних извора (Geneva Centre for Democratic Control Armed Forces, 2006).
- Вернон Валтерс (Vernon Walters), бивши заменик директора ЦИА-е дефинише *untelligence* као информације које нису увек доступне јавности, које се односе на снаге, ресурсе, способности и намере стране државе, а које могу утицати на животе грађана и безбедност матичне државе (ЦИА, 2024).
- Службеник Националног обавештајног савета САД (National Intelligence Council – NIC) Марк Ловентал (Mark Lowenthal), *intelligence* тумачи као процес којим се траже специфичне врсте информација важне за националну безбедност; прикупљају, анализирају и користе по налогу законите власти, те се властите информације и обавештајни производи штите од страних противобавештајних активности (ЦИА, 2024).

Анализа постојећих дефиниција неспорно указује на сложеност појма „intelligence /обавештајно". С једне стране, под тим се подразумева информација о другима, а с друге, делатност за прибављање таквих информација односно организација која, спроводећи такву делатност, има задатак да прибави информације о другима. Дакле, појам „обавештајно" подразумева и *информацију и делатност и организацију* (Moore, 2007). При томе је потребно истаћи да појам „обавештајно" (intelligence) има квалитативно већу вредност, односно да је квалитативно много више од информације. Intelligence укључује

континуирано и системско прикупљање, верификацију и анализу података односно информација како би се омогућило што потпуније схватање и разумевање одређеног проблема, догађаја или ситуације. При томе, битно је да тај крајњи „intelligence“ производ, који омогућава разумевање и схватање одређеног проблема, садржи и акциони елемент, тј. да је подлога за доношење одлука актерима надлежним за одлучивање, то јест предузимање одређених акција (Биланџић, 2008: 38). *Дакле, формално посматрано, реч Intelligence подразумева буквалан превод – обавештајно. У суштинском смислу, термин Intelligence преводимо као (са)знање – ново знање настало у низу: податак-информација-обавештајна информација (знање).*

Други аспект теоријске недоречености безбедносне аналитике у пракси, поготово кад су државне и војне службе у питању, јесте однос њиховог назива и намене. Тако, рудиментарно, на нивоу државе и у оружаним снагама, кад је ова делатност у питању, постоје *обавештајна* и *безбедносна* служба, које се обједињено називају као *службе безбедности* или одвојено као *обавештајне* и *безбедносне (контраобавештајне) службе*. Циљ њиховог деловања је исти – безбедност војске и државе, само су им задаци и начин рада различити. Док обавештајна служба, примарно, прикупља податке и информације о непријатељу (*субјекту угрожавања*), дотле се безбедносна служба бави општебезбедносним и контраобавештајним пословима. Општебезбедносни и контраобавештајни послови примарно су усмерени на одбрану/заштиту *субјекта безбедности* (систем безбедности) и *референтног објекта* заштите/безбедности. Оно што спаја обавештајну и безбедносну (контраобавештајну) службу (агенцију) јесу информације (сазнања), на основу којих те службе (агенције) раде или сазнања која достављају доносиоцима одлука у систему безбедности потребних за њихов рад (одлучивање и предузимање активности). Та чињеница о потреби за прикупљањем информација (сазнања) и њиховим превредновањем за потребе свог или деловања доносилаца одлука у систему безбедности, безбедносну аналитику формално фокусира на „обавештеност“ (информисаност), те се и именује као *обавештајна аналитика.*

Трећи аспект својеврсне недоречености безбедносне аналитике јесте шири процес у коме се та делатност одвија. Интересантно је да без обзира на то о којој врсти безбедносне аналитике говоримо (подручје у ком се примењује), тај шири процес у коме се она одвија именује се на исти начин као *обавештајни циклус.* У теорији се појављују радови који

указују на то да је израз „обавештајни циклус“ више традиционалан и да вуче корене из војске, али да се, као такав, задржао до данашњих дана.

Иако је наведена дефиниција обавештајног циклуса јасна и прецизна, ипак, у пракси постоји мноштво приступа о активностима (корацима) које тај циклкус чине (Табела 3).

Табела 3. *Различити погледи на садржаје обавештајног циклуса*

	АУТОР	**САДРЖАЈИ ОБАВЕШТАЈНОГ ЦИКЛУСА**
1,	Шерман Кент	1. Појава обавештајног проблема који заслужује пажњу стратегијских обавештајних служби 2. Анализирање обавештајног проблема и детаљно сагледавање свих његових страна 3. Разматрање расположивих и прикупљање нових података 4. Критичко процењивање података 5. Проучавање процењених података као предуслов за одређивање хипотеза 6. Прикупљање података у правцима које одређују постављене хипотезе 7. Излагање – утврђивање веродостојности једне или више хипотеза
2.	Хари Ренсом	1. Прикупљање „сирових обавештајних података“ 2. Процењивање и производња тј. проверавање, разврставање и процењивање веродостојности прикупљених информација, извлачење значајних закључака и њихово тумачење у складу са потребама корисника 3. Уступање обавештајних сазнања корисницима у најприкладнијој форми
3.	Лок Џонсон	1. Планирање 2. Прикупљање информација 3. Обрада и анализирање информација 4. Уступање информација
4.	Лиса Кризан	1. Планирање и усмеравање 2. Прикупљање информација 3. Обрада информација 4. Анализа информација и продукција 5. Уступање (дисеминација) аналитичких производа
5.	Вилијам Одом	1. Управљање обавештајним радом 2. Прикупљање обавештајних информација 3. Анализа 4. Производња завршних обавештајних сазнања 5. Уступање производа 6. Повратна спрега
6.	Младен Бајагић	1. Уочавање безбедносног проблема 2. Утврђивање обавештајних потреба 3. Преношење обавештајних захтева 4. Иницијатива 5. Планирање и организовање обавештајног истраживања 6. Прикупљање сирових обавештајних информација 7. Обрада информација 8. Израда сирових обавештајних докумената 9. Уступање завршних обавештајних докумената 10. Техничка интерпретација завршних обавештајних сазнања 11. Повратна спрега

Извор: *Бајагић, 2010 (допунила ауторка дисертације)*

Према подацима из Табеле 3, уочавамо да се број активности (корака) обавештајног циклуса креће од три до 11. При томе, интересантно је уочити да се нигде не користи реч

„аналитика“, већ „анализа“ или „израда обавештајних докумената“ (аналогно – анализа). Једино је Хари Ренсом у свом приступу обавештајном циклусу, у другом кораку, идентификовао активност која би могла да се именује као аналитика, односно шире од појма анализа. Да бисмо што верније приказали функционисање безбедносне аналитике у пракси, анализираћемо њене врсте у оружаним снагама и у полицији, односно службама безбедности појединих држава, ОЕБС и у ЕУ.

2.1 Обавештајна аналитика

Од када постоје односи међу државама, постоји и обавештајни рад у неком облику. Сакрити сопствене поверљиве податке, а дознати туђе одувек је био императив безбедносне превенције, али и проактивног деловања. Обавештајни рад је данас недвосмислено повезан са националном безбедношћу и политичком стабилношћу. Стога се владе и политичко руководство држава чврсто ослањају на рад обавештајних служби. Основни задатак ових служби је прикупљање информација и података који су значајни за вођење политике земље и предузимање различитих поступака у рату и миру у циљу остварења политичких и државних циљева. Ове службе се старају да се државно руководство оријентише само ка веродостојним и провереним подацима. Тако обавештајне службе изузетно доприносе функционисању државног апарата како на унутрашњем тако и на спољашњем плану.

Обавештајна активност, као један од три кључна канала информисања и битан елемент националне моћи сваке савремене државе и њеног система безбедности, у најопштијем смислу „подразумева целисходно, правовремено, планско, тајно и организовано прикупљање и обраду обавештајних информација које се кроз процес анализе, обраде и интеграције претварају у завршно обавештајно знање о датом проблему, појави или догађају и, у форми завршних обавештајних докумената, уступају крајњим корисницима“ (Бајагић, 2010: 193).

Суштину постојања обавештајних служби чини обавештајни рад, односно обавештајна активност чији је развој условљен и снажно детерминисан класним обележјем. Обавештајна активност је пре свега политички процес јер „представља скуп понашања и активности различитих облика груписања и повезаности људи који се руководе одређеним потребама и интересима, одређеним представама и схватањима, који

употребљавају различита средства и методе како би утицали на друштвена кретања у складу са својим потребама, интересима и схватањима“ (Савић и сар., 2002: 7).

У теорији се често наилази на ставове да је обавештајна делатност стара колико и људска историја. Они аутори који желе да ближе одреде зачетке обавештајне делатности обично је везују за настанак држава и међудржавних односа. Везивање за државу као творевину која диктитра и највише користи обавештајну делатност протеже се и на савремене државе које теже да дођу до података о тајним плановима, намерама и активностима других држава, а да истовремено сакрију сопствене податке. У том процесу значајну улогу имају обавештајне службе и аналитички сектор. Тако Стајић (2008) наводи да „обавештајна служба ствара услове да руководство земље (политичко, војно и др.) своју активност усмерава само ка поузданим, веродостојним и тачним подацима“ (стр. 124).

Крајем 20. и почетком 21. века безбедност постаје значајна тема за различите научне дисциплине, а у оквиру безбедности како националних држава тако у контексту међународне безбедности посебно место заузима обавештајна активност. Све више се јављају схватања која обавештајну активност повезују са појмом моћи.

Како наводи Џозеф Нај (2021) (Joseph Nye): „моћ је способност да остваримо нашу сврху или достигнемо наше циљеве. Још прецизније речено, то је способност да се утиче на друге и да се остваре жељени резултати. Постоји много фактора који утичу на нашу способност да добијемо оно што желимо, а варирају у зависности од контекста односа“ (). У смислу ових навода, уколико једна страна поседује више информација о другој страни лакше ће је навести да учини оно што прва страна жели. На тај начин обавештајна активност може заиста бити повезана са појмом моћи.„ С обзиром на то да је обавештајна активност често истраживана област у теорији међународних односа, она се схвата и као градивни део националне моћи државе, али и средство за усмеравање употребе те моћи у облику офанзивне силе или разумевања нечијег окружења и могућности, и начина како применити силу или моћ и против кога. Стога се обавештајна активност мора разумети као незаобилазна категорија у проучавању савремене међународне стварности, посебно у контексту новог безбедносног окружења XXI века“(Бајагић, 2010: 194

Иако општеприхваћена дефиниција обавештајне активности не постоји, може се рећи да она, у општем смислу, „подразумева целисходно, правовремено, планско, тајно и

организовано прикупљање и обраду обавештајних информација које се кроз процес анализе, обраде и интеграције претварају у завршно обавештајно знање о датом проблему, појави или догађају и, у форми завршних обавештајних докумената, уступају крајњим корисницима“ (Бајагић, 2010). Из наведеног се види значај оперативности и праксе када се говори о обавештајним активностима и, стога, тешко је теоријски одредити овај појам без тесне повезаности са практичном применом. Можемо рећи да је теоријски оквир обавештајне активности заснован на пракси, то јест на искуствима обавештајних служби савремених држава. Различити приступи у пракси су између осталих и један од разлога зашто не постоји општеприхваћена дефиниција овог појма.

Данас је више него икада јасно да обавештајни рад није пуко прикупљање информација већ и да је у великој мери координатор политичких активности како на унутрашњем тако и на међународном плану. „Зато се у савременим условима развоја међународних односа на почетку XXI века обавештајна активност сматра једним од кључних елемената националне моћи држава и међународног система у целини, пре свега због њеног значаја у превенцији глобалних претњи безбедности (тероризам, организовани криминал, оружје за масовно уништење и др.)“ (Бајагић, 2010: 200.). Централни појам у литератури која се бави обавештајним активностима јесте појам *обавештајног циклуса* па стога овај појам завређује посебну пажњу у разматрању савремених обавештајних активности.

2.1.1 Обавештајни циклус

Колико је израз *обавештајни циклус* традиционалан и везан за војску, толико и још више синтагма *обавештајна аналитика* среће се само у војсци, док се у осталим секторима безбедности конкретније одређује додавањем атрибута тог сектора, као на пример, криминалистичко-обавештајна аналитика. Тако, обавештајна аналитика се примарно везује за спољну компоненту безбедност државе, те је предмет рада државних и војних служби безбедности.

Форца и Аночић (2018) за обавештајну аналитику кажу: „Обавештајна аналитика је посебна дисциплина безбедносне аналитике; област аналитике која је тежишно окренута ка спољној безбедности; користи широк спектар извора података; примењује посебне

поступке за процесуирање података; примењује специфичне мисаоне процесе и логичке операције у поступку израде обавештајних информација“ ().

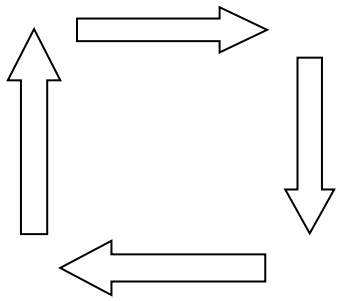
„Обавештајни циклус представља врсту модела по коме се управља обавештајним захтевима и самим процесом прикупљања и обраде података и достављања обавештајног производа крајњим корисницима. Обавештајни циклус се састоји из више динамичних фаза и има цикличан карактер јер обавештајни рад захтева континуитет и ажурност. Стога је обавештајни циклус процес који се константно понавља у раду обавештајних субјеката“ (Андрић, Терзић, 2023: 4.).

У обавештајном циклусу користи се велики број научних метода, примењивих за конкретна обавештајна истраживања. Обавештајни циклус се, као и научно истраживање, одвија по одређеним логичким и техничко-организационим правилима. То подразумева да се током прикупљања података комбинују обавештајне и научне методе. Такође фазе обавештајног циклуса су у великој мери сличне научном истраживању.

Обавештајна (војна) аналитика се одвија у оквиру обавештајног циклуса, о коме, у смислу фаза (корака) који га чине, постоје различита виђења. У домаћој обавештајној пракси (Форца и Аночић, 2018), као и у *НАТО обавештајној доктрини (*Allied Joint Intelligence, AJP, 2003), кораци (фазе) обавештајног циклуса су: 1) *издавање задатака* (наређења), 2) *прикупљање података*, 3) *производња обавештајних информација – аналитика*, и 4) *достављање обавештајних информација корисницима*. Дакле, фаза (корак) „производња обавештајних информација“ именована је као аналитика. Иако су чланица и водећа сила НАТО, у оружаним снагама САД се обавештајни циклус операционализује на шест фаза: 1) планирање и издавање задатака, 2) прикупљање података, 3) процесуирање – обрада и експлоатација, 4) анализа и производња информација, 5) достављање обавештајних производа и 6) пријем повратних података о ваљаности достављеног обавештајног производа (Joint and National Intelligence Support to Military Operations, J-2-01– 5, 2012).

У свом делу *Грешке и заташкавања војно-обавештајних служби* Џон Хјуз-Вилсон (John Hughes-Wilson) обавештајни циклус приказује као у наредној табели (Hughes-Wilson, 2013).

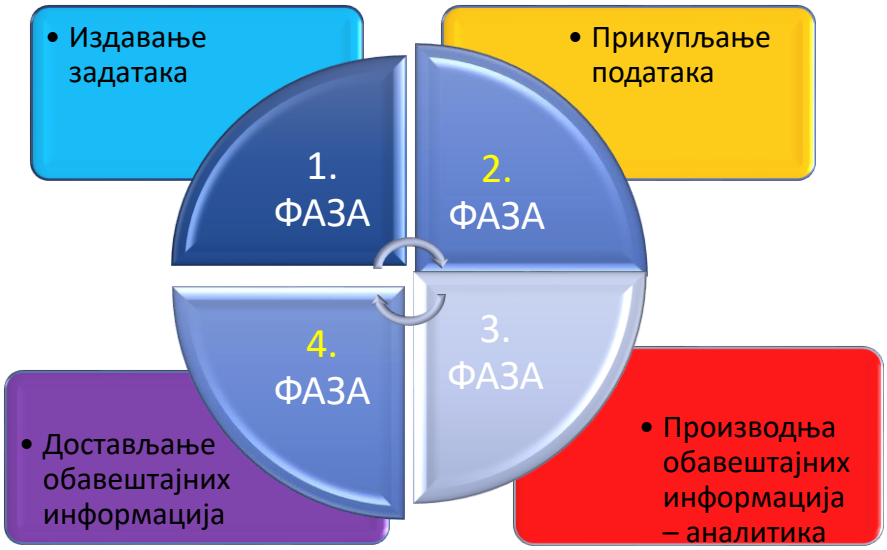
Табела 4. *Обавештајни циклус*

<table>
<tr><td colspan="3">Обавештајни
Циклус</td></tr>
<tr><td></td><td>Издавање задатака
Командант или политички лидер износи свој обавештајни захтев, обично у форми питања</td><td></td></tr>
<tr><td>Достављање корисницима
Може имати различите форме: писани извештај, хитна порука, обавештајни преглед или, углавном у хитним случајевима, усмени извештај политичком лидеру или команданту</td><td>  </td><td>Прикупљање података
Обавештајни штаб претвара командантов обавештајни захтев у серију суштински важних елемената информације и даје задатке обавештајним агенцијама применом Плана прикупљања података</td></tr>
<tr><td>Анализа, тумачење и закључивање
Прикупљени и сређени подаци се анализирају, тумаче и доносе закључци у форми обавештајне информације.
Ово се обично решава давањем одговора на кључна питања:
ко ради, шта ради и шта то за нас значи</td><td>Израда обавештајних информација</td><td>Процесуирање – евидентирање, слагање и упоређивање података
Обавештајни штаб или аналитички део службе сређује и упоређује све расположиве обавештајне податке, израђујући лако доступну базу података.
Суштински је важно да се за све прикупљене податке зна из ког извора потичу</td></tr>
</table>

Извор: *Хјуз-Вилсон, 2013 (обрада ауторке дисертације)*

Без обзира на наведене класификације садржаја обавештајног циклуса, њихова суштина се своди на логичан след корака: 1) правовремено прикупити неопходне податке и информације, 2) обрадити их применом строгих правила аналитичког процеса, 3) проценити их и 4) израдити готов обавештајни производ који ће на време бити доступан кориснику или наручиоцу – доносиоцу одлука или политичком лидеру (Вилсон, 2013).

У различитим документима, како смо приказали, могу се наћи различите класификације фаза обавештајног циклуса па се негде помиње и пет и шест и више фаза. Међутим, већина аутора се слаже да постоје четири кључне фазе обавештајног циклуса: 1) издавање задатака (наређења), 2) прикупљање података, 3) производња обавештајних информација – аналитика и 4) достављање обавештајних информација корисницима (Андрић, Терзић, 2023).



Слика 6. *Графички приказ обавештајног циклуса*

Извор: *Андрић и Терзић, 2023.*

„Из познатих теоријских и организацијских модела обавештајног циклуса уочава се да се, као и код процеса спољнополитичког одлучивања, ради о планском процесу који почиње и пре самог отпочињања прикупљања обавештајних података.“ (Бајагић, 2015: 98). Дакле, пре него што дође до издавања задатка, постоје одређене околности из окружења које доводе до сазнања да постоји обавештајни проблем на који треба усмерити пажњу. Политичко руководство у сарадњи са обавештајним структурама усмерава рад обавештајних субјеката. Форца (2018) наводи да се фаза издавања задатака састоји од: 1) одлучивања о обавештајним захтевима, 2) планирања процеса прикупљања података, 3) издавања захтева и наређења за прикупљање података и 4) континуираног праћења продуктивности прикупљачких органа и агенција (Форца и Аночић, 2018).

У војно-обавештајним органима, који се тежишно баве обавештајном аналитиком, та аналитика се поистовећује са трећим кораком обавештајног циклуса – *израда обавештајних информација.* То је, свакако, практично упрошћавање процеса, јер, иако ће обавештајна информација бити продукт аналитике, не сме се занемарити обиман и сложен мисаони, аналитичко-синтетички напор аналитичара да до те информације дођу. Стога, и у нашој обавештајној пракси и пракси САД, израду обавештајних информација можемо рашчланити на два корака која обухватају 1) *процесуирање* – обрада података и

информација и 2) *закључивање и процењивање* – анализа, тумачење и процена информација (Форца и Аночић, 2018).

2.1.1.1 Процесуирање (обрада) улазних података и информација

Ово је, практично, први корак (фаза) обавештајне аналитике као дела обавештајног циклуса. Принципијелно, овај корак (фаза) састоји се од следећих активности: 1) оцена поузданости извора и тачности податка, 2) разврставање и упоређивање података и информација и 3) слагање података и информација у базу.

1) Податак је основно сазнање или чињеница о неком догађају, појави, процесу, организацији или личности. Податак, као „сиров", сам за себе (по себи), како је дефинисан, нема велику употребну вредност за обавештајног аналитичара, док се не провери његова веродостојност (да није намерно потурен – дезинформација). Такође, у обавештајној аналитици сиров податак се мора довести у конкретну, прецизно утврђену форму. Када се податак преведе у одређену форму, а по унапред утврђеним методима оцене поузданости, обавештајни аналитичари приступају оцени поузданости извора који је доставио податке, као и самих података.

Обавештајне службе применом различитих обавештајних метода и коришћењем свих обавештајних извора прикупљају како сирове (необрађене) податке *так*о и оне који могу, а неретко и морају, бити хитно достављени политичком, војном или обавештајном руководству. Ова фаза подразумева прикупљање података из отворених (јавних) и тајних извора. „У последње две деценије дошло је и до развоја размене података између сарадничких служби безбедности преко официра за везу. Напретком технологија, посебно у области електронских комуникација, службе безбедности су почеле интензивно да се ослањају на прикупљање података пресретањем комуникација, где се не прикупља само садржај комуникација *већ* читав низ других података, попут, на пример, с ким је комуницирано и колико често, као и време, место и дужина трајања комуникације, који се најчешће збирно називају метаподаци. У ове податке спадају и они који се односе на употребу интернета и друштвених мрежа" (Петровић, 2020: 90).

„Неки аутори (аналитичари) у својим радовима наводе процене о томе колико се од укупног фонда прикупљених података добија из отворених, а колико из затворених извора. Ти проценти се крећу од 80 према 20 одсто до 90 према 10 одсто у корист података

из отворених извора. Иако се однос процената тешко може прецизно израчунати, чињеница је да отворени извори дају много више података“ (Бошковић, 1996: 122).

Овакав обим јавно доступних података омогућио је и да се на нека питања до одговора може доћи само на основу отворених извора података, те да илегални или прикривени методи рада уопште нису потребни. Наравно, увек се полази од јавно доступних података, а потом се они користе и током прикривеног обавештајног рада. Такође, коришћење оваквих извора, где околности то дозвољавају, омогућава и економисање расположивим људским и техничким ресурсима. Тако се они могу усмерити на решавање сложенијих и одговорнијих задатака, где је с обзиром на крајњи циљ оправдана и употреба илегалних метода и средстава.

Како наводи Бошковић (1996), постоје три основне области у којима се користе отворени извори:

- **Опште политичке, војне и економске информације** које су потребне за процену политичких прилика, војног чиниоца, економског потенцијала и морално-политичког стања у држави и њеним оружаним снагама које су објект обавештајног истраживања. Подаци из те групе су најшири према обиму и изворима и могу да послуже за стратегијску процену војних и цивилних органа и за пропагандно-психолошку активност.
- **Стручне и специјализоване обавештајне информације** и подаци који се односе на конкретне области науке, економике, технике и војске. Намењене су за ужи круг стручњака и служе као материјал за разраду стратегијских планова.
- **Биографски подаци** Односи се на прикупљање података о значајним војним, политичким и другим личностима земље. Овде предмет интересовања могу бити и мање запажене личности или младе особе које могу имати одређени потенцијал или неку значајну улогу у будућности. Овакви подаци помажу аналитичару да предвиди будуће понашање те личности, његове организације или војне јединице. Познато је да се америчка ЦИА посебно бавила прикупљањем оваквих података, сматрајући их изузетно корисним.

Планирано и систематско прикупљање и анализа обавештајних информација одликује усмереност на научне методе, односно давање одговора о:

1) трендовима и шаблонима догађаја који се истражује,
2) његовој фреквенцији (учесталости) и
3) процени вероватноће његовог даљег развоја и последица које може изазвати (Бајагић, 2015).

Бошковић и Матијевић (2010) наводе више модела (метода) оцене поузданости извора и тачности података, од којих су у теорији најпознатији „4 x 4“, „5 x 5“ и „6 x 6“. Можемо уочити разлике модела у САД (Табела 5) и модела који примењују наши обавештајни аналитичари (Табела 6).

Табела 5. *Модел САД („6 x 6“)*

Поузданост извора		Тачност податка	
A	потпуно поуздан	**1**	потврђен из других извора
B	углавном поуздан	**2**	вероватно тачан
C	прилично поуздан	**3**	могуће тачан
D	углавном непоуздан	**4**	Сумњив
E	непоуздан	**5**	није вероватан
F	поузданост се не може оценити	**6**	истинитост се не може оценити

Извор: *Форца и Аночић, 2018.*

Табела 6. *Наш модел („4 x 4”)*

Поузданост извора		Тачност податка	
A	поуздан	**T**	Тачан
B	углавном поуздан	**V**	Вероватан
C	углавном непоуздан	**S**	Сумњив
D	непоуздан	**L**	Лажан

Извор: *Форца и Аночић, 2018.*

Из табела 5 и 6 може се закључити да је обавештајни систем САД захтевнији по питању одређивања прикупљачких органа према добијеним подацима, што је и разумљиво ако се има у виду ширина спектра извора и платформи за прикупљање података којима располажу САД.

Прелиминарна оцена поузданости извора у суштини зависи од искуства аналитичара о подацима које је одређени извор већ достављао, али је увек субјективна. С друге стране, уколико су подаци прикупљани техничким средствима (сензор), њихова поузданост је непосредно везана за карактеристике техничких средстава (сензора) којима су ти подаци прикупљени. Оцена поузданости извора и тачности података не смеју се, *a priori*, узимати у директној корелацији, о*дно*сно треба посебно да се анализирају. Наиме, искуства показују да и најпоузданији извор не мора увек давати високо поуздане податке. С друге стране, подаци добијени од извора који је оцењен као „углавном непоуздан“, понекад се појављују потпуно тачним.

Како би обавештајни аналитичар могао да верује извору, буде уверен у релевантност податка за проблем истраживања, те убеђен да располаже подацима значајним за закључивање (процењивање), потребно је да зна каква је природа улазног податка. Најчешће, улазни, сирови подаци се квалификују као 1) *опипљив податак и 2) податак базиран на уверењу извора*. Опипљивим се сматрају тзв. материјални подаци, односно они

подаци који су записани на неком медију – карта, скица, фоно или видео запис са различитих платформи, аеро-фото снимак, сателитски снимак. С друге стране, подаци засновани на уверењу се добијају у непосредном разговору са извором (тзв. живи извор).

Обавештајни аналитичар на разне начине утврђује вредност опипљивог и податка заснованог на уверењу (Табела 7).

Табела 7. *Утврђивање вредности сирових података*

ОПИПЉИВ ПОДАТАК	ПОДАТАК ЗАСНОВАН НА УВЕРЕЊУ
АУТЕНТИЧНОСТ: Да ли је податак заиста оно што изгледа да јесте?	**ПОУЗДАНОСТ ИЗВОРА**: Оцењује прикупљач података или аналитичар. Не постоје трајно поуздани извори! „Живи извори“ могу имати различите разлоге да саопште лажан податак.
ПРЕЦИЗНОСТ: Да ли је извор или сензор могао да открије оно што мислим да податак саопштава?	**УБЕДЉИВОСТ „ЖИВОГ ИЗВОРА“:** Подаци засновани на уверењу су мање убедљиви од опипљивих података.
РЕЛЕВАНТНОСТ ЗА ПРОБЛЕМ: Да ли сам из различитих извора добио исте или сличне резултате?	

Извор: *Форца и Аночић, 2018.*

2) Разврставање и упоређивање података и информација јесте корак у обавештајној аналитици, који следи након провере поузданости извора и тачности података-информација. Разврстати податке значи груписати их у складу са њиховом повезаношћу ради даљег рада са њима. То груписање подразумева евидентирање свих пристиглих података и извештаја, а спроводи се 1) додељивањем идентификационог броја, те увођењем у евиденцију и 2) слагањем у одговарајућу категорију или групу, наношењем на радну карту, попуњавањем индекса података или уносом у електронску базу података. Подаци се разврставају одвајањем по унапред утврђеним групама (категоријама), у зависности од проблема који се решава или од природе самих података. За то постоје картотеке, елаборати и друге форме разврставања података. На пример, подаци о некој личности разврставају се у *картотеку личности*, а подаци о страним оружаним снагама разврставају се у *елаборату оружаних снага* страних држава и слично. Неки подаци, због хитности поступања, одмах се шаљу на даљу обраду, **одно**сно достављају овлашћеним корисницима (Форца и Аночић, 2018).

Ретко се дешава, иако није немогуће, да се ради о потпуно новим подацима који се прикупљају. У том смислу, *упоређивање података* јесте мисаоно закључивање о

сличности и разликама новопристиглог са подацима којима служба располаже. Поређење података је обавезан корак у поступку њихове обраде, јер се тим кораком, између осталог, сазнаје да ли: 1) нови податак потврђује већ расположива сазнања о објекту или проблему истраживања и да ли се може сложити у базу података, 2) нови податак није сагласан са расположивом базом података, те га је потребно накнадно допунити из истог извора или проверити ангажовањем нових извора и 3) нови податак је таквог значаја да је неопходно хитно поступање ради његовог адекватног процесуирања и достављања надлежним органима (Форца и Аночић, 2018).

Производња обавештајних информација – аналитика је трећа кључна фаза у обавештајном циклусу. Ова фаза се често назива и фаза обраде података, где сирови податак или више њих након обраде може да постане аналитичка информација. ..Аналитичка информација је више од информације, реч је о синтези података и информација која конституише знање, с намером да се оно искористи за одређено (конкретно) поступање (потребу) корисника (на пример, решавање проблема, откривање потенцијалне прилике за деловање, избегавање проблема и сл.)“ (Ђурђевић и Милић, 2020: 90). Дакле, ова фаза обавештајног циклуса се завршава израдом обавештајног производа који може бити у различитим формама. „Продукти такве обраде су разни документи- обавештајне информације, анлитичке и динамичке обраде, стратегијске информације, процене и слично“ (Бошковић, 1996: 127). Значајно је напоменути да је ова фаза интелектуално најзахтевнија и захтева одређене способности и умешност аналитичара који врши обраду података.

Сврха прикупљања информација и њихова обрада у оквиру обавештајног рада је долазак до закључка о постојању одређених веза између појава и процеса које су предмет обавештајног интересовања. Процес обраде података у обавештајном циклусу чини више међусобно повезаних активности:

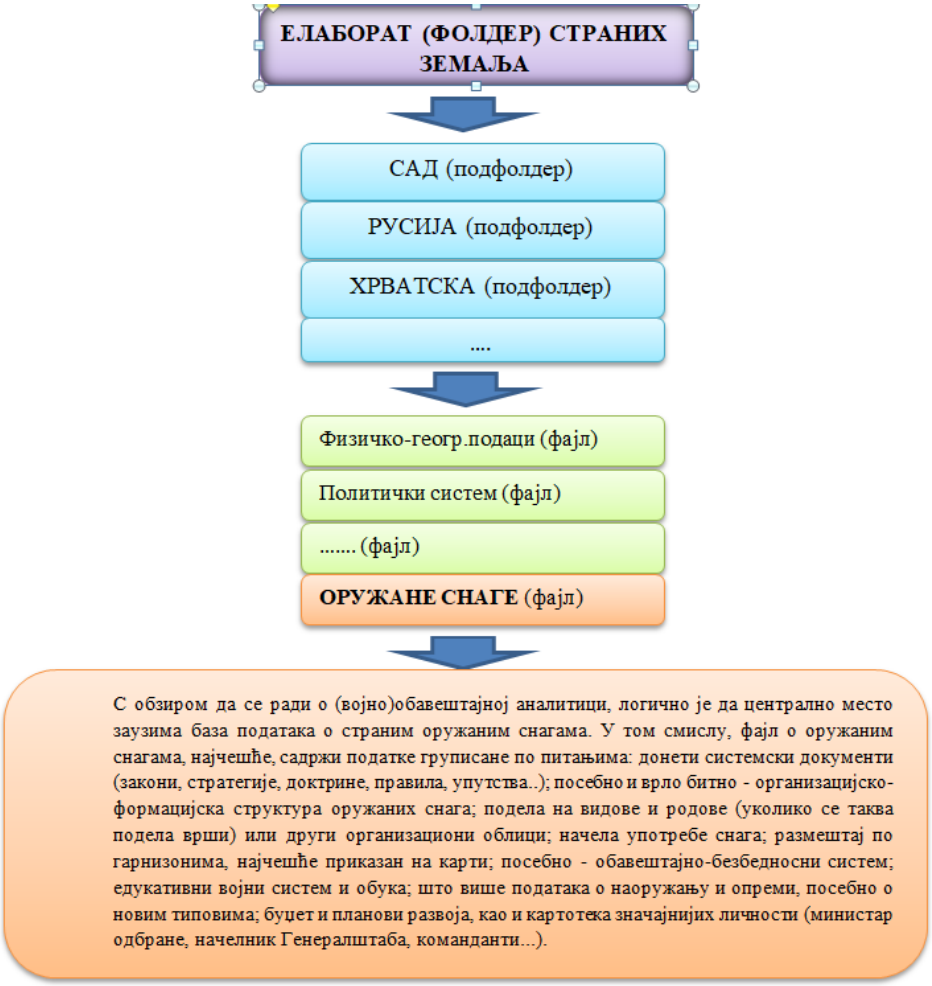
- разврставање (класификација) сирових информација, њихово процењивање и
- анализирање, тумачење и обједињавање.

Из наведеног видимо да постоји сличност са методама научног истраживања, као што су класификација, индукција и дедукција.

„Коришћење укупног обавештајног материјала може да се подели у неколико категорија. Примарна категорија је временски чинилац, тј. када је информација приспела,

који омогућује да се све сређује хронолошки. Информације могу да се групишу и систематизују према предметима, тј. областима интересовања, односно основна подела информација обавља се према њиховој садржини“ (Бошковић, 1996: 127). Класификација прикупљених података се може вршити по више критеријума. Тако се подаци могу разврставати по природи на економске, еколошке, политичке, војне и слично. Подаци се даље могу класификовати по областима па се тако, на пример, у области одбране подаци по значају могу класификовати на стратегијске, оперативне и тактичке. Такође, прикупљени подаци се упоређују са дотадашњим сазнањима. Где опет наилазимо на сличност са научном методом компарације.

3) Смештање података и информација у базу јесте корак обавештајне аналитике, након што су подаци разврстани и упоређени са претходним. Оцењен, разврстан и упоређен (база података) с другима, податак се похрањује (слаже) у постојећу базу података или се прослеђује на даље процесуирање аналитичкој служби. Базе података модерних обавештајних служби су електронске, засноване на модерној информационој технологији. Међутим, те базе могу бити и писане (картотека). Независно од врсте базе података (електронска или писана картотека), подаци који се налазе у бази морају да буду сложени одговарајућим редом и по логичким целинама, као и да буду потпуно разумљиви и стално доступни. Типичан (обавезан) пример сложених података у бази обавештајних служби јесте *Елаборат страних држава*. У електронској форми вођен, тај елаборат - (фолдер) садржи потфолдере са називима оних држава о којима водимо податке. Надаље, потфолдере чини унифициран (за све земље се води по јединственом општем садржају) скуп докумената (фајлова) који, на пример, обухватају: физичко-географске податке (површина, број становника...); податке о политичком систему; податке о буџету, економији, индустрији, пољопривреди; податке о значајнијим научно-техничким достигнућа и плановима и, наравно, податке о оружаним снагама (који су опет приказани по тачно утврђеном моделу) и друго (Слика 7).



Слика 7. *Елаборат (фолдер) страних земаља*

Извор: *Форца и Аночић, 2018 (обрада ауторке дисертације)*

Постоји још један документ – *Табела индикатора и упозорења*, који се не сматра посебним кораком у обавештајној аналитици, али јесте оперативни документ који има практичну употребу. То није унифицирани документ који би могле да користе све обавештајне структуре, у свим ситуацијама. Напротив, овде је реч о радном документу који је специфичан за сваку обавештајно-безбедносну аналитичку службу и за сваки ниво обавештајног штаба.

Конкретна питања се формулишу у зависности од проблема који се решава. Тако, на пример, ако се желе установити офанзивне намере суседне земље, наша аналитичка служба ће поставити следећа питања:

- да ли је противник набавио ново офанзивно наоружање;
- какво је расположење јавности противника према нама;

- какав став има међународна заједница према проблему;
- какве изјаве дају дипломатски представници те државе;
- какав је однос према нашој мањини у тој држави;
- да ли је интензивиран обавештајни рад;
- да ли је интензивирано увежбавање ваздухопловних снага итд.

Одговори на ова питања налазе се у бази података или се дају задаци прикупљачким органима да допуне оно што није познато. С друге стране, обавештајни штаб команде корпуса који је посео положаје за одбрану у својој зони, поставиће другачији сет питања настојећи да реши проблеме као што су: када ће непријатељ напасти, који му је главни правац напада, како ће груписати и употребити расположиве снаге:

- где се налази рејон прикупљања снага противника,
- какав му је борбени распоред,
- има ли подршку авијације и које врсте;
- који је калибар артиљеријских оруђа и где се налазе ватрени положаји;
- да ли је извршена мобилизација резервног састава;
- да ли старешине одлазе кући или бораве у касарнама;
- има ли вежбовних активности противника итд.

Као што се види, за два различита проблема постављена су два различита сета питања, што је сасвим логично. Такође, ако противник не поседује морнарицу ни балистичке ракете које могу досећи на нашу територију, логично је да нећемо тражити одговоре на питања где су усидрени бродови или има ли неуобичајених активности око силоса са ракетним наоружањем.

Конкретно постављена питања у табели индикатора и упозорења представљају основу за израду плана прикупљања података, о коме смо говорили у поглављу *Обавештајни циклус*. Када почну да пристижу информације и извештаји од прикупљачких органа, они се, у зависности од одговора, слажу у одговарајућу рубрику (по могућству се одговори формулишу као „да“ или „не“ или „нема података“). Унакрсним поређењем одговора долази се до јасне индикације о намерама противника. На табели се обично користе три боје које индикују степен опасности: зелена – нема опасности, црвена – има опасности, црна – нема одговора на питање (Табела 8).

Табела 8. *Табела индикатора и упозорења (радни документ)*

ПИТАЊА ИЗ ПЛАНА ПРИКУПЉАЊА ПОДАТАКА	Нема опасности	Има опасности	Нема података
Где се налази рејон прикупљања снага противника?			
Какав му је борбени распоред?			
Има ли подршку авијације и које врсте?			
Да ли је извршена мобилизација резервног састава?			
Има ли вежбовних активности противника?			

Извор: *Форца и Аночић, 2018.*

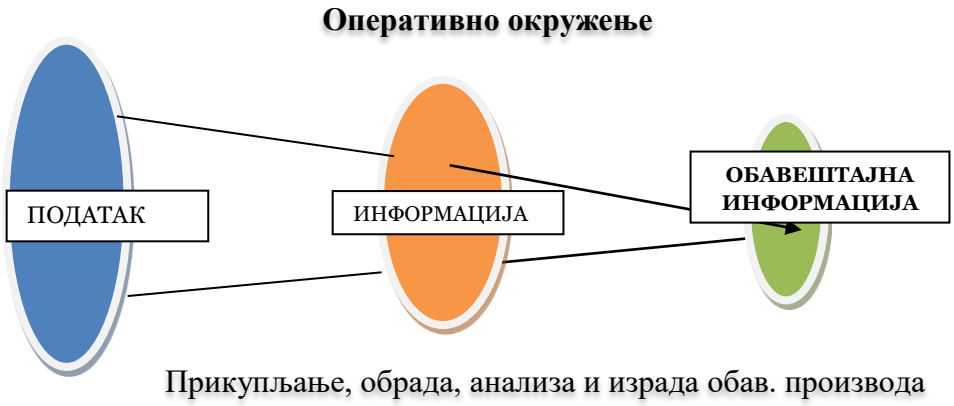
Дакле, ако је, на пример, од пет постављених питања одговор на три у зеленој зони, онда можемо закључити да нема тренутне опасности, што не значи да не треба даље пратити ситуацију. Исто тако, ако је одговор на три питања у црвеној зони, онда све аларме треба одмах укључити. Овде су могуће разне комбинације црвеног, зеленог и црног, а свака комбинација захтева посебан, креативан приступ обавештајног аналитичара том проблему. Посебан куриозитет представља црна боја, то јест одсуство података. Ово никада није добро, јер значи неизвесност, захтева додатне напоре и утиче на логичко резоновање аналитичара. Због тога треба тражити да се неизвесност што пре оконча. Одсуство података не значи и одсуство неке активности, већ је само нама индикатор да обратимо посебну пажњу на то питање. Ако је, пак, реч о одсуству активности као некој неправилности или одступању од уобичајеног поступка (нпр. изостанак редовне годишње обуке, одсуство важних личности са церемонијалних догађаја, забрана коришћења годишњих одмора и одсуства за војна лица итд.), а наши прикупљачки органи су то уочили, онда такви подаци могу имати изузетан значај у табели индикатора и упозорења[13].

2.1.1.2 Закључивање и процењивање – анализа, тумачење и процена информација

Ово је кључна фаза (корак) обавештајне аналитике која треба да резултује обавештајно-аналитичким производом, који ће обавештајна служба да користи у свом

[13] Врло је илустративан пример коришћења *Табеле инидкатора и упозорења* у IV арапско-израелксом рату, 1973. Наиме, Египат и Сирија су својим активностима постигли стратегијско изенађење у нападу на Израел, јер руководство Израела није придавало пажњу тим активностима. Међутим, све те активности је коректно бележио капетан Обавештајне службе Израела у Табели индикатора и упозорења, која је касније пронађена. Египат је повратио Синај, а Сирија део Голанске висоравни. Капетан је, накнадно, ванредно унапређен, али је за Израел било касно. Шире у: **Џон Хјуз Вилсон** (2013), *Грешке и заташкавања војно-обавештајних служби*, Албион-Букс, (Превео: Бранислав Аночић), Београд.

раду и/или који доставља доносиоцима одлука у систему (националне) безбедности. За разумевање израза „обавештајно-аналитички производ“ користи се скала значења: **Податак (data)** је основно сазнање или чињеница о неком догађају, појави, процесу, организацији или личности. **Информација (information)** је податак до кога су дошли прикупљачки органи обавештајне службе, а за који су утврђени поузданост извора и оцењена веродостојност – тачност садржаја. **Обавештајна информација или процена (intelligence)** јепроцесуирана, обрађена информација (проверена, упоређена, сложена) на основу које је, затим, уз примену тачно дефинисаних метода логичког мишљења и закључивања, израђен **„обавештајни производ“** који може имати карактер описа неке чињенице, појаве, процеса или предвиђања – процене будућих догађаја (Слика 8) (Форца и Аночић, 2018).



Слика 8. *Однос између податка, информације и обавештаје информације*

Извор: *Joint Intelligence, USA, JP 2.0, page I-2, 22 June 2007.*

Дакле, у наведеном низу обавештајна информација је производ аналитичког рада. Уједно, то је и један од основних обавештајно-аналитичких производа. Врло корисну и разумљиву дефиницију *обавештајне информације* дао је Вашингтон Плат (Washington Platt), пионир стратегијског обавештајног рада у САД. Он наводи да је то „разумљива тврдња изведена из информације која је одабрана, оцењена, протумачена и коначно представљена тако да је њен значај за конкретан актуелни проблем националне политике јасан“ (Joint Military Intelligence College, 2006).

Све наведено указује да је сврха и бит обавештајне аналитике да од прикупљених, протумачених и оцењених података начини употребљив обавештајни производ (дело). Из напред наведених дефиниција и датих објашњења може се извести закључак да постоје две главне врсте обавештајних производа – 1) *обавештајна информација* – ОИ и 2) *обавештајна процена* – ОП. При томе, у пракси се наведена два производа разликују у томе што обавештајна информација, начелно, говори о капацитетима противника, а обавештајна процена о његовим намерама (Форца и Аночић, 2018). Такође, из праксе се може извући закључак о врстама обавештајних информација и процена (Табела 9).

Табела 9. *Класификација обавештајне информације и обавештајне процене*

ОБАВЕШТАЈНА ИНФОРМАЦИЈА	**ОБАВЕШТАЈНА ПРОЦЕНА**
Обавештајни извештај	Општа обавештајна процена
Посебна обавештајна информација	Посебна обавештајна процена
Обавештајни пресек ситуације	

Извор: *Форца и Аночић, 2018.*

У претходној табели се наведени обавештајни производи разликују по намени и сврси, а што је приказано у Табели 10.

Табела 10. *Карактер обавештајних производа*

ДОКУМЕНТ	ОПИС	СВРХА	ПРИМЕР
ОБАВЕШТАЈНА ИНФОРМАЦИЈА			
Обавештајни извештај	Аналитички документ из ближе или даље прошлости о догађајима који имају утицаја на безбедност.	Искуство, поука, методе и начини употребе снага и сл.	Вежбе НАТО снага у Литванији 2023.
Посебна обавештајна информација	Аналитички документ који се односи на конкретно питање или проблем од утицаја на безбедност.	Упознавање руководства са актуелним догађајима који носе безбедносне изазове и ризике.	Размештај руских снага у Црном мору. Карактеристике кинеског авиона Ј10. Држање албанског премијера током самита ОЕБС-а 2023.
Обавештајни пресек ситуације	Аналитички документ најопштијег карактера који говори о стању у некој земљи или региону.	Упознавање руководства са општим стањем безбедности у одређеном региону.	Актуелно стање безбедности у Украјини. Утицај пријема Финске у НАТО на безбедност Европе.
ОБАВЕШТАЈНА ПРОЦЕНА			
Општа обавештајна процена	Најзначајнији обавештајни производ који даје предвиђање ситуације у одређеном региону у одређеном будућем временском периоду.	Упознавање руководства са очекиваним развојем безбедносне ситуације	Годишња обавештајна процена. Дугорочна обавештајна процена.
Посебна обавештајна процена	Анализа једног или више узрочно--последичних догађаја на безбедност земље.	Предвиђање развоја догађаја поводом неког конкретног проблема.	Подизање модуларних зидова на граници Мађарске и Србије. Хрватска затворила свој граничне прелаз.е

Извор: *Форца и Аночић, 2018.*

Обавештајно-аналитички производи могу да објашњавају шта се и како догодило, што није њихова круцијална вредност. Суштина тих производа требало би да буду одговори на питања: зашто се нешто догодило, како ће се то развијати (предвиђање) убудуће и, посебно – шта, у вези с тим, ваља чинити. О карактеру обавештајно-аналитичких производа врло поучно говори Мајкл Колијер (Michael W. Collier) у свом чланку *Прагматичан приступ развоју обавештајних аналитичара* (*A Pragmatic Approach to Developing Intelligence Analysts*):„Предвиђајућа анализа јесте хлеб и со аналитичара Обавештајне заједнице (ОЗ). Научници из области друштвених наука спроводе релативно мали број предвиђајућих анализа. Клаузер (Clauser) и Вир (Wier) сугеришу три категорије предвиђајућих анализа. **Прва категорија описује догађаје који се дешавају са таквом регуларношћу да су скоро неизбежни**. На пример, лет ‚Британиш ервејза' број 117 стиже у Њујорк из Лондона сваки дан у 11 часова и 15 минута. За предвиђање оваквих догађаја треба мало савремених

,алата'. **Друга категорија описује догађаје који се дешавају током неког временског периода где постоји само минимална сумња у њихов крајњи исход.** На пример, потврђено је да Кинези граде нову класу подморниица, али оно што није познато је када ће први и последњи примерак бити испоручен и колико ће подморница бити у тој класи. Предвиђање ове друге категорије догађаја је мало теже и може захтевати тим научно-техничких и политичко-војних аналитичара који ће радити заједно на овом проблему, уз коришћење разноврсних ,алата'. **Трећа категорија описује краткорочне, јединствене догађаје који се дешавају у одређеном временском оквиру.** На пример, да ли ће Иран развити програм нуклеарног оружја? Ова последња категорија предвиђајуће анализе је најтежи изазов за политичко-војне обавештајне аналитичаре" (Collier, 2005).

Као што се види из напред наведеног цитата, производи проценске (предвиђајуће) анализе су од суштинског значаја за целокупан обавештајни рад. Обавештајне процене које су израђене применом строгих критеријума објективности и правовремено достављене политичком или војном руководству јесу разлог постојања једне обавештајне службе.

Завршна фаза аналитичког процеса (израде обавештајних производа) јесте *интерпретација*. Тако, у *Здруженим обавештајним процедурама НАТО* (Allied Joint Procedures, 2002) *интерпретација* се дефинише као „финални корак у фази обавештајног циклуса – процесуирање – у коме се просуђује значај информације у односу на расположива сазнања. То је завршна фаза процесуирања, где информација која је упоређена, оцењена, анализирана и интегрисана мора бити коначно протумачена ради комплетирања процеса конверзије информације у обавештајни производ. Интерпретација је објективан мисаони процес поређења и дедукције који се базира на здравом разуму, животном искуству, војним подацима и о противнику и о пријатељским снагама, и постојећим информацијама и проценама... Овај мисаони процес може се рашчланити на три принципијелна питања која се морају поставити о информацији која се разматра: а) *Идентификација. Ко је то? Шта је то?* Ово није само пуко одређивање идентитета неке јединице или назива техничког средства, већ разматрање свих последица присуства те јединице или средства на одређеној тачки у одређеном времену и простору; б) *Активност. Шта то ради?* Значај активности која се спроводи мора се увек поредити са информацијама о претходним активностима како би се открило да ли има разлике у обрасцу понашања и в) *Значај. Какви су одговори на прва два питања? Какав је њихов значај? Да ли су и како повезани са борбеним индикаторима који су дефинисани?*

Интерпретација (тумачење) је мисаони процес чији је излазни резултат обавештајна информација или процена. До те информације или процене долази се применом

адекватних метода и модела логичког закључивања, којима се описује, објашњава или процењује – предвиђа неки догађај, процес или појава.

Претходно наведено упућује на једно логично питање: *Да ли је обавештајна аналитика наука или вештина?* Одговарајући на наведено питање, поменути Мајкл Колијер (2005) врло убедљиво и илустративно закључује:

> „Упркос овде јасно наглашеној тежњи за више науке у процесу обавештајне аналитике, још увек постоји велика потреба за јаку дозу вештине – коју ћемо овде дефинисати као ‚примена креативности, имагинације и иновације у том процесу'. Добро поређење може да се направи између лекара дијагностичара и обавештајних аналитичара. Најбољи доктори дијагностичари комбинују достигнућа медицинске науке, стечена образовањем и искуством са израженим способностима критичког мишљења. Постати добар лекар дијагностичар је чак и већи изазов, јер он мора да буде експерт у више наука, као што су:– биологија, хемија, физика и анатомија да би успешно обављао свој посао. Исто важи и за најбоље обавештајне аналитичаре, који морају бити експерти за интердисциплинарне друштвене науке попут политичке теорије, економије, психологије и социологије и да онда ангажују своје образовање и искуство, примењујући способности критичког мишљења обогаћена креативношћу, имагинацијом (маштом) и иновацијом" (Collier, 2005: 19).

Табела 11. *Извори сазнања за аналитичко закључивање*

Извор сазнања	О п и с
Ауторитет	Експерт или неко са ауторитетом (родитељ, наставник или супервизор) нуди сазнање и њему се верује без поговора.
Вера	Сазнање се прихвата без чврстих доказа (религија, идеологија, митови).
Здрав разум	Логично сазнање добијено од других,– „једноставно, то сви знају".
Интуиција	Сазнање које имамо без свесног објашњења истог. Оно долази из унутрашњих логичних уверења или имплицитног повезивања чињеница.
Рационализам	Сазнање добијено кроз виши ниво логичног резоновања (постављање теорије) и засновано на људској способности да резонује независно од актуелног искуства у стварном свету.
Емпиризам	Сазнање генерисано из искуства и систематског посматрања појава и процеса, нпр. прикупљање података помоћу пет чула.
Наука	Комбинација рационализма и емпиризма.

Извор: *Колијер, 2005.*

Обавештајни аналитичар, ма колико био образован (наука) и имао искуства, у интерпретацији обавештајно-аналитичког производа увек се пита: *Да ли сам обманут?* Стога, закључивање мора да пролази кроз фазу постављања, оповргавања и избора хипотезе која је „највероватнија". То је захтев који постављају принципи аналитичко-критичког мишљења. О томе Дејвид Мур (Moore, 2007) пише:

> „Основни елементи мишљења у аналитичко-критичком мишљењу јесу: *циљ* поступка мишљења – зашто истражујемо проблем; *проблем* који се разматра – која се кључна питања постављају; *чињенице* – којим битним подацима располажемо; *закључци и тумачења* – шта

> се може закључити на основу расположивих доказа; *концепти* – које теорије, дефиниције, аксиоми, закони, принципи или модели чине основу за решење проблема истраживања; *претпоставке* – које су претпоставке узете као реалне; *импликације и последице* – шта се дешава, шта се може десити; *друга гледишта* – која друга решења треба размотрити“ (Moore).

Критичко мишљење, претендујући на научност, у истраживању неког проблема пролази кроз следеће фазе: 1) поставити хипотезу; 2) проценити однос већ расположивих информација и новопримљених података; 3) тестирати и оценити хипотезу на основу свих расположивих података и информација и 4) извести логички закључак. Постављање хипотезе је прва фаза у процесу интерпретације. Уобичајено је у раду аналитичких служби да се, на основу расположивих информација, дефинишу две до три могуће хипотезе као прелиминарни одговор на проблем истраживања (Форца и Аночић, 2018).

Хипотезе се тестирају тако што аналитичари сами себи постављају низ логичких питања, те релацијом питање-одговор долазе до исправних закључака: *Зашто бих веровао да је информација битна за проблем, Зашто да верујем да је извор података поуздан,; Да ли моји закључци проистичу из расположивих информација; Имам ли предрасуда по овом питању и како оне утичу на мене; Имам ли предрасуда по овом питању и како оне утичу на мене* и *Да ли су моји закључци логични?* (Форца и Аночић, 2018).

Искусан аналитичар (аналитички тим), који је уз то и поткован знањем, након наведног поступка (релације) питање-одговор приступа фази решавања проблема, користећи логичан след корака: 1) схватање проблема и изналажење ефикасних средстава за његово решење, 2) критичко разматрање претпоставки, предрасуда и карактеристика решења која му се нуде, 3) тумачење података, оцена изведених доказа и процена ставова како би се препознале логичке везе међу предлозима решења; 4) извођење поузданих закључака и уопштавања на основу расположивих доказа; 5) тестирање закључака, стално тражећи контрадикторне ставове који утичу на кредибилитет изнетих тврдњи; 6) спровођење непристрасне расправе о закључцима, која се заснива на чињеницама и 7) разматрање процеса примењеног резоновања ради његове оптимизације убудуће (Форца и Аночић, 2018).

На крају, паметан аналитичар неће никад изнети категоричку тврдњу када се одређује према обавештајном производу који има проценски (предвиђајући) карактер, већ ће увек себи оставити одступницу и имати резерву, рачунајући на могућност да је

погрешно схватио чињенице или да је, што се често дешава, жртва обмане супротстављене стране.

Напослетку долази фаза *доставе обавештјаног производа* или *дисеминације*. Иако се чини да ова фаза нема конкретних додира са обавештајним радом, она је и те како значајна, јер цео обавештајни процес није завршен док политичко и војно руководство не добије потребне информације. Поред тога што треба водити рачуна да информације буду поуздане, оне морају бити и благовремено достављене. Јер уколико обавештајни апарат касни са доставом информација, смањује се или нестаје могућност деловања државе по питањима значајним за националну безбедност. Такође, овакве информације морају бити достављене у разумној и прегледној форми и морају бити повезане са постављеним задатком. Ово није увек једноставно извести с обзиром на мноштво података из јавних и тајних извора. Задатак аналитичара је да од сировог материјала направи корисну информацију уобличену конкретно и јасно. Резултат аналитичког рада могу бити и закључци које је могуће одмах донети на основу расположивих података, али и они закључци до којих се не може одмах доћи.

Конкретни облици у којима се саопштавају резултати активности обавештајне службе су различити и варирају од једне до друге обавештајне службе. Међутим, постоје заједнички и општи елементи. Свакако, најважнији је онај који се односи на материјалну суштину, тј одговор на задатак који је поставио наредбодавац. Како ће он бити саопштен, у којем облику, зависи првенствено од обавештајне службе и начина њеног деловања, односно од циљева које је себи поставила. „Логично је да обавештајне службе великих сила, поготову оних које воде глобалну светску политику, претендују на то да буду обавештене о свему што се дешава не само у посебним регионима него и на целој земаљској кугли. Због тога оне имају више облика саопштавања резултата. У пракси постоји тзв. текуће информисање, периодично или хитно информисање“ (Бошковић, 1996: 129). Док, на пример, ЦИА преседнику САД доставља дневни извештај који садржи све битне информације о дешавањима у целом свету.

У ЦИА се израђује и тзв, извештај о ситуацији. Ти извештаји, како се наводи у литератури, праве се заједничким напорима свих америчких обавештајних служби, на основу свих информација које сви поседују о одређеној области или питању. У њима су садржани и закључци које је могуће одмах донети, али и они до којих се не може одмах

дођи. Бивши шеф ЦИА адмирал Рејборн у једном интервјуу дао је назив за тај извештај и његову дефиницију као: ,,коначна национална обавештајна информација“, под којом је подразумевао информацију чија је тачност проверена и која је допуњена анализом свих расположивих извора. Дакле, сви елементи о истој ствари интегисани су на једном месту“(Бошковић, 1996: 130). Ово указује на потребу да се безбедносна аналитика на националном нивоу интегрише на такав начин да обухвати све различите податке и њихове изворе како војне тако и цивилне у једну целину.

Највиши степен важности у целокупном аналитичком процесу има рад на обавештајној процени. Она се ради као врхунски производ у областима или у вези с проблемима о којима нема познатих конкретних података, а ипак су нужни одговарајући закључци и процене, на пример будућег развоја догађаја или предвиђања шта ће се десити у непосредној будућности. За то се ангажује комплетан научноистраживачки и аналитички потенцијал обавештајне службе, који покушава да пружи слику о стварима које се не могу установити на основу конкретних критеријума. У том подручју обавештајна служба често ,,пада на испиту“, јер то није наука и не постоје емпиријске методе помоћу којих би се унапред предвидело понашање неке владе или неког појединца (Бошковић, 1996).

,,Стратегијска информација, дакле, садржи елементе који могу да узрокују измену формираних сазнања на стратегијском нивоу, а тиме и непосредну промену политике и политичких одлука. У њеном средишту су обрађена значајна питања од чијег решења или убрзавања у једном или другом смеру зависи и крајњи успех (или неуспех) оружаних снага или друштвене политике у целини. За добру, правовремену и са свих аспеката обрађену информацију која има стратегијски значај може се фигуративно рећи да ‚поплочава пут ка остварењу главног задатка’, односно ка постизању дефинитивног успеха земље која води рат“(Бошковић, 1996: 133).

Напослетку, треба поменути и такозвану повратну информацију. То је обавештење од претпостављеног, био он политички лидер, војни командант или директор производне или финансијске корпорације, о утицају добијене информације на одлуку коју је донео или ће донети. Сазнање да је обавештајна информација била корисна (у најширем значењу тог појма) или да је, с друге стране, ‚потпуно промашила тему’, врло је битно за даљи рад и усмеравање како прикупљачких тако и капацитета за израду обавештајних производа“,

наводи бивши начелник Обавештајне управе Генералштаба Бранислав Аночић (Форца и Аночић, 2018).

2.2 Криминалистичка аналитика

У савременом облику, криминалистичко-обавештајна аналитика се примењује тек од осамдесетих година 20. века, коришћењем компјутерских технологија је доживела свој врхунац у великом броју земаља света. Развој обавештајног рада у полицији, у данашњем облику, најчешће се везује за Велику Британију. Тако и национални обавештајни модел Велике Британије ближе одређује циљеве обавештајно вођеног полицијског рада на основу четири кључна аспекта:

- усмеравање полицијског рада пре свега на учиниоце кривичних дела, а нарочито на активне криминалце, коришћењем и јавних и тајних метода,
- контролисање кризних места за криминал и општи јавни ред,
- истрага повезаних серија кривичних дела и других инцидената и
- примена превентивних мера, укључујући и сарадњу са локалним интересним групама да би се смањила укупна количина криминала и јавног нереда (Ratcliffe, 2013).

До озбиљног заокрета и унапређења рада обавештајних служби, али и полиције, дошло је након 11. септембра 2001. године, то јест након терористичког напада у САД. У анализама рада свих субјеката безбедности у Северној Америци које су уследиле након овог напада дошло се до закључка да обавештајни систем није добар и да се напад могао спречити да су се информације између различитих служби размењивале. На пример, одређене службе су имале информације о обуци у управљању летелицама многих исламских припадника, друге о илегалној набавци материјала који се могу искористити у прављењу бомби и слично. Међусобном разменом информација и њиховим укрштањем (аналитиком) могло се доћи до сазнања о потенцијалној претњи на коју се могло правовремено реаговати.

Радомир Милашиновић наводи да обавештајна служба би била делатност одређених органа државе који имају задатак да прикупљају и изучавају податке економског, политичког и војног карактера о активном или вероватном непријатељу у циљу обезбеђења мера владе које ће осигурати безбедност државе (Савић, 2012).

Према Савићу (2012), постоје различите организационе целине обавештајних служби, а најважније међу њима су:

- јединица за оперативне послове,
- јединица за аналитичке послове,

- јединица за документацију,
- јединица за техничке послове,
- јединица за послове веза и
- јединица за кадровске послове (Исто).

„Јединица за аналитичке послове врши селекцију, обраду, анализу и завршну процену прикупљених података на нижим нивоима и израђује обавештајна документа која се преко централе презентују корисницима. Делатност наведене јединице се најчешће одвија у три смера:

- израда текућих извештаја, проблемских информација и процена,
- апострофирање пропуста и позитивних искустава обавештајне праксе и
- дефинисање нових захтева према организаторима и извршиоцима обавештајних истраживања“ (Савић, 2012: 71).

„Потребно је направити разлику између обавештајног и криминалистичко-обавештајног рада. Обавештајни рад, који се по правилу примењује према држављанима или органима других држава, одвија се ван законских оквира и правне регулативе, што се не може рећи за криминалистичко-обавештајни рад, који се примењује углавном према лицима на сопственој територији и субјектима који могу деловати на прекограничној основи и који су повезани са организованим криминалитетом, тероризмом или другим тешким кривичним делима, а све у складу са домаћим и међународним законодавством“ (Фатић, 2009: 5).

Обавештајне службе су углавном усмерене ка спољашњим факторима ризика и оперишу изван државе, док контраобавештајне службе имају задатак спречавања деловања страних обавештајних служби на сопственом терену. Међутим, оно што им је заједничко јесте тајност у раду и чување података везаних за различите задатке далеко од јавности, док су посао полиције и криминалистичко-истражне радње далеко транспарентнији. Под обавештајним радом се може схватити рад припадника обавештајних служби (безбедносно-обавештајних служби) као што су: БИА, ВБА и ВОА, а под криминалистичко-обавештајном делатношћу подразумева се рад служби у оквиру Министарства унутрашњих послова (организационе јединице за борбу против организованог криминала, тероризма, ратних злочина, за спровођење посебних доказних радњи итд.). Такође, обавештајне делатности су блиско повезане са војним, политичким и економским циљевима, те се оне не могу самостално посматрати, нити изоловано од политичке воље државе којој припадају.

„Криминалистичко-обавештајна аналитика представља систем који омогућава коришћење прикупљених података у криминалистичким обрадама на начин да се предупреде будуће криминалне појаве и разреше постојећа кривична дела. Подаци који су прошли процес анализе могу се користити као подршка у одлучивању и реализацији конкретних операција“ (Gottlieb et al., 1994: 11). Крајња сврха криминалистичко-обавештајне делатности је прикупљање, систематизација, квалификовање информација тако да оне буду подобне за даљу обраду, која ће довести до одговора на конкретно питање.

Међу најраспрострањеније врсте аналитике (условно безбедносне аналитике) у појединим државама, али и организацијама (ЕУ, ОЕБС) спада криминалистичко-обавештајна аналитика, која се најчешће именује само као криминалистичка анализа. Како сам назив упућује, реч је о делатности у сфери криминалитета, којом се примарно баве полиција и судство. Међутим, ова врста аналитике није једнозначно дефинисана и операционализована. Тако, кад је сам назив у питању, срећемо изразе: криминалистичко-обавештајни рад (КОР), криминалистичко-обавештајна делатност (КОД), криминалистичко-обавештајна аналитика (КОА), криминалистичка аналитика (КАн) и криминалистичка анализа (КАл).

Упоредо са термином криминалистичко-обавештајна аналитика користи се и термин криминалистичко-оперативна аналитика, који је уједно и заступљенији у домаћој полицији. Криминалистичко-оперативна аналитика је делатност обједињавања, прегледа, анализирања прикупљених информација и изналажења кључних чињеница у вези са разним облицима и видовима криминалних активности (МУП Србије, 2009).

„Криминалистичко-обавештајна аналитика је један од сегмената криминалистичке аналитике која, иначе, обухвата четири сегмента: аналитику криминала (crime analysis), истражну аналитику или профилисање (investigative analysis or profiling), аналитику делатности (operational analysis) и криминалистичко-обавештајну аналитику (intelligence analysis)“ (Копал и сар., 2003: 7).

„Криминалистичко-аналитичко истраживање је логички и технички систем менталних и других пратећих криминалистичко-аналитичких активности (радњи) којима се применом криминалистичко-аналитичких метода препознају, проверавају и верификују

већ постојећа или стичу нова криминалистичко-аналитичка сазнања“ (Манојловић, 2008: 73).

„Криминалистичко-аналитичке методе су оне методе које су применљиве на различите врсте полицијских, судских и криминалистичких истрага. Ове методе се користе са циљем расветљавања кривичних дела. Полазна основа за примену криминалистичко-аналитичких метода је криминалистички процес. Криминалистичко-аналитички процес подразумева серију активности или процедура које воде ка најпрецизнијим и највалиднијим закључцима који се могу добити из информација којима располажемо. У наведени појам спадају: прикупљање података, процена података, упоређивање, индексирање података, интеграција и тумачење података и други „(Манојловић, 2008: 213).

Производ криминалистичко-аналитичког процеса назива се криминалистичко-аналитички податак, који по својој природи може бити општи и посебан. Општи криминалистичко-аналитички податак обухвата шири сет криминалних активности, што је својствено мањим полицијским јединицама или надлежностима, док се посебан криминалистичко-аналитички податак усредсређује на специфичан тип криминалне делатности, као што су: тероризам, преваре, организовано криминално деловање и слично. Постоји стратешка и тактичка примена криминалистичко-аналитичког податка. „Стратешки криминалистичко-аналитички податак примењује се у дужим роковима са задацима и циљевима попут: идентификације најважнијих криминалних организација и појединаца, пројекција типова криминалних делатности, утврђивање приоритета и слично. Тактички криминалистичко-аналитички податак употребљава се према актуелном случају или објекту, са тренутним утицајем на криминалну делатност“ (Тодоровић-Радовановић, 2015: 54).

2.2.1 Intelligence-led policing и његова примена у страним државама, ОЕБС и ЕУ

У савременим условима примене криминалистичке аналитике, најчешће је у употреби шири и општи израз „обавештајно вођен полицијски рад“, као превод синтагме из енглеског језика: *Intelligence-led policing* (ILP), чији је аналитика/анализа само један део (корак, фаза). У даљем тексту управо ћемо се осврнути на страна и домаћа решења тог ширег аспекта организовања и рада полиције – *Intelligence-led policing.* „Полицијски рад,

под вођством обавештајних информација, представља модел борбе против криминала који се базира на ефективном прикупљању и анализи информација, који има потенцијал да буде најважније средство за органе безбедности у 21. веку“ (Kelling & Bratton, 2006: 5).

Традиционални модел организовања за остваривање безбедности у држави (Standard model of policing) се базирао на репресији, односно деловању надлежних органа тек након сазнања за извршење кривичног дела које се углавном дешава по пријави оштећеног. Овај модел је критикован јер је реакција надлежних органа изостајала све док не наступи штета. Није постојао систематизован и организован начин деловања на безбедносно интересантним локацијама и према безбедносно интересантним лицима. Дакле, у традиционалном моделу полиција је деловала скоро искључиво реактивно, то јест деловала је тек након избијања инцидентних ситуација.

„Кључне недостатке традиционалног приступа сузбијању криминалитета превазишао је нови модел „рад полиције у локалној заједници“ (Community-oriented policing). Код нас је овај модел познатији као „полиција у заједници“ и подразумева поред позорничке и патролне делатности и бољи, срдачнији однос и интензивнију комуникацију са локалним становништвом. Успостављањем поверења и отворених канала за комуникацију између заједнице и полиције довешће до позитивних ставова грађана о целокупној безбедносној ситуацији. На основу предлога грађана биће много лакше организовати и усмерити рад полиције ка отклањању субјекта угрожавања безбедности. Програм рада у локалној заједници обухвата састанке са представницима група из заједнице и отворену дискусију о свим проблемима“ (Иветић, 2017: 133-140). Полиција у заједници је заправо превентивни модел који има двоструке ефекте. Први је прикупљање информација од грађана, на пример, о трговини наркотицима, лицима која могу бити безбедносно интересантна, корупцији и слично, док је други стварање већег поверења грађана у сопствени систем безбедности.

„Даље, постоји рад полиције заснован на рачунарској статистици (CompStat – compare stats – компаративна статистика). То је модел управљачке одговорности који користи рачунарску аналитику виших (руководећих) службених лица у циљу да се спроведу у дело замисли нижих службених лица. Нижа (извршилачка) службена лица обављањем свакодневних активности у заједници прикупљају информације о стању безбедности и достављају их руководиоцима на даље одлучивање, који на основу њих одређују безбедносно интересантне локације и лица захваљујући криминалистичкој

аналитици која, додуше, није иста као што је то случај у полицијско-обавештајном моделу“ (Habbib, 2011: 6-11).

Ово је савремени модел који настаје касније, што значи да се овакав модел рада не базира само на репресији и реаговању на учињено кривично дело, већ се односи и на проактивно и превентивно деловање. Подаци се чувају у посебној системској књизи (COMPSTAT book), која се односи на одређено временско раздобље и анализирају је посебне службе (аналитике). Осим прикупљања и обраде, битан корак је и размена информација са другим органима безбедности, па је неопходно успостављање сарадње између Министарства унутрашњих послова и других органа безбедности, најбоље кроз јединствене базе података.

Intelligence-led policing представља савремени криминалистичко-обавештајни модел који је у основи пословни модел руковођења који се базира на прикупљању података и њиховој анализи како би се створио адекватан оквир за одлучивање руководиоца у првацу смањења криминалитета, предузимања акција према спровођењу мера према учиниоцима кривичних дела и спровођења стратегија и планова.

Основни разлози прибегавања савременим криминалистичко-обавештајним моделима су у томе што модели засновани на репресији нису дали адекватне резултате у борби против криминалитета, напротив, дошло је до његовог пораста. Такође, савремене технологије донеле су напредак у прикупљању и обради великог броја података, што је за последицу имало и унапређење рада органа безбедности. И као трећи кључни разлог за прелазак на савремене моделе полицијског рада, често се наводи отварање граница и међународно повезивање које није само омогућило промет роба и услуга међу државама већ и међу криминалцима. Као одговор на ове новонастале услове развијен је Intelligence-led policing модел као проактивни модел насупрот традиционалним реактивним моделима.

Идентификовање снага и слабости у примени проактивних модела рада, као што су Compstat и „рад полиције у заједници“, допринело је доношењу закључака и препорука за унапређење проактивних модела рада, што је представљало довољан основ за успостављање полицијско-обавештајног модела (OSCE, 2017).

„У светској научној литератури постоје многобројне дефиниције полицијско-обавештајног модела које указују на то да је реч о менаџерској филозофији, чији је циљ доношење одлука о организовању полицијских послова на основу релевантних, потпуних,

правовремених и употребљивих информација о криминалитету“ (Томашевић и Рацић, 2019: 85). Ипак, у научној литератури најчешће се наводи Ретклифова дефиниција полицијско-обавештајног модела: „Пословни модел и менаџерска филозофија, где су анализа података и информације о криминалитету од главног значаја за објективан оквир за доношење одлука који омогућава смањење криминалитета и проблема, превенцију кроз стратешки менаџмент и ефективно спровођење стратегија који су усмерени на озбиљне преступнике” (Ratclife, 2008: 85).

„Суштина дефинисања полицијско-обавештајног модела лежи у три кључна елемента, а то су: менаџерска филозофија, обрада података (аналитика) и проактиван приступ полицијским пословима. То је модел који на објективан начин формулише стратешке приоритете за рад полиције, као основу за алокацију полицијских ресурса, усмеравање истражних активности према учиниоцима који представљају највећу друштвену опасност и просторима са највећом стопом криминалитета. Суштина је да полицијско-обавештајни модел, односно прикупљени и анализирани подаци послуже као основа за оперативан рад, а не да оперативни рад дефинише захтев за прикупљање оперативних (обавештајних) података. У анализи изазова у супротстављању криминалитету указује се на проблеме криминалитета који је регистровала полиција, броја покренутих судских поступака и донетих осуђујућих пресуда. Осим тога, као посебно важан предмет анализе присутни су повратници и места где се извршава највећи број кривичних дела (жаришне тачке)“ (Рацић, 2023: 34). Полицијско-обавештајни модел захтева од полиције да успостави низ партнерстава са актерима који нису државни органи, али могу допринети протоку података попут невладиних организација, грађана, волонтера, припадника приватног обезбеђења и слично.

„Може се закључити да анализа представља кључну улогу за обавештајни рад у оквиру полицијске организације. Управо, криминалистичко-обавештајни процес започиње подношењем захтева за израду криминалистичко-обавештајне информације и завршава се њеним достављањем стратешкој групи и оперативној групи. На основу криминалистичко-обавештајне информације доносе се адекватне одлуке које треба да усмере даљи оперативни рад“ (Рацић, 2023: 35).

Паретов принцип, као специфична техника за одређивање приоритета приликом решавања проблема указује на изузетан значај проактивног приступа у спречавању и

сузбијању криминалитета. Према том принципу, 20% извршилаца изврши 80% кривичних дела, што подразумева да се идентификацијом тих 20% извршилаца и усмеравањем полицијског рада на спречавање њихове криминалне делатности може спречити значајан број кривичних дела (Стевановић, 2019).

„ILP се фокусира на систематско прикупљање и евалуацију података и информација кроз дефинисани процес анализе, претварајући их у стратешке и оперативне аналитичке производе, који служе као основа за побољшано, информисано и доношење одлука засновано на доказима“ (OSCE, 2017: 6). Дакле, овај модел дефинише приоритете засноване на обавештајним подацима. И поред супротстављања организованом криминалу, овај модел се показао и као ефикасан у борби против тероризма и екстремизма који може водити у тероризам.

„Иако су се горенаведени примери ILP фокусирали само на традиционални улични злочин, а посебно на криминал са оружјем, верује се да постоји велики потенцијал у коришћењу ILP модела за одговор на тероризам. Хапшења након лондонског метроа и бомбашких напада на воз у Мадриду, на пример, сугеришу да су обавештајни подаци прикупљени из више извора, укључујући надзорне камере, доушнике из заједнице и затворске службенике били инструментални у истрагама након догађаја. Хапшења осумњичених терориста у Сједињеним Државама (Флорида), Канади и Британији сугеришу да би обавештајци могли да идентификују терористичке групе и омогуће интервенцију пре напада. Ово је у складу са извештајима земаља као што је Израел, са дугим искуством у борби против тероризма“ (McGarrell et al. 2007: 147).

Чињеница да су насилни екстремисти у вези са недавним терористичким инцидентима, укључујући вукове самотњаке, остали испод радара за спровођење закона, позвала је на проактиван приступ и истакла потребу за свеобухватним дељењем и централизованом анализом релевантних података и информација. Схватање да се терористички напад и рано откривање других озбиљних инцидената не могу решити на реактиван начин ставило је ILP у центар пажње на међународној сцени за спровођење закона. Ово је било очигледно након напада 11. септембра, што се одразило у налазима САД. Комисија од 11. септембра је закључила да су постојале различите информације на различитим нивоима пре напада, али због пропуста агенција да их поделе нису могле да се координирају како би пружиле свеобухватну слику (OSCE, 2017).

„Примена полицијско-обавештајног модела је с временом еволуирала, тако што су га у пракси полицијске организације прилагођавале и развијале сходно својим потребама, због чега у савременим условима не постоји његова јединствена стандардизована форма. Упркос томе, суштина његове примене у раду полиције остала је непромењена, тако да подразумева подршку у доношењу одлука стратешких и оперативних управљачких група, кроз обједињене обавештајне функције и базе података из више различитих организационих јединица полиције, што доприноси усмеравању ресурса на приоритете дефинисане у стратешким и оперативним плановима“ (Томашевић и Рацић, 2019: 85).

„Применом полицијско-обавештајног модела полицијски послови се надограђују недостајућим елементима, као што су: прикупљање, обрада и анализа података, израда криминалистичко-обавештајних информација, доношење одлука и планова и њихово спровођење које укључује координацију, контролу и управљање квалитетом. Према томе, полицијски послови се усмеравају на: стратешки приступ, чији је циљ сузбијање криминалитета, координацију рада свих полицијских службеника (униформисаних и криминалистичке полиције), успостављање равнотеже, нарочито у реактивном и проактивном поступању; планирање оперативних акција усмерених на вишеструке извршиоце најтежих кривичних дела који изазивају узнемирење јавности и инкорпорирање проактивног рада као саставног дела стратегије за контролу криминалитета“ (Ђурђевић и Радовић, 2017: 447).

ILP омогућава напредан и проактиван приступ управљању полицијом. Његова успешна примена последњих година у великом броју земаља широм света за решавање озбиљних злочина и транснационалних претњи подстакла је развој концепта ILP од тога да се углавном примењује на борбу против организованог криминала до општијег стратешког пословног модела за решавање широко разноврсних полицијских проблема на локалном, регионалном и националном нивоу. Овај развој је директно повезан са тражењем метода за спровођење закона који би омогућили полицији да има већи утицај на криминал, развој криминала и друштвену штету од криминала са ограниченим ресурсима и у временима повећане потражње за одговорношћу (OSCE, 2017:). С обзиром на то да се полицијско-обавештајни модел константно развија, потребно је анализирати искуства различитих земаља у примени овог модела како би се стекао бољи увид у суштину његове примене.

„Терминолошки, за исти појам користе се различити називи у зависности од земље која је модел имплементирала. Већина држава, као што су: Сједињене Америчке Државе, Немачка, Шведска, Холандија, Аустралија, Канада користи назив Intelligence-led policing, за разлику од Велике Британије, која за означавање истог појма користи назив Национални – обавештајни модел. Синтагма појма Intelligence-led policing у српском законодавсту се користи под називом *полицијско-обавештајни модел"* (Марковић, 2019: 172).

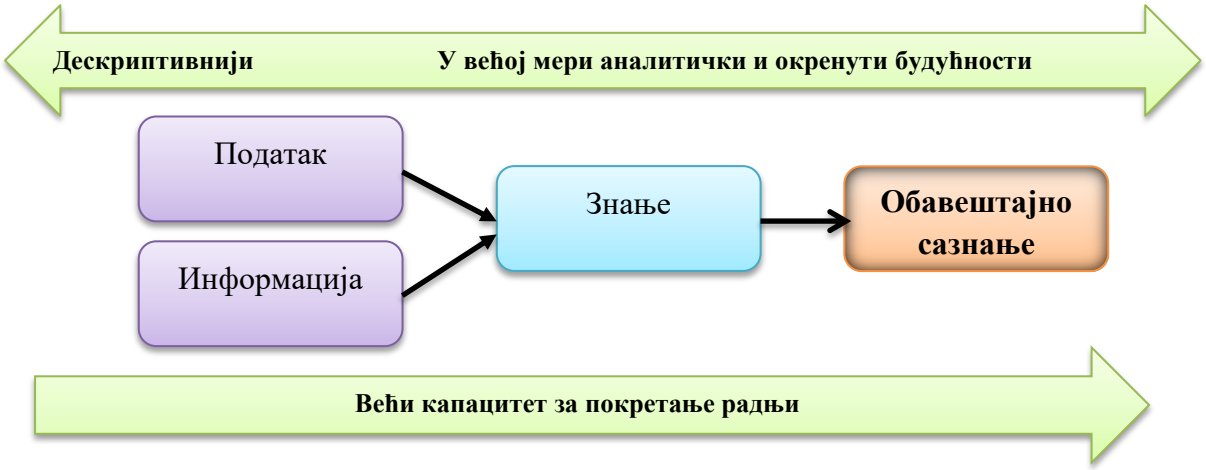
2.2.1.1 Приступ ОЕБС-а

Према подацима ОЕБС-а, истраживачи и литература о спровођењу закона најчешће деле методологије спровођења закона на пет модела рада полиције: 1) традиционални рад полиције, 2) рад полиције оријентисан ка заједници, 3) проблемски оријентисан рад полиције; 4) рад полиције заснован на рачунарској статистици (CompStat) и 5) рад полиције заснован на обавештајним сазнањима (Intelligence-ed policing). У новије време све више је у жижи управо ILP (OSCE, 2017: 18).

Као што нема јединственог превода енглеског термина *intelligence,* тако је проблем и у преводу синтагме *Intelligence-led policing.* Тако, срећемо следеће преводе: обавештајно вођен полицијски рад, рад полиције заснован на обавештајним информацијама и рад полиције заснован на полицијским знањима. Такође, и по питању времена и места настанка ILP различити су ставови у теорији. По једним виђењима, ILP датира од почетка 20. века и везује се за полицију Њујорка (САД) (Манојловић, 2008). По другима, ILP се почиње развијати у Великој Британији скраја прошлог и почетком овог века.

„Да би учврстили позицију свог превода за ILP као рад полиције заснован на обавештајним сазнањима, у ОЕБС-у су извели основне појмове (Слика 9) који имају следећа значења:

- *Подаци* су сирова и нерастумачена запажања и мерења. Примери су одлике криминалне активности које је лако квантификовати, као што су пријаве кривичних дела и друга статистика криминала, базе података о починиоцима и полицијска задужења.
- *Информација* је податак стављен у контекст и оснажен значењем, чиме добија већу релевантност и сврху.
- *Знање је информација* којој су дати тумачење и разумевање. Када особа информацији дода своју мудрост, она постаје знање.
- *Обавештајна сазнања* су подаци, информације и сазнања који су оцењени, анализирани и представљени у формату за одлучивање за потребе деловања" (OSCE, 2017: 19).



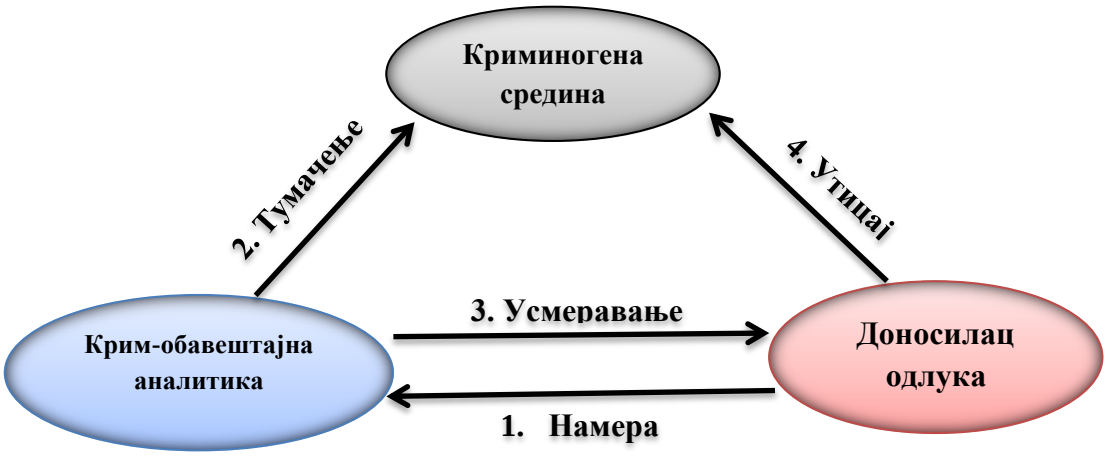
Слика 9. *Од податка до обавештајног сазнања*

Извор: *Ратклиф, 2016: 72*

Посебан проблем се појавио у покушајима да се ILP дефинише. Док неки сматрају да се ILP односи на обављање процена претњи, други тврде да се односи на процес прикупљања података и информација. У том смислу, у Приручнику ОЕБС-а се полази од Ратклифовог тумачења ILP, јер се тај теоретичар из САД сматра и његовим теоријским творцем и најчешће цитираним аутором. Ратклиф (2017) за ILP каже:

> „Рад полиције заснован на обавештајним сазнањима наглашава анализу и обавештајна сазнања као кључне елементе објективног оквира одлучивања у којем се приоритет придаје жариштима криминала, жртвама поновљених кривичних дела и врло активним преступницима и криминалним групама. Он олакшава смањење, заустављање и спречавање криминала и штете кроз стратешко и тактичко управљање, распоређивање и провођење“.

У приказу суштине ILPкористи се почетни модел „3-i“, који је успоставио Ратклиф, а који је касније еволуирао у „4-i“ (Слика 10). Претходни „3-i“ модел није садржао први корак – *intent* (*намера)*, који је касније додат.



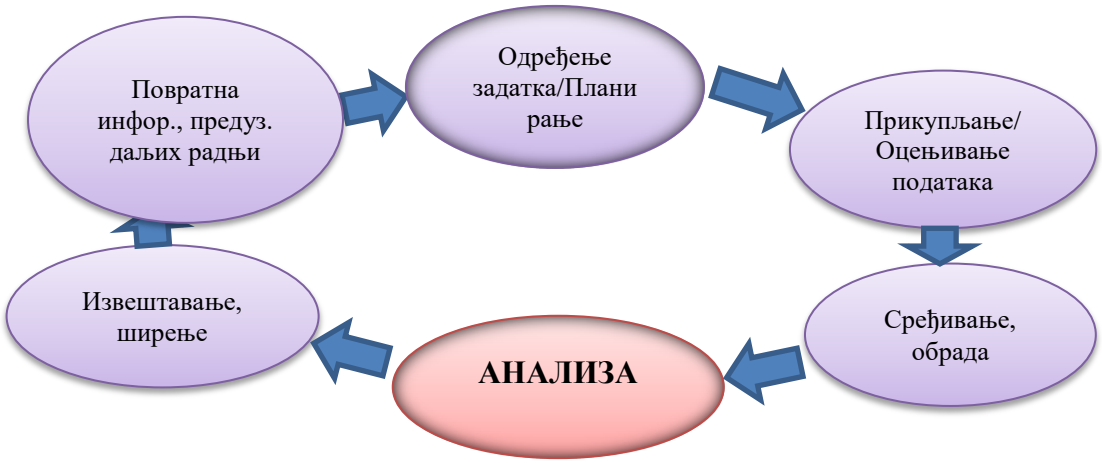
Слика 10. *Модел „4-i“: intent (намера), interpret (тумачење), influence (усмеравање) и impact (утицај)*

Извор: *Ратклиф, 2016: 83*

Модел „*4-i*“: *intent* (намера), *interpret* (тумачење), *influence* (усмеравање) и *impact* (утицај) помаже у објашњавању улога и односа међу кључним актерима у концепту ILP: криминогене средине, криминалистичко-обавештајног аналитичара и доносиоца одлука у полицији. Све четири компоненте на „i“ морају се примењивати и правилно функционисати да би модел ILP могао остварити свој пун потенцијал. Овај модел ставља нагласак на однос између анализе криминала и доносилаца одлука. Доносиоци одлука (руководиоци) одређују задатке, усмеравају рад, саветују и воде криминалистичко-обавештајне аналитичаре. **Прво**, доносиоци одлука морају објаснити своје намере и да се увере да су правилно схваћене. **Друго**, аналитичари тумаче криминогену средину и **треће,** они усмеравају доносиоце одлука налазима анализе. На основу тих налаза, доносиоци одлука (**четврто**) утичу на криминогену средину путем стратешког управљања, акционих планова истрага и операција.

Процес прикупљања обавештајних сазнања – *криминалистичко-обавештајни процес*, који се традиционално назива *обавештајним циклусом*, описује и одређује шест општеприхваћених стандардних корака помоћу којих се сирови подаци и информације претварају у обавештајна сазнања с додатом вредношћу намењена деловању. У идеалном случају овај процес започиње *одлуком или одређивањем задатка*, након чега следи *фаза планирања*, после које аналитичари прелазе на *прикупљање информација и података* који се морају оценити на основу формално признатог система оцењивања („4 x 4“, „5 x 5“, „6 x 6“). Следећи корак је фаза у којој се, заправо, врши *обрада*, која почиње сређивањем и структурирањем доступних података и информација и њиховим уносом у базу података. Подаци и информације се затим *анализирају* – (аналитика**)**, што резултује *израдом обавештајног производа који се доставља клијенту* (руководиоцу, истраживачу или другима који одређују задатак аналитичарима или захтевају њихову аналитичку подршку) и другим релевантним актерима. Клијент оцењује обавештајни производ у складу са својим потребама и захтевима. Добијене *повратне информације* користе се за унапређење постојећег производа или као улазни методолошки елементи за будуће сличне производе.

Обавештајни циклус није статички низ шест корака, већ динамички процес у којем су различите фазе међусобно тесно повезане и претачу се једна у другу, због чега аналитичари морају радити на различитим елементима обавештајног циклуса. Циклус приказан на Слици 11 предвиђа уређену и лако разумљиву структуру и процес и може се користити као основни процес како у стратешкој тако и у оперативној анализи.



Слика. 11 *Криминалистичко-обавештајни циклус*

Извор: Приручник ОЕБС-а: *Рад полиције заснован на обавештајним сазнањима, 2017: 35*

Анализа – аналитика је најбитнија фаза криминалистичко-обавештајног циклуса. Као што је случај и с различитим врстама обавештајних информација, за класификацију анализе користе се различити изрази. Оно што је у једној организацији *оперативна анализа,* у другој се назива *тактичком анализом*, а оно што једна полицијска служба назива *мрежном анализом,* у суседној земљи се назива *анализом веза* или *мапирањем веза.* Најчешће класификације анализе су *стратешка анализа, оперативна анализа* и *тактичка анализа.* У Приручнику ОЕБС-а о ILP су тактичка и оперативна анализа сврстане заједно под оперативну анализу.

Стратешка анализа подржава доношење одлука, креирање политике, планирање и одређивање приоритета и расподелу полицијских ресурса и одређује одговарајући приступ за решавање проблема с различитим врстама криминала. Она, такође, пружа обавештајним сазнањима вођену подршку спровођењу закона на терену тако што олакшава идентификовање кључних претњи, угрожености, ризика и прилика за деловање

(процене претњи и ризика). Стратешка анализа не обухвата личне информације (OSCE, 2017).

Оперативна анализа помаже у управљању и спровођењу краткорочнијих задатака на терену ради остваривања оперативних циљева и подржава текуће истраге. Оперативна анализа може обухватити личне информације о осумњиченима (OSCE, 2017).

Фаза *анализе* је у центру обавештајног процеса зато што се бави одређивањем и сагледавањем значења, контекста и основних одлика доступних информација. Анализа података скреће пажњу на недостајуће информације и снаге и слабости података, те одређује даље кораке. Главни циљ фазе анализе је проналажење значења у првобитним информацијама да би се обавештајна сазнања могла практично искористити. Када су резултати криминалистичко-обавештајне анализе непосредно повезани и одговарају утврђеном задатку/проблему који се истражује, анализа постаје драгоцена као оперативно средство.

Аналитички процес се састоји из две фазе – *интеграција података* и *тумачење података.* **Прва фаза** (интеграција података) комбинује оцењене (4 x 4 или 5 x 5) и сређене информације из различитих извора ради израде иницијалних хипотеза и предвиђања, идентификовања обавештајних образаца и извлачења закључака. **Друга фаза** (тумачење података) подразумева залажење иза доступних података и њихово тумачење. У овој фази се тестирају иницијалне хипотезе, што за резултат има подржавање, модификовање или оспоравање претходно развијених хипотеза (OSCE, 2017).

Хипотеза је оквирна радна теорија заснована на претходно израђеним показатељима и премисама извученим из расположивих података и информација, која захтева додатне информације да би се потврдиле или оспориле претходне претпоставке. Хипотезе помажу у идентификовању обавештајних јазова, фокусирању на даље прикупљање и извођњу тачних закључака, предвиђања и процена.

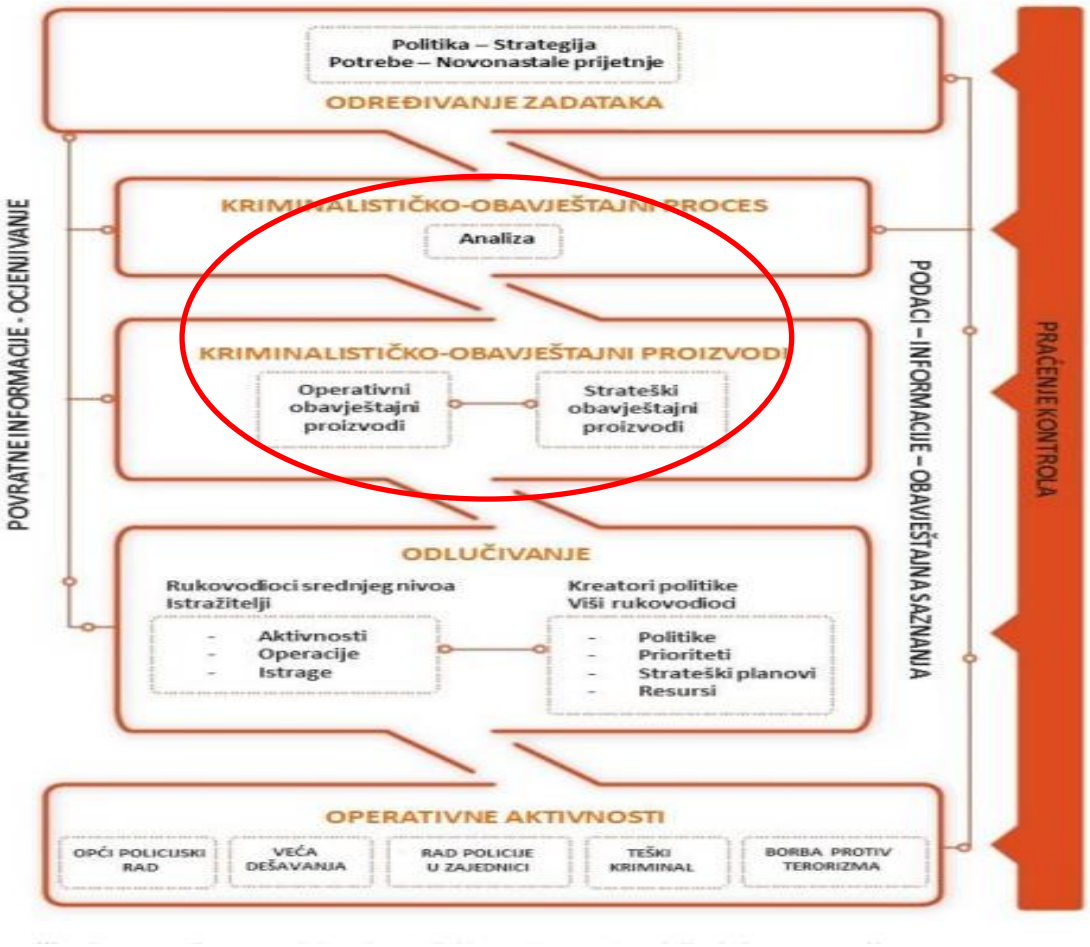
Развој и тестирање хипотеза добија на значају у оквиру обавештајне анализе. Хипотезе садрже велику количину спекулација и стога их аналитичари морају тестирати (потврдити, модификовати или одбацити). Тестирање хипотеза требало би да обухвати: аргументе у прилог и против хипотезе, њене импликације, преглед поступка размишљања и прикупљање и ревидирање потребних података. Хипотеза или било који изведени закључак треба садржавати одговоре на следећа кључна питања (која се често називају „5W и 1X“):

- Ко? Кључни појединац/појединци
- Шта? Криминалне активности
- Како? Методи који се користе
- Где? Географске информације и обухват
- Зашто? Мотив
- Када? Временски оквир (OSCE, 2017).

На пример, Национални обавештајни модел (NIM) *Канцеларије Уједињених нација за дрогу и криминал* (UNODC) изведен је из девет аналитичких техника и производа, који поткрепљују информисано, стратешко и/или оперативно одлучивање и развој професионалног познавања делотворних, проактивних техника спровођења закона:

- **анализа образаца криминала** је широк појам за низ типова анализе, укључујући и идентификовање трендова и анализу жаришта,
- **анализа демографских/друштвених трендова** процењује утицај друштвено-економских и демографских промена на криминалитет, као и промене у популацији и бескућништво,
- **анализа мрежа** процењује правац, учесталост и јачину веза међу учесницима у криминалној мрежи;
- **профили тржишта** процењују криминално тржиште за одређену робу, као што су дроге или проституција;
- **криминални пословни профил** одређује пословни модел и технике које користе преступници или организоване криминалне групе;
- **анализа ризика** процењује размере ризика или претњи које преступници или организације представљају за појединачне потенцијалне жртве, полицију и јавност;
- **анализа циљног профила** описује криминалца, његове снаге и слабости, животни стил, мреже, криминалне активности и могуће тачке пресретања у животу циљаног преступника;
- **оперативна обавештајна процена** оцењује да ли је прикупљање информација у складу с претходно договореним циљевима и идентификује пукотине у обавештајном раду операције (користи се у масовним пројектима и операцијама);
- **анализа резултата** оцењује делотворност активности спровођења закона и прати напредовање планова.

ОЕБС-ов модел ILP који се примењује у пракси приказан је на Слици 12. Модел је сачинило *Одељење за стратешка полицијска питања Сектора за транснационалне претње ОЕБС-а*, на основу Ратклифових (2016) дефиниција. У изради графикона такође је коришћен и приказ протока информација дат у документу *UNODC-a Police Information and Intelligence Systems* (2006).



Слика 12. *ОЕБС-ов модел рада полиције вођеног обавештајним сазнањима*

Извор: Приручник ОЕБС-а: *Рад полиције заснован на обавештајним сазнањима, 2017: 49*

На претходној Слици приказан је целокупан рад полиције, који се се заснива на обавештајним сазнањима, како га виде експерти ОЕБС-а. То је један непрекидан циклус у коме је крим-аналитика (анализа!) само један његов део (фаза). Тако, крим-обавештајна анализа (сазнања) јесте полазна основа за доносиоце одлука у систему безбедности и спровођење оперативних активности у свим областима криминалитета.

2.2.1.2 Уједињено краљевство (национални обавештајни модел)

У теорији постоје бројни извори у којима се сматра да је у данашњем, модерном облику криминалистичко-обавештајни рад заживео у Енглеској, где је 1992. године основана *Национална криминалистичко-обавештајна служба* (National Criminal

Intelligence Service – NCIS). На регионалном нивоу служба је имала своје јединице за координацију прикупљања података и израде различитих анализа. Већу тежину су добили подаци из јавних извора, а такође се модернизовао систем рада с информаторима. У почетку није био проактивно усмерен, његов мото је био „intelligence is information designet for action“ (Дворшек, 2023: 4), што би у преводу значило: „обавештајне информације намењене акцији“. С обзиром на то да је криминалистичка аналитика у полицији већ имала традицију, криминалистички обавештајни рад третирао се само као побољшана варијанта криминалистичке аналитике.

Средином деведесетих година 20. века почеле су јачати иницијативе за проактивно полицијско деловање. То је, између осталог, подразумевало предвиђање криминалних активности у будућности. Да би то било могуће било је потребно прибавити што више корисних информација из криминалног подземља, а што је било могуће једино уз повећање криминалистичко-обавештајне делатности. Преиспитивање стратегије полицијског рада које је уследило, пре свега на основу извештаја Ревизорске комисије за ефикасност полиције из 1993. године, довело је до преиспитивања методолошког фокуса карактеристичног за реактивни полицијски рад, а то је готово искључиво фокус на кривична дела, уместо на починиоце. Последица наведених активности била је та да је у Енглеској оформљен *Национални криминалистичко-обавештајни модел* (*National Intelligence Model – NIM*), који се протезао на свим нивоима: локалним, регионалним, прекограничним, међународним; тешке случајеве криминалитета; организовани криминалитет. Наиме, Закон о реформи полиције из 2002. био је законска основа за успостављање Националног обавештајног модела у свим областима рада полиције.

„Национални обавештајни модел је први пут „пилотирала“ у Енглеској и Велсу 2000. године Национална обавештајна служба за криминал, а спонзорисало га је Удружење главних полицијских службеника. Владин први Национални план полиције, који покрива период 2003-2006, захтевао је да све 43 полицијске снаге у Енглеској и Велсу усвоје NIM (и буду у складу са његовим процедурама) до априла 2004. Модел стога представља оно што је у Британији необично одлучан покушај из „центра“ да стандардизује полицијску праксу и, заиста, да се то уради око одређене полицијске парадигме – полиција вођена обавештајним подацима“ (Maguire & John, 2006: 5).

Намера иза NIM-а је да се фокусира на оперативни рад полиције и да се постигне несразмерно већи утицај из расположивих ресурса. Заснован је на јасном оквиру анализе података и информација, омогућавајући приступ решавању проблема спровођењу закона и техникама превенције криминала. Очекивани резултати су побољшана безбедност заједнице, смањење криминала и контрола криминалитета и нереда који води ка већем уверавању јавности и самопоуздање. NIM није ограничен на употребу стручњака. Релевантно је за све области спровођења закона: криминал и његова истрага, неред и безбедност заједнице. Све у свему, NIM је пословни модел за оперативни рад полиције (OSCE, 2017).

NIM даје објашњење обавештајног циклуса и процеса доласка до обавештајних производа, али истовремено представља и начин доношења одлука. Дакле, представља вид менаџмента који треба за резултат да има смањење киминалних активности. Усмерен на проактиван рад последично треба да доведе до спречавања злочина пре него што се они реализују. Ови процеси могу да се воде на три нивоа. Подаци који се прикупљају и обрађују по овом моделу могу да функционишу на једном нивоу или да буду засновани на размени података и информација између различитих актера на различитим нивоима у зависности од тога шта је предмет истраге.

„Постоје три нивоа обухвата криминала у Великој Британији: **први** је онај чије се активности врше на територији једне јурисдикције (надлежности), **други** је онај чије се активности врше на територији више јурисдикција и **трећи** који је међународни. НИМ је дизајниран да свој утицај има на сва три нивоа криминалних активности“ (Шебек, 2017: 16-35):

- Ниво 1 – *Локални криминал и неред*, локални криминал, криминалци и други проблеми који имају утицај на полицијску организацију локалног нивоа или мању област.
- Ниво 2 – *Прекогранична питања* која утичу на више од једне BCU (Basic Command Units – BCU); криминалне активности или други специфични проблеми који имају утицај на више од једне полицијске територијалне надлежности.
- Ниво 3 – *Тешки и организовани криминал*, обично делује на националном и међународном нивоу, размере које захтевају идентификацију проактивним средствима и одговор првенствено кроз циљане операције наменских јединица.

Модел је требао да омогући прикупљање и размену информација на свим нивоима, па и израду стратешких продуката за различите нивое. Главне делове модела представљају процес одређивања задатака, координација криминалистичко-обавештајног рада међу нивоима и расподела продукта коначним корисницима. На овакав начин примена криминалистичке обавештајне делатности донела је позитивну евалуацију дотадашњих активности на прикупљању доказа у конкретним истрагама, а у исто време на вишем нивоу придонела прикупљању информација за стратешке потребе. Као типични продукт проактивних стратегија спомињу се, на пример: стратегија сузбијања насиља у вези са трговином дрогама, криминалитет у вези са забрањеним миграцијама и други (Шебек, 2017).

„Управљачки процеси NIM-а се у суштини реплицирају на сваком нивоу, што у принципу омогућава да се информације из сваке основне командне јединице упореде на нивоу снага и према томе информишу доношење одлука на том нивоу, а заузврат да се производи из сваке јединице упореде на нивоу снага. На пример, проблем дрога се може решити холистички и истовремено кроз одговарајуће одговоре на сваком нивоу“ (Maguire & John, 2006: 5).

Кључни производ на нивоу 3 је годишња процена претњи у Великој Британији, названа *Национална стратешка процена озбиљног и организованог криминала* (НСА). Произвела ју је Национална агенција за криминал Уједињеног Краљевства (НЦА) на основу података које су доставиле полицијске снаге, царина, обавештајне и безбедносне агенције и друга тела за спровођење закона. НСА пружа свеобухватну слику ризика по Уједињено Краљевство и његове интересе озбиљним и организованим криминалом. Пружа националном нивоу информације о томе који су приоритети и које акције ће се предузети, очекивани резултати и како ће се мерити успех (OSCE, 2017).

„Сваки ниво води и стратешке и тактичке групе за задатке и координацију, које се често значајно преклапају у особљу, али имају различите сврхе: стратешке групе постављају широку ‚стратегију контроле’ за област (идеално узимајући у обзир стратегије контроле које производе групе на другим нивоима и у суседним областима), док се тактичке ближе фокусирају на планиране оперативне одговоре на специфичне проблеме или претње“ (Maguire & John, 2006: 5).

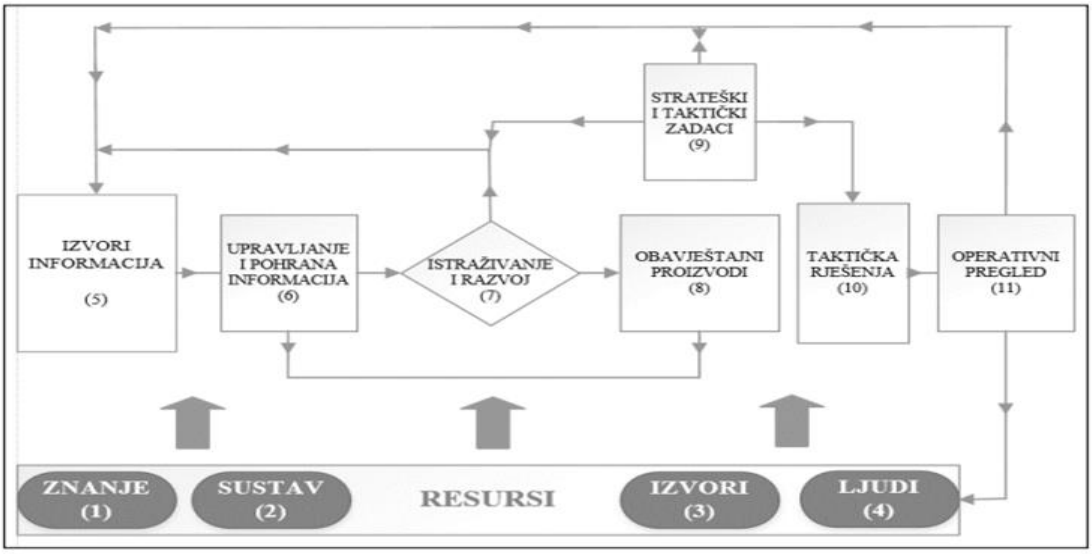
Овакве групе су састављене од менаџера, то јест од руководиоца различитих сектора који имају ингеренције да доносе одлуке о активностима, а пре свега о употреби расположивих ресурса. С обзиром на обим посла и на то да се стратешке групе баве креирањем стратегије која треба да да одговор на питање како најадекватније употребити расположиве расурсе и у складу са приоритетима, оне се састају квартално или једном у пола године. Тактичке групе баве се мањим обимом питања и локализованим проблемима, те се оне састају једном седмично или једном у две недеље.

Intelligence се дефинише као „информација која подлеже дефинисаној евалуацији и процесу процене ризика како би се помогло полицији да одлучује“ (Maguire & John, 2006: 5). Поред евалуације, информације се анализирају. Анализа укључује идентификовање критичних веза и асоцијација које помажу у разумевању образаца злочина, увреда, проблема понашања и инцидента. Из те анализе развијају се обавештајни производи и разматрају на састанцима било стратешких или тактичких задатака и координационе групе. На овим састанцима се идентификују приоритети и доносе се одлуке о распоређивању ресурса.

„Да би полицијска служба постала вођена обавештајним подацима, процес NIM-а мора да буде уграђен у локални и национални ниво полиције. Основе за то називају се средствима (ресурси), а обухватају:

- **средства знања** – познавање рада полиције и разумевање закона, политике и смернице;
- **системска средства** – поседовање одговарајућих система и структура, укључујући и безбедно окружење и праксе;
- **изворна средства** – обезбеђивање да се информације ефикасно прикупљају и управљају од што већег броја извори што је могуће и
- **људски ресурс** – успостављање професионалне структуре особља са обученим и одговарајућим квалификовано особље за обављање потребних функција у оквиру модела“ (NCPE, 2006: 14).

Модел NIM, подразумевајући и наведена средства (ресурсе), састоји се из 11 активности (Слика 13).



Слика 13. *Шема процеса Националног обавештајног модела*

Извор: *Краљ, 2019: 23*

„Жељени исходи делатности агенција за спровођење закона су: безбедност у заједници, смањење криминала, контрола криминала и контрола поремећаја. Национални криминалистичко-обавештајни модел то постиже кроз четири компоненте:

- *Процес постављања задатака и координацију*: процес постављања задатака и координацију (Tasking and Coordinating Process – T & CG) омогућава менаџерима са овлашћењима за доношење одлука да управљају својим пословима како тактички тако и стратешки. Процес се одвија кроз активности стратешких и тактичких група. Стратешко постављање задатака и координација (Strategic Tasking and Coordination – ST & CG) има за циљ постављање или измену контролних стратегија. Тактичко постављање задатака и координација (Tactical Taskong and Coordination – TT & CG) има за циљ пуштање у рад и примену тактичког менија до контролне стратегије, одговора на новонастале потребе и праћење спровођења договорених планова.
- *Четири кључна криминалистичко-обавештајна производа*: криминалистичко-обавештајни производи се ‚испоручују' како би полицијски рад могао бити вођен (усмераван) на основу криминалистичко-обавештајних информација. Овакав полицијски рад захтева четири типа криминалистичко-обавештајних производа, а то су: *стратешке процене, тактичке процене, профил мете/циља, профил проблема*.
- *Производи знања:* представљају низ производа, било локалних икли националних, којима се дефинишу правила за вођење послова из надлежности или ‚најбоље праксе', као и под којим условима се рад између агенција може спроводити.
- *Производи система:* ови производи заједно са производима знања подржавају НИМ како би планиран полицијски рад био вођен криминалистичко-обавештајним информацијама (ILP)" (Шебек, 2017: 26).

„Овај модел у почетку није лако прихваћен у полицијском раду. За многе је спадао у домен обавештајних служби и детективског посла, те су сматрали да наметање овог модела полицији нису схватали као помоћ за боље управљање полицијским послом у целини него као нешто што је наметнуто. Такође се чинило да је овај модел у супротности с другим моделима које је полиција усвојила у свом раду широм Краљевства. Док је, на пример, имао сличности са моделом оријентисаним ка решавању проблема, с друге стране био је у сукобу са онима који се тичу ‚услуга јавности'. Међутим, и реактивна тактика поступања полиције у Великој Британији у супротстављању криминалитету доживела је велике критике, пре свега због реактивне стратегије, која се огледала у примању притужби и представки, насумичним радом патрола, без претходне идентификације криминалних жаришта, запошљавањем великог броја полицијских службеника са циљем да се прикаже видљивост полиције, укључујући и спровођење рутинских криминалистичких истрага" (Рацић, 2023: 43).

„Руководиоцима полицијских станица и органима за спровођење закона је постало сасвим јасно да прикупљени и евидентирани подаци могу послужити као основ за доношење одлука. Полицијски службеници који су обрађивали такве податке добијају назив аналитичари. Организационо, аналитичари нису припадали истој организационој јединици у односу на обавештајне службенике, што је отежавало процес израде аналитичких производа. Такав отежан процес рада манифестовао се и одсуством аналитичара у полицијским одељењима, првенствено у подршци оперативном менаџменту приликом доношења одлука и одсуству њиховог учешћа у креирању стратегијских докумената" (Ericson & Haggerty, 1997: 10-15).

Када је у питању све већи нагласак на управљању учинком у вези са истрагом обимних злочина, најочигледније области потенцијалне некомпатибилности са NIM-ом су а) повратак фокусу на реактивну истрагу појединачних кривичних дела (приступ који су рани заговорници „проактивног" напали као неефикасан), „полиција вођена обавештајним радом" и б) све већи нагласак на „броју" (злочина, хапшења, оптужби, осуда, итд.) на могући рачун „квалитета" (Maguire & John, 2006).

„Применом NIM-а се знатно унапређује процес прикупљања података применом функција на основу стандардизовног криминалистичко-обавештајног процеса којим се уз примену националног криминалистичко-обавештајног система обједињују обавештајне,

превентивне и оперативне активности на стратешком, регионалном и локалном нивоу“ (Рацић, 2023: 50).

„У пракси полиција Велике Британије је направила највећи искорак успостављањем проактивног модела рада полиције, који је претежно усмерен на прикупљање обавештајних сазнања, који је у свету познат као полицијско-обавештајни модел“ (Ratclife, 2016: 16). Прво је спроведен пилот-пројекат, који је дао одличне резлтате и основу за увођење овог модела. Његово увођење се поклопило са почетком великог развоја информационих технологија, када је модел током времена еволуирао. Значајан напредак је учињен самом чињеницом да је сваки полицијски службеник на подручју своје месне надлежности могао да опише приоритете из области криминалитета и прекршаја, управља ризиком, усмерено прикупља информације према регистрованим појединцима и криминалним групама, што је у доброј мери утицало на економичност ресурса и представило могућност улагања у дугорочне мере за смањење криминалитета и прекршаја како би се извршила ресоцијализација појединаца и криминалних група. Поред унапређења функције прикупљања информација успостављањем криминалистичких јединица, јавила се потреба за успостављањем аналитичких јединица које ће имати задатак да све прикупљене информације и податке најпре обраде, анализирају и доставе руководиоцима, како би се донеле правовремене и релевантне одлуке. Успостављањем таквих аналитичких јединица структурирале су се функције прикупљања, обраде и анализе, што је представљало основ за успостављање криминалистичко-обавештајних послова“ (Рацић, 2023). Упркос отпорима британски национални-обавештајни модел је заживео као основа за Intelligence-led policing модел и не само то. Постао је и пример из праксе на коме су се развијале сличне праксе у другим земљама.

2.2.1.3 Примена полицијско-обавештајног модела у САД

„Ослањајући се на развој националног обавештајног модела у Великој Британији, примена полицијско-обавештајног модела у Сједињеним Америчким Државама се заснива на аналитичком, проактивном приступу рада у циљу идентификовања безбедносних претњи, пре него што се кривично дело изврши, чији основ чине оперативне информације на којима се заснива даљи оперативно-плански приступ рада. Од суштинског значаја за ову дискусију је да спречавање криминалитета и тероризма представља процес заснован

на сету оперативних претпоставки. Овај процес захтева посвећеност филозофији проактивног поступања, иако већина закона у основи правно уређује реактивно поступање“ (Cartera & Carter, 2009: 150).

Међутим, док су поједини научници промовисали примену британског NIM-а у САД, други су опомињали на разлике које постоје у полицијама ових двеју држава. Те разлике су се огледале у броју полицијских службеника и броју квадратних метара који спадају у њихову надлежност, затим у буџетима којима полицијске снаге располажу и разликама у стандардима. У поређењу са британском полицијском структуром, већина од приближно 17.985 америчких агенција за спровођење закона, од којих многе имају мање од 10 службеника, имају различите полицијске стандарде између и унутар држава. Буџети већине ових агенција су мали, у поређењу са онима у УК и обично долазе из локалних фондова допуњених краткорочним федералним грантовима. Нове филозофије полиције, нове иницијативе и федерални стандарди и препоруке су углавном неприменљиви осим ако није експлицитно наведено у посебним условима гранта. Иако се најбоље праксе могу извући из NIM-а и применити на полицију у САД, имајући у виду фрагментирану и разнолику природу америчког спровођења закона, филозофија ILP-а је много другачија у САД (Carter & Phillips, 2015).

Оно што разликује Intelligence-led policing модел који се примењује у САД од националног обавештајног модела у Уједињеном Краљевству је прикупљање „сирових“ информација и размена података не само између владиних агенција већ и са приватним сектором, те долази до сарадње између различитих агенција за спровођење закона, јавних институција које се не баве безбедношћу попут здравства и чак приватних компанија. „Амерички нагласак је заиста на размени информација у вези са могућим претњама и стварању обавештајних производа који се могу применити као резултат овог проактивног напора који може спречити или ублажити претње. Британски модел ILP-а, настао од NIM-а, фокусиран је на генерисање и анализу података о ситуационом криминалу и уобичајеним преступницима како би се донеле боље информисане одлуке у вези са полицијским ресурсима и циљањем на специфичне проблеме криминала“ (Carter & Phillips, 2015: 3).

Терористички напад Ал-Каиде на Куле близнакиње (Њујорк) 2001. године променио је безбедносну слику у целом свету. Као најочигледнија последица овог напада у сфери

безбедности су пооштрене безбедносне процедуре по аеродромима широм света. После овог напада свет није остао исти, а највеће промене десиле су се управо у америчком систему безбедности. Анализе које су извршене након овог напада показале су да је напад могао бити спречен да су различите агенције међусобно ефикасније размењивале податке и ту се управо огледа филозофија Intelligence-led policing модела. ,,На наведени догађај је првенствено утицао децентрализовани систем агенција за спровођење закона, где у САД постоји више од 17.000 одвојених полицијских организација“ (Томашевић и Рацић, 2019: 89).

У марту 2002. године више од 120 стручњака за криминалистичку обавештајну делатност из целог САД окупило се на *Самиту обавештајних служби*, који је финансирала Канцеларија за полицијску службу оријентисану на заједницу, а чији је домаћин било Међународно удружење шефова полиције. Као резултат, створена је Глобална обавештајна радна група, чији је први производ био Национални план за размену обавештајних података о криминалу (НЦИСП), у којем се наводи да „све агенције, без обзира на величину, морају имати минималну способност размене обавештајних података о криминалу“ (Carter & Phillips, 2015). Сматра се да ово не би могло да се спроведе без политичке одлуке, те да је за резултате овог самита посебно значајна одлука председника Џорџа Буша о унапређењу размене информација између агенција за примену закона. Ово је у пракси значило чвршћу сарадњу између војске, полиције и цивилног сектора.

Дакле, оно што је овај модел донео за америчке службе безбедности и полицију је груписање криминалистичко-обавештајних послова које би требало да води ка проактивном и ефикаснијем приступу у борби против организованог криминала, тероризма и слично. Савремене технологије су додатно подстакле имплементацију овог модела јер су олакшале не само размену података већ и њихово складиштење и обраду путем електронских база података. Последично, ово је захтевало и централизован систем одлучивања, али и то да сваки припадник полиције и сличних служби у потпуности разуме шта подразумева полицијско-обавештајни модел.

,,Посебно се истиче неопходност да се обезбеди да сви припадници полиције на исти начин разумеју и прихвате да примењују обавештајни рад као темељ свих операција. Потреба за његовом применом настала је после анализе и закључивања да би пре

имплементације припадници свих организационих јединица полиције требало истински да разумеју основне појмове везане за примену обавештајног рада и полицијско-обавештајног модела“ (Рацић, 2023: 53). Уз минималне смернице и повећану потражњу за ILP, вероватно ће постојати агенције које себе називају „вођене обавештајним подацима“, али немају функционалне способности да заиста управљају приступом вођеним обавештајним подацима (Carter & Phillips, 2015).

Полицијско-обавештајни модел у САД, који је усвојен као метод рада након наведених напада из 2001. године је посебно значајан не само за спречавање терористичких напада већ и за спречавање радикализације појединаца и саморадикализације. Ово значи да полицијски и други органи не раде само на прикупљању података о могућим учиниоцима тероризма, њиховим мотивима, методама и циљевима, припремним активностима и слично већ да је њихов посао да спрече и да неко ко није има раније проблема са законом и насиљем не постане терориста под утицајем радикализације.

Агенције за спровођење закона и америчка јавност сада имају повишену свест о опасности од тероризма. Иако ови учиниоци раде независно од традиционалних терористичких мрежа и група, они су често под утицајем таквих група кроз процес у који улазе као ненасилни појединци, а на крају постају насилни. Напори полицијских агенција за смањење таквих претњи ослањају се на развој и унапређење криминалистичко-обавештајне праксе. У средишту ове праксе је улаз необрађеног податка, информације у обавештајни процес (Fuentes, 2006).

Може се рећи да је полицијско-обавештајни модел рада полиције онај модел који укључује примену обавештајног циклуса у супротстављању савременим претњама безбедности какав је тероризам. Такође, овакав модел претпоставља сарадњу различитих делова система безбедности једне државе. Дакле, податке морају да укрштају и размењују и војска и полиција и сви релевантни делови цивилног сектора (становништво, удружења, различите агенције, приватници итд.) како би могло да се делује проактивно у оперативном раду полиције, што јесте филозофија овог модела рада. Ово значи да полиција не може да делује самостално, већ јој је потребна подршка и осталих сектора како би се дошло до кључних информација благовремено. Исто тако, инфромације се морају размењивати на различитим нивоима, од локалног до националног нивоа, а по

потреби информације се морају размењивати и са другима путем међународних организација.

Тренутно, већина обавештајних података о тероризму из Сједињених Америчких Држава долази управо са националног нивоа, као што су федералне службе. Након спроведених истраживања о децентрализованој улози рада полиције у Сједињеним Америчким Државама, један део научне јавности је мишљења да локални полицијски службеници не располажу компетенцијама, знањима и вештинама за прикупљање обавештајних података на економичан начин. Други део тврди да управо локални полицијски службеници, који су у сталном контакту са заједницом, представљају кључну карику у циљу прикупљања обавештења, нарочито имајућу у виду чињеницу да су терористи инфилтрирани у становништво и да су у статусу спавача све до момента када треба да изврше терористички акт (UNODOC, 2011).

„Праћење учинка је био део владиног процеса у Сједињеним Америчким Државама како би се сагледали резултати успешности полиције. Многи трвде да је квалитет рада полиције применом полицијско-обавештајног модела у погледу контроле криминалитета и личног понашања полицијских службеника побољшан као резултат ових догађаја. Међутим, јавност у Сједињеним Америчким Државама и у другим енглеским говорним подручјима указује да су полицијски службеници честа тема у медијима, нарочито кроз разне документарне емисије и програме“ (Рацић, 2023: 55-56).

2.2.1.4 Полицијско-обавештајни модел у Европској унији

Европска унија је специфична када је у питању примена ILP-а, с обзиром на то да чини економску и трговинску унију више држава, али нема остале елементе државности као што је случај са САД. Европска унија нема сопствену ни војску ни полицију па је самим ти отежана примена полицијско-обавештајног модела у оваквој заједници, али управо то је и чини интересантном за анализу. Када је размена информација између различитих држава чланица у питању, она је наишла на низ препрека не само у размени информација већ и у координацији такве размене. На првом месту проблем је страх држава чланица да би уступањем информација могле да упадну у замку губљења суверенитета.

Од свих безбедносних изазова, ризика и претњи по безбедност, тероризам је одређен као највећа опасност по безбедност ЕУ и постоје доста реалне могућности да ЕУ постане мета терористичких деловања. Након терористичких напада у САД из 2001, уследио је и низ напада на европском тлу, попут оних у Лондону и Мадриду, што је тероризам ставило у фокус ЕУ. Та опасност је велика и данас, а посебно након мигрантске кризе. Међутим, када је у питању размена информација о тероризму, ситуација се додатно компликује. „Препреке у сарадњи у борби против тероризма на међународном нивоу јављају се и у виду језичких, легислативних и културолошких разлика, као и разлика у полицијским праксама држава. Препреке могу бити и неадекватна контрола граница, недовољно издвајање финансија за борбу против тероризма, грађански немири и све оно што једну државу онемогућава да све своје безбедносне капацитете усмери на откривање и борбу против тероризма“ (Андрић и Ковач, 2021: 117).

Ипак, упркос наведеном, мора се приметити да су последњих деценија запажени значајни резултати у области полицијске сарадње у оквиру ЕУ. Европол је формиран 1998. године, а званично је почео са радом годину дана касније, као веома изражен и упечатљив облик координације полицијских служби држава које се налазе у саставу ЕУ. Он знатно поједностављује и олакшава проток и размену података и обавља стратешке анализе и извештаје, а исто тако обезбеђује техничку и стручну подршку у истрагама које су у току и које су у надлежности држава чланица. „Европол не представља неку наднационалну институцију са извршним задацима већ је он један специфични вид међудржавне полицијске помоћи и подршке и размене информација у циљу спречавања тешких облика кривичних дела која прелазе националне границе и са којима националне полцијске снаге не могу да се носе“ (Симић и Никач, 2010: 62). Примарни задатак Европола је прикупљање и обрада података везаних за криминал и поред Интерпола представља најбројнију међународну полицијску организацију. Такође, за безбедност ЕУ и рад Европола и полиција у државама чланицама значајна је и Европска безбедносна стратегија на којој је изграђена политика безбедности ЕУ. Ова стратегија је значајна јер помаже ЕУ да омогући приступ подацима и мрежама информација државама чланицама и да координише тај процес размене. Поред тога, ова стратегија као значајан документ подстиче и државе чланице да деле податке који су значајни за безбедност.

Европска унија се значајније усмерила на изградњу модела ILP након терористичких напада на Вашингтон и Њујорк (11. 9. 2001), те у Лондону и Мадриду нешто касније, а посебно после усвајања прве Европске безбедносне стратегије (2003). Коначно, увођењем ЕУ стратегије, која експлицитно препознаје претње организованог криминала по безбедност ЕУ, дошло је до различитих иницијатива осмишљених да побољшају способност институција ЕУ и држава чланица да одговоре изазовима организованог криминала. Најзначајније од њих су развој *Европског криминалистичко-обавештајног модела* (*European Criminal Intelligence Model – ECIM*), као и механизама за процену угрожености чланица ЕУ од претњи најтежим облицима криминала које у данашњим облику познајемо као *Процена претњи тешког и организованог криминала* (Serious and Organised Crime Threat Assessment – SOCTA) (Шебек, 2017).

ECIM-у је пружена улога да обезбеди ефикасније смањење озбиљних (тешких) форми криминала у области безбедности ЕУ, на основи идентификације претњи, односно угрожености. То се постиже кроз криминалистичко-обавештајни процес који има за циљ идентификовање криминалних претњи на основу информација и криминалистичко-обавештајних информација достављених Европолу, с обзиром на то да је ова институција централна тачка за пријем, складиштење и анализу прикупљених информација, што је основа за производњу *Процене претњи од организованог криминала* (Organised Crime Threat Assessment – OCTA). OCTA је представљао годишњи стратешки документ произведен на основу информација и криминалистичко-обавештајних информација које су државе чланице испоручиле Европолу, али и информација добијених од држава изван ЕУ, као и међународних организација за спровођење закона. Међутим, није то све ишло како се очекивало[14].

[14] На овом месту је потребно и изнети чињеницу о уоченим слабостима оваквих процена, а које се углавном односе на то да OCTA није оперативно оријентисана. Такође, развој OCTA је отежан чињеницом да су неке државе чланице вољне да пруже потребне информације Европолу, док са појединим то и није случај, а на које се Европол у потпуности ослања. Како Бредли истиче, док је током 2006. године једна држава чланица поднела преко 500 страница криминалистичко-обавештајних информација, друга чланица је допринела са само једном страном. Тако према: Bradley, H., (2008). Europol and the European Criminal Intelligence Model: A Non-state Response to Organized Crime, *Policing 2*(1): 107. Такође, државе чланице још увек су резервисане када је у питању давање информација институцијама као што је Европол, па у пракси више воле да сарађују билатерално, путем прекограничних истрага и разменом информација на *ad-hoc* основи, користећи изграђене билатералне односе. Иако свесни значаја комуникације и размене информација, у многим полицијским срединама (како истиче Ретклиф) постоји култура у којој се информације посматрају као власт. По добијању информације истражитељи покушавају да одрже власт, да докажу свој значај на радном месту

Током 2009. и 2010. године спроведен је пројекат (Harmony Project) који су водиле Белгија, Холандија и Велика Британија са Европолом, а који је имао за циљ преиспитивања и јачања европског криминалистичко-обавештајног модела кроз усклађивање функционисања свих подсистема овог модела. Резултат оваквих напора јесте развој и успостављање вишегодишњег циклуса политике деловања (Multi-anual policy cycle), (Council of the European Union, 2010), који ће обезбедити делотворну сарадњу између држава чланица ЕУ, агенција за спровођење закона, институција ЕУ, агенција ЕУ, као и релевантних партнера у борби против тешког и организованог међународног криминала. Полазна тачка овог циклуса политике деловања јесте *Процена претњи озбиљног и организованог криминала* (Serious and Organised Crime Threat Assessment – SOCTA). Овим документом Европол пружа аналитичке закључке који ће се користити за успостављање политичких приоритета, стратешких циљева и оперативних акционих планова (Шебек, 2017). Пун четворогодишњи циклус спровођења политике развоја овог модела почео је током 2013. године, када је развијен и стратешки документ Европола - *SOCTA 2013* (Europol, 2013).

Савет (министара) ЕУ је донео кључна документа за функционисање ECIM[15], који се одвија у четири фазе:

- У првој фази чланице ЕУ похрањују податке у базе Европола са криминалистичко-обавештајним информацијама на основу којих се сачињава SOCTA, поштујући приоритете ЕУ у борби против организованог криминала.
- У другој фази *Стални комитет за унутрашњу безбедност* (Standing Committee on Internal Security – COSI) формулише приоритете у борби против криминалитета на основу *Саветодавног документа о политици* (Policy Advisory Document – PAD), који доносе Председништво и Европска комисија и достављају Савету на усвајање. На основу SOCTA приоритета и осталих стратешких докумената, процена и политика, Савет усваја завршни

и на тај начин себи обезбеде бољу промоцију. Ово према: **Ratcliffe, J. H.,** (2008). *Intelligence-Led Policing,* Collompton, Devon, UK (Willan Publishing), p. 130.

[15] Закључак Савета о успостављању ECIM (10180/4/05); Заључак Савета о изради и имплементацији Циклуса OCTA (15358/10); Закључак Савета о захтевима корисника SOCTA (12267/15); Закључак Савета о континуитету Циклуса OCTA, за период 2018. до 2021 (7704/17) и Закључак Савета о постављању приоритета ЕУ у борби против организованог и озбиљног криминала у периоду 2018-2021 (9450/17). Види у: **Лештанин, Б., Божић, В., Никач, Ж.,** *Правни оквир за успостављање криминалистичко-обавештајног модела по стандардима ЕУ*, Зборник радова са међународног научног скупа „Усаглашавање правне регулативе са правним тековинама Европске уније – стање у БиХ и искуства других“, Истраживачки центар, Бањалука, 2018, стр. 241-254.

SOCTA документ. Сваки од ових приоритета захтева усвајање *Вишегодишњег стратешког плана* (Multi-Anual Strategic Plan – MASP) са неколико стратешких циљева.

- У трећој фази сачињавају се *Оперативни акциони планови* (Operational action plans – OAPs) за сваку годину циклуса како би се постигли различити стратешки циљеви везани за различите приоритете који се имплементирају и чија се примена контролише.
- У четвртој фази COSI израђује средњорочну и финалну процену резултата предузетих акција, како би се измерила достигнућа стратешких циљева и побољшала оперативна имплементација. На крају циклуса врши се независно вредновање (евалуација) процеса која служи као улаз у наредни циклус (Europol, 2013).

Хашки програм: јачање слобода, безбедности и правде у Европској унији, који је Савет ЕУ усвојио 2004. године, увео је основне принципе криминалистичко-обавештајне делатности који представљају темеље за успостављање европског криминалистичко-обавештајног модела заснованог на принципима полицијског рада вођеног криминалистичко-обавештајним информацијама – ILP. У том смислу, Савет ЕУ је позвао земље чланице ЕУ да омогуће Европолу кључну позицију, односно улогу у борби против организованог криминала и тероризма, а кроз успостављање правног основа за обавезно достављање криминалистичко-обавештајних информација и информација држава чланица ЕУ ка Европолу, као и међусобну размену информација (Шебек, 2017).

Ослањајући се на практична искуства и резултате које су остварили полиције Велике Британије и САД са Intelligence-led policing-ом и Европска унија 2005. године оснива европски криминалистичко-обавештајни модел (ECIM). Идеја је била да се на основу заједничке процене о угрожености ЕУ, а кроз размену криминалистичко-обавештајних информација на нивоу Уније, дође до већег степена безбедности.

„Иако је планирано да државе чланице и њихове полицијске организације постепено у потпуности прихвате ECIM, од почетка је постојала широка сагласност да је овај модел помогао да се ускладе полицијске праксе широм ЕУ, као и да се уводи ‚модерно', криминалистичко-обавештајним актиностима вођено, стратешко планирање" (Europol, 2009: 18) „Државе чланице ЕУ су први пут тестирале нови начин рада заједно 2006. године" (Шебек, 2017: 16-35).

Овим моделом Европол је стављен у централни положај када је у питању размена криминалистичко-обавештајних информација и његов задатак је да такве размене подстиче и између појединачних држава чланица. На основу Европолових извештаја,

руководећи органи ЕУ су доносили стратешке одлуке обликоване у стратешка документа. Међутим, проблем настаје када поједине државе чланице треба да операционализују та документа. Да би овај модел функционисао у пракси, било је потребно увезати низ агенција, организација и институција из различитих држава.

У ЕУ 1,2 милиона европских полицајаца ради на веома различите, а понекад и некомпатибилне начине. Данска, Финска и Ирска имају по једну националну полицијску службу, централизовану под јасно одређеним „шефом“. Али у Великој Британији и Холандији полиција је децентрализована – Велика Британија, на пример, има 50 одвојених полицијских снага. У неким земљама полиција има независна овлашћења за истрагу, док друге преузимају вођство од националних тужилаца. Полиција одговорна тужиоцима има тенденцију да реагује на злочин, поступајући тек након што је кривично дело почињено. Они раде мало превентивног рада. Ова разлика у улогама значи да се и полицајци и тужиоци из различитих земаља деле у два табора, проактивни и реактивни, када говоре о томе како се треба борити против транснационалног криминала.

Такође, легислатива у различитим земљама чланицама и процедуре рада су се разликовале, а ситуација се додатно усложавала када су савремене технологије и интернет узели примат у комуникацији између криминалаца. Тако је Савет Европе 2000. године ажурирао конвенцију о узајамној помоћи у кривичним стварима тако да укључује захтеве за тајне операције у иностранству, пресретање телефонских и интернет комуникација преко граница и операције надзора као што су „контролисане испоруке“ (где власти тајно надгледају злочине као што је трговина дрогом да би се открила криминална мрежа).

На пример, холандски службеници могу да врше надзор над осумњиченима у Белгији, са или без претходног обавештења. Италијански полицајци могу да прате осумњиченог кријумчара дроге у „врућој потери” у Аустрији док не стигне локална полиција. Полицајци широм шенгенског подручја такође деле информације о осумњиченима, украденој роби и аутомобилима преко „Шенгенског информационог система“ (СИС), мултинационалне полицијске базе података. Полиције у земљама Бенелукса помажу једна другој у свакодневним питањима закона и реда и чак имају заједничке стандарде за обуку и опрему. Пре Светског првенства у фудбалу 2006, Немачка и Аустрија су потписале споразум којим се њихова полиција ставља под команду једна друге у случају потребе и омогућава службеницима сваке од њих да спроводе

неограничене тајне операције на територији друге стране. Немачка је касније потписала сличан споразум са Холандијом. Нордијске земље већ годинама воде заједничке патроле и полицијске станице у ретко насељеним пограничним регионима. Исто раде и Шпанци са својим француским колегама дуж Пиринеја (Рацић, 2023).

Пун четворогодишњи циклус спровођења политике развоја овог модела почео је током 2013. године, када је развијен и стратешки документ Европола – SOCTA 2013 (Шебек, 2017). Идеја је да се приволе полиције из различитих земаља да у сарадњи планирају истраге користећи доступне обавештајне податке. Овај модел то постиже тако што ће осигурати да националне полицијске снаге, Европолови аналитичари, криминалистичке обавјештајне службе и шефови полиција раде заједно на истим претњама безбедности.

Овај модел у ЕУ функционише кроз неколико корака. Прво, полиције држава чланица деле обавештајне податке са Европолом, на основу кога се сачињава процена укупне претње организованог криминала са којом се суочава ЕУ. Користећи се овом проценом, Савет министара издваја приоритете са којима ће се њихова полиција заједно позабавити. Шефови полиција ЕУ затим започињу заједничке операције против криминалаца и враћају информације и научене лекције Европолу, на време да се припреми следећа процена претње.

Међутим, у пракси постоје проблеми у функционисању овог модела. Неке државе чланице не пружају довољно података Европолу, док су друге издашне у дељењу обавештајних података. Такође, у Европолу некада раде појединци који немају довољан ауторитет ни ингеренције у сопственим државама да спроведу оно што се од њих очекује. Опет, с друге стране, треба имати у виду да се овај модел рада усавршава из дана у дан и да Европол добија на важности како пролази време.

Такође, од изузетне важности за рад овог модела јесте безбедност информација које се дистрибуирају у Европол, те се стога приступа правилном вредновању и означавању *кодова за пренос* ка Европолу. По овим кодовима извор може бити: поуздан, обично поуздан, обично непоуздан и не може се проценити, док информација може бити: тачна без сумње, информација позната извору, информација није лично позната извору и не може се проценити.

Кодови за руковање информацијама су комплементаран и неопходан додатак процесу евалуације (процене) извора и информације, а размењују се преко Европола.

Кодови за руковање информацијама штите извор информација, осигуравају будућност информације и обезбеђују да се информације обрађују у складу са жељама власника информација.

Ови кодови могу бити:

- информација се не сме користити као доказ у судском поступку без одобрења даваоца информације,
- информација не сме бити дистрибуирана даље без дозволе даваоца информације
- или остала ограничења која треба применити (слободна форма).

2.2.1.5 Полицијско-обавештајни модел у Србији

Оно што се назива Intelligence-led policing у Србији је у фрагментима познато одраније кроз дугу обавештајну праксу. Међутим, *полицијско-обавештајни модел,* како се ILP назива, у Србији је усвојен делимично и због усклађивања прописа и рада полиције са оним из ЕУ, а делимично због пораста организованог криминала преко такозване балканске руте. Више у теоријском него у практичном смислу, у Републици Србији су праћени савремени трендови у организовању и раду полиције. Наиме, још пре него што је најављено увођење *Полицијског обавештајног модела* – ПОМ, заснованог на *Intelligence-led policing-u,* писано је о криминалистичко-обавештајном раду (КОР), односно криминалистичко-обавештајној делатности (КОД). Тако, Шебек (2017) тврди:

> „Пре важећег *Закона о полицији*, криминалистичко-обавештајна делатност па самим тим и модел полицијског рада вођен криминалистичко-обавештајним информацијама нису били нормативно дефинисани. На тај начин пракси је остављено да прилагоди поступање и дефинише основне смернице за рад, што се у истој показало као недовољно због чињенице да се криминалистичко-обавештајна функција тумачила произвољно и недоследно“.

Кад је у питању теоријски аспект криминалистичко-обавештајне делатности (КОД), Драган Манојловић каже да је исти најлакше објаснити преко послова које ради криминалистички аналитичар, у које убраја: 1) посматрају криминалну појаву, делатност, организацију, кривично дело и учеснике у криминалним делатностима, 2) опсервирају криминални миље и учеснике у њему, 3) захтевају примену оперативне технике; 4) прикупљају; 5) описују; 6) дефинишу; 7) проверавају; 8) класификују; 9) мере; 10) објашњавају; 11) предвиђају; 12) експериментишу; 13) уопштавају; 14) анализирају; 15) вреднују и (16) дисеминирају информације, податке и аналитичке информације које се односе на криминалне делатности, криминал и извршиоце кривичних дела. Све те послове

криминалистичких аналитичара Манојловић групише у неколико фаза: 1) прикупљање сазнања, 2) описивање прикупљених сазнања, 3) класификација прикупљених и описаних сазнања; 4) дефинисање прикупљених сазнања; 5) објашњење прикупљених података; 6) провера прикупљених сазнања и 7) криминалистичко-аналитичко предвиђање (Манојловић, 2008). Иначе, Манојловић сматра да је првобитни модел *криминалистичко-обавештајне аналитике*, у нашој литератури, преузет од ANACAPA модела, како се поима у страној теорији и пракси.

Министарство унутрашњих послова Републике Србије одлучило је да имплементира ILP у Србији како би се унапредило спровођење закона и подигли резултати у борби против криминала и других безбедносних претњи на виши ниво, као и да се рад полиције усклади са стандардима, структуром, квалитетом и терминологијом полицијских снага у развијеним земљама Европе и света. У вези са овим, Србија је 2016. усвојила нови *Закон о полицији* који дефинише ILP и даје упутства о томе како то применити у српској полицијској пракси (OSCE, 2017).

У Републици Србији је Закном о полицији из 2016. године утврђено да се уводи *Полицијско-обавештајни модел – ПОМ*. У годинама које су следиле тај модел је теоријски описан и нормативно утврђен, како би се приступило његовом увођењу у праксу. У бројним полицијским прописима у нас истиче се да је ПОМ преузет из развијених земаља Европе, а на бази *Intelligence-led policing-a,* како су га теоријски описали Ретклиф и други аутори.

Целовито (у општем смислу), чак и у нормативним прописима, ПОМ је у нас представљен као тзв. полицијска осмица, заправо приказ у облику броја осам (Слика 14).

Слика 14. *Полицијско-обавештајни модел као „осмица“*

Извор: *МУП Републике Србије, 2017.*

Са претходне слике уочаваоамо да ПОМ, у структурном смислу и као криминалистичко-обавештајни процес (КОП), чине три дела (целине): 1) руковођење и управљање, 2) криминалистичко-обавештајни послови и 3) оперативно-полицијски послови, који се именују као „планирани“. Наведена чињеница нам указује на то да се говори о целовитом раду полиције на сузбијању криминала, а не само о обавештајном делу. Та тврдња се повећава када се ПОМ, то јест КОП, развије у „осмицу“ функција (Слика 15).

Слика 15. *„Осмица“ функција ПОМ (КОП)*

Извор: *МУП Републике Србије, 2017 (обрада ауторке дисертације)*

Пре важећег Закона о полицији, криминалистичко-обавештајна делатност па самим тим и модел полицијског рада вођен криминалистичко-обавештајним информацијама нису били нормативно дефинисани. На тај начин пракси је остављено да прилагоди поступање и дефинише основне смернице за рад, што се у истој показало као недовољно због чињенице да се криминалистичко-обавештајна функција тумачила произвољно и недоследно (Шебек, 2017).

Из развијеног облика ПОМ као КОП уочавају се његове функције, где је криминалистичка анализа (реч „аналитика“ је касније уведена, прим. ауторке), једна од

функција криминалистичко-обавештајних послова. Тај развијени (функције) облик ПОМ, као КОП, а у складу са „4i“ моделом ILP, може се описати на следећи начин:

- Органи руковођења и управљања полицијом, на основу Закона и других прописа који регулишу њихове послове и надлежности, као и конкретне ситуације на стратегијском, оперативном и тактичком нивоу, постављају задатак делу за криминалистичко-обавештајне послове (intent – намера) да им доставе обавештајне информације (сазнања) о криминогеној средини.
- Органи за КОП прикупљају, обрађују, сређују и анализирају обавештајне податке и информације о криминогеној средини (interpret – тумачење), претварају их у крим-аналитичке производе и достављају их органима руковођења и управљања са предлогом мера (influence – усмеравање).
- Органи руковођења и управљања, на бази крим-аналитичких информација и сазнања, постављају задатке органима оперативно-полицијских послова да реагују у криминогеној средини (impact – утицај).
- Органи за оперативно-полицијске послове планирају и реализују активности из своје надлежности, а у складу са задатком који им је поставио орган за руковођење и управљање полицијом (МУП Србије, 2016).

Наведени циклус се константно понавља, уз непрекидну оцену свих његових фаза, коју спроводе органи руковођења и управљања полицијом, на општем, али и сваки структурни елеменат ПОМ (КОП) на свом нивоу. Дакле, то је комплексан модел рада полиције који обухвата и крим-обавештајне послове и анализу (аналитику) као њихов централни део, али и управљање и руковођење и планиране оперативне полицијске послове. У том смислу, превести *Intelligence-led policing* само као *полицијско-обавештајни модел*, јесте сужено виђење једног ширег процеса и модела рада полиције. Заправо, за *Intelligence-led policing* више би одговарао дослован превод *обавештајно вођен полицијски рад.* С друге стране, иако се ПОМ често упоређује са Обавештајним циклусом, он је значајно шири од њега, јер обухвата и управљање и руковођење, као и планиране оперативно-полицијске послове.

Криминалистичка анализа (аналитика, прим. ауторке) је део криминалистичко-обавештајних послова као процеса, а шире једне од три целине ПОМ-а. Као што се уочава на Слици15, криминалистичко-обавештајни послови (као процес) састоје се од пет корака (фаза): „1) планирање криминалистичко-обавештајних послова, 2) прикупљање података и информација, 3) обрада података и информација; 4) анализе података и информација и 5) достављање криминалистичко-обавештајних информација/производа“ (МУП Србије, 2016: 47). Сама криминалистичка анализа, као четврти корак криминалистичко-обавештајних послова, у нашим документима дефинисана је као: … процесно и методолошки најкомплекснија функција криминалистичко-обавештајних послова, којом

се прикупљени и обрађени подаци и информације обједињавају, структурирају, процењују и тумаче, на основу чега се изводе релевантни закључци и дају препоруке неопходне за доношење одлука за предузимање оперативно-полицијских активности (МУП Србије, 2016).

„Криминалистичка анализа, у оквиру криминалистичко-обавештајних послова у МУП-у Србије, операционализована је у осам садржаја (фаза/корака): 1) обједињавање података и информација, 2) идентификација празнина и несигурности у подацима и информацијама, 3) тумачење информација; 4) развој и тестирање хипотеза; 5) извођење закључака; 6) препоруке; 7) структурирање криминалистичко-обавештајних информација/производа и 8) верификација криминалистичко-обавештајних производа/информација“ (МУП Србије, 2016: 62).

У криминалистичкој аналитици, по угледу на страна искуства, примењују се стратешка и оперативна анализа.

1) „**Стратешка анализа** приказује тренутно стање и упозоравајуће трендове, промене, ризике и претње у области криминала и других безбедносно-угрожавајућих појава, могућности за спровођење оперативних активности и развој стратегије за борбу против криминала. Стратешка анализа описује, објашњава и предвиђа криминалне догађаје на основу узрочно-последичних веза (етиологије и феноменологије криминала). Стратешка анализа је посебно усмерена на проактивни рад полиције и обезбеђује и имплицира сарадњу полиције са свим субјектима на националном и интернационалном нивоу у области супротстављања криминалитету. То, пре свега, значи стварање стратегије супротстављања криминалитету која је фокусирана на идентификацију и отклањање узрока и околности које погодују различитим врстама криминалитета, а пре свега организованог криминала, корупције и других изузетно тешких кривичних дела“ (Исто, 52).

2) „**Оперативна анализа** приказује конкретне криминалне случајеве, лица и криминалне групе и њихове међусобне везе. Резултати оперативне анализе воде превентивном поступању полиције и ефикасном расветљавању и доказивању извршених кривичних дела“ (Исто, 57).

По угледу на напред наведени NIM, примењују се бројне врсте анализа, које су некада именоване и као методе (Манојловић, 2008), као, на пример: анализа образаца

криминала, анализа демографских и социјалних трендова, анализа криминалног тржишта; анализа криминалне мреже; анализа криминалних активности; анализа ризика; анализа резултата; анализа случаја; анализа телефонских разговора и друге (МУП Србије, 2016).

Криминалистичко-обавештајни производи су резултат заједничког рада и сарадње полицијских службеника ангажованих у обављању свих криминалистичко-обавештајних послова. Постоји велики број криминалистичко-обавештајних инфрмација/призвода, а четири њихове основне категорије (по угледу на британски NIM) јесу: 1) *стратешка процена јавне безбедности*, 2) *оперативна процена јавне безбедности*, 3) *профил безбеднсно интересантног лица/групе* и 4) *профил проблема* (МУП Србије, 2016).

„Период имплементације полицијско-обавештајног модела у полицији Републике Србије прати петнаест година дуг процес и покушај да се традиционални начин рада полиције усмери на проактивну примену савремених модела“ (Рацић, 2023: 67). Иако криминалистичко-обавештајно поступање није новина за снаге безбедности у Србији, ипак, увођење полицијско-обавештајног модела у рад српске полиције је процес који траје. Рад полиције у Србији је традиционално првенствено реактиван и репресиван насупрот ILP који је проактиван.

„Увођење полицијско-обавештајног модела у рад српске полиције је започело кроз сарадњу са шведском полицијом, а фокус овог пројекта биле су едукације и обуке. Затим је овај процес настављен кроз следећи пројекат, који се односио на анализу свих потребних активности које би за последицу имале стварање услова за имплементацију овог модела поредећи га са Шведском као референтним моделом. Затим су уследили пилот-пројекти у Новом Саду и Краљеву. Најзначајнији напори да се успостави полицијско-обавештајни модел постигнути су у периоду од 2015. до 2018. године, када је овај модел дефинисан као приоритет у Акционом плану за спровођење Програма Владе Републике Србије, што је уједно и стратешки приоритет у раду полиције Републике Србије“ (Рацић, 2023: 68).

„Савремени развој технике и техничких достигнућа, нарочито са аспекта примене савремених аналитичких алата и интегрисаних база података, утичу и на рад српске полиције. У покушају да се унапреди рад у циљу прикупљања података и информација успостављена је електронска апликација под називом „Оперативни извештаји“, која представља програмски софтвер или скуп програмских софтвера чија је основна намена

управљање подацима и део је јединственог информационог система МУП-а Републике Србије у делу „оперативних евиденција“ (Исто, 69).

Дакле, увођење полицијско-обавештајног модела у рад српске полиције захтевало је поред политичке воље и финансијска средства која су добијана углавном из страних фондова. Овакав модел захтева и техничко-технолошке могућности, с обзиром на убрзани развој савремених технологија, као и економске и људске ресурсе. Поред имплементације нових база података, потребно је и обучити кадрове да рукују са оваквим базама, а посебно је захтевно обучити аналитичаре који на основу обавештајних информација добијених из различитих извора имају способност да изводе стратешке закључке. Такође, изазов који и даље остаје је увезивање различитих служби, агенција и организација у један централизован информациони систем.

Након детаљног проучавања развијених модела ILP, као што су британски, амерички, канадски, аустралијски и шведски модел, Министарство унутрашњих послова је израдило српски ILP модел, који је у потпуности прилагођен специфичностима полицијског система у Републици Србији (OSCE, 2017).

***

Сумирањем искустава наведених држава може се закључити да је безбедносни оквир, који чине савремене транснационалне и хибридне претње, захтевао еволуирање полицијских организација од реактивних ка проактивним, како би биле способне да на такве претње одговоре. Увођење полицијско-обавештајног модела заживело је и у САД и у Европи, па чак и у мањим државама попут наше. Разлози за организовање полицијских послова у складу са ILP су различити од државе до државе, али на првом месту ту су транснационални организовани криминал, тероризам, корупција и друга тешка кривична дела која захтевају одговор заснован на провереним, тачним и обавештајним подацима који долазе из различитих извора.

Иако су различите безбедносне потребе наметнуле тенденцију ка увођењу овог модела, може се приметити да је заједничко за све описане државе да је постојао известан отпор код припадника полиције, али и јавности, приликом његове имплементације у рад полицијских организација. Његово увођење је процес који захтева низ припремних активности и прилагођавања, те такав пројекат није једноставан и захтева одређен временски период како би у потпуности заживео. Такође, заједничко је и то да су

трансформација и увезивање различитих делова система безбедности са радом полиције захтевали низ организационих измена и оснивање нових тела, јединица у оквиру организације или органа који врше координацију различитих извора из којих информације долазе.

Посебно је значајно оснивање аналитичких јединица и центара и стављање акцента на оспособљавање људских ресурса који се баве аналитичким пословима, те се закључује да аналитички послови нису стриктно полицијски и да захтевају шире знање и посебне вештине код кадрова који обављају послове аналитичара. Различити делови система безбедности у оквиру полицијско-обавештајног модела имају задатак да благовремено прибаве тачне податке који могу, али и не морају, да имају посебан значај. Задатак аналитичара је да те податке филтрирају и обраде како би на крају дошли до предлога за руководеће органе на које претње безбедности је потребно ставити фокус кроз предиктивно анализирање постојећих података. Иако је полиција централна организација за овакав модел рада, он пак укључује и друге делове система безбедности и представља нешто што се може идентификовати као платформа за безбедносну аналитику.

Без обзира на отпоре који су се јављали код полицијских службеника и код дела јавности у државама у којима је спроведен ILP, резултати су показали да овај модел у пракси боље ради него реактивни полцијски модел. Искуства су позитивна у смислу да је модел рада полиције заснован на унапређењу обавештајне функције полиције напослетку ефективнији, ефикаснији и економичнији у погледу искоришћавања људских, техничких и свих других ресурса у супротстављању савременим претњама безбедности.

ДРУГИ ДЕО: ТЕОРИЈСКИ МОДЕЛ БЕЗБЕДНОСНЕ АНАЛИТИКЕ

У првом делу дисертације, осим теоријског одређења безбедносне аналитике, описан је рад у домену њених појединих врста, примарно именованих као „обавештајна аналитика“ (војска) и „криминалистичко-обавештајна аналитика“ (полиција). Суштински посматрано, наведене две врсте аналитике односе се на спољну безбедност (обавештајна аналитика) и унутрашњу безбедност (криминалистичко-обавештајна аналитика). Међутим, главни циљ истраживања јесте да се креира јединствен теоријски модел безбедносне аналитике на националном нивоу, којим би били обухваћени безбедност државе и грађана, из најмање три разлога. **Први**, безбедност је поодавно проширена из чисто војног сектора (рат као оружани сукоб) у политички, економски, друштвени (социјетални и социјални) и еколошки сектор (Buzan et al., 1998). **Други**, Устав Републике Србије, у надлежности државе, посебно утврђује да: „Уређује и обезбеђује одбрану и безбедност Републике Србије и њених грађана“ (Устав РС, 2006). **Трећи** јесте истраживачки покушај да се оптимизује процес управљања системом националне безбедности Републике Србије у домену стицања свеобухватне информације о угрожености државе и грађана.

У складу с наведеним, научно оправдано је било да се покуша креирати јединствен *теоријски модел безбедносне аналитике*, којим би били обухваћени сви аспекти безбедности државе и грађана, с једне, као и процеса рада аналитичара који у свом раду користе разне методе и технике и изграђују посебне стандарде, с друге стране. Тако, теоријски модел безбедносне аналитике, примарно, јесте *база знања*, чије се креирање у овом истраживању проверава на супротстављању тероризму.

1. МЕТОДА МОДЕЛОВАЊА

Према науци, али и другим системима идеја, веровања или деловања произилази да је моделовање саставни део људског мишљења. Наиме, у свим реалитетима и процесима, људи мисле у одређеним стандардима и ослонцем на њих. Притом, формирање нових појмова остварује се преко стандардних и већ познатих. Упркос томе, метода моделовања нема дугу историју примене.

Према методолошкој литератури, моделовање је рационалан, системски и сложен поступак адекватног представљања битних одредаба одређеног процеса, појаве, односно реалитета или њихових замисли, као одређене целине. Поједностављено казано, моделовање је процес израде модела (Миљевић, 2007).

Жигић и сарадници (1992) пишу: „Моделовање се убраја у основне научне методе научног истраживања. Заснива се на ‚тесној повезаности теорије и праксе', те овај метод служи истраживачима у објашњавању теоријских система помоћу система из праксе. Модел није ништа друго до мисаона конструкција једног једноставнијег система помоћу кога се на разумљив начин објашњава неки други, далеко сложенији систем. Модел се, дакле, налази у одређеном односу са својим оригиналом".

Душан Симић (2002), на пример, истиче: „Између модела и оригинала постоји аналогија или сличност, која у основи представља једнакост структура, функција или понашања или само неких од наведених, на основу чега је могуће да се проучавањем модела М дође до нових сазнања о самом систему С. Модел, у основи, има три задатка: 1) описивање и разумевање проучаване појаве, 2) повећавање моћи предвиђања и 3) демонстрирање теорија и хипотеза".

Према мишљењу професора Богдана Шешића, као последица развоја кибернетике настала је метода моделовања, као општа научна метода. Ова метода, како каже Шешић (1974), „има основну карактеристику да чини јединство теорије и праксе, које је на вишем квалитатитвном нивоу него код статистичке методе".У том смислу, пише Шешић (1974): „Под моделовањем се не подразумева само чулно представљање и физичко подражавање, него и свако психичко представљање, чак и замишљање било ког предмета или појаве".

Пишући о истраживањима у политичким наукама, Славомир Милосављевић (1980) сматра да је моделовање једна од фундаменталних научних метода и тврди: „Ова метода се појављује као општа теорија друштвено-политичких односа, систем политичких, правних и других норми и као одређени систем остварења у пракси – као моделни експеримент". У том смислу, полазећи од становишта да је моделовање конститутивни део сваког процеса људског мишљења, Милосављевић са Радосављевићем (1975) закључује: „Под појмом моделовање се подразумева рационалан, систематски, сложен поступак адекватног представљања битних одредаба процеса, појаве, односно друштвених реалитета или њихове замисли као целине".

У складу с наведеним, можемо да закључимо: *Моделовање је чулно представљање, физичко подражавање и умно замишљање било каквог предмета или појаве.*

Разни аутори на сличне, али ипак различите начине утврђују и описују примену методе моделовања у истраживању. Тако, на пример, Милосављевић и Радосављевић (1975) истичу да примена методе моделовања има следеће фазе: дефинисање потреба и сврсисходности израде модела; избор предмета моделовања; избор врсте и типа модела; избор средстава моделовања; избор сарадника у изради модела; пројектовање модела и његова израда; тестирање модела и његова евентуална дорада и представљање и употреба модела .

Сакан Момчило (2006) је става да процес моделовања чине следеће фазе: 1) утврђивање намене модела, 2) анализа својстава оригинала, 3) конструкција модела и 4) провера и побољшање модела.

Дакле, према наведеним, али и другим ауторима, модел је централни део методе моделовања. У том смислу, о појму и врстама модела у теорији постоје доста слични, али и различити ставови. Навешћемо неке.

Према мишљењу професора Раденковића и сарадника (1999), „модел је упрошћена и идеализована слика реалности, која нам омогућава да се суочимо са реалним светом (системом) на поједностављен начин, избегавајући његову комплексност и иверзибилност, као и све опасности (у најширем смислу те речи) које могу проистећи из експеримента над самим реалним системом“.

Милосављевић и Радосављевић (1975) за модел кажу да је: „имитација, прототип или пројекција неког предмета – дела постојеће, прошле и могуће будуће друштвене реалности“.

На основу опсежних анализа бројних теоријских извора, Раденковић и сарадници (1999), у смислу гносеолошке природе модела, разликују следеће основне врсте модела: теоријски, практични, реални, идеални; прости; сложени; структурни; функционални; парцијални; глобални; аналитички; типолошки и мрежни; детерминистички; стохастички и статистички. Осим наведених, често се користе и мешовити или комбиновани модели, као што су, на пример: теоријско–практични, структурно-функционални или комплексни.

Приступајући моделовању и моделима из прагматичних разлога, Мирослав Михаљишин (2010) закључује: „Моделовање треба да омогући стварање јасне и реалне

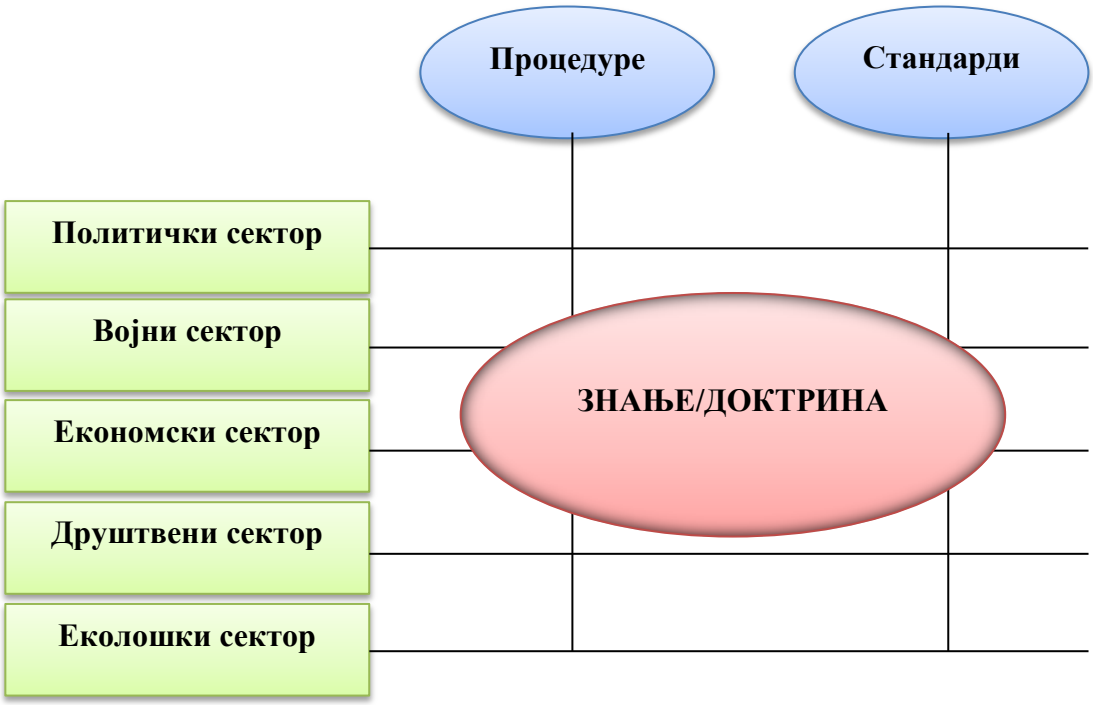
представе – визуелизација система (појаве, процеса), тако да можемо да га видимо какав јесте, односно онаквог каквог желимо да га реализујемо. Модел треба да омогући разумевање система (појаве, процеса), а тиме и бољу спецификацију структуре и понашања система (појаве, процеса). На основу модела требало би бити могуће дефинисати шаблон – образац који помаже приликом конструисања или управљања системом (процесом, појавом)".

Истраживање за потребе ове дисертације има за циљ изградњу теоријског модела безбедносне аналитике. У том смислу, иако тај модел, пре свега, треба да послужи пракси, нас посебно интересује теоријски модел.

Теоријски модел. У класификацији модела, између осталих, разликујемо практичне, идеалне и идеализоване моделе. „Теоријски модел јесте идеализовани модел, који делом чине саставни делови праксе, а делом норме, захтеви, упутства и потребна знања усмерена ка пракси" (Миљевић, 2007).

2. ОСНОВЕ ТЕОРИЈСКОГ МОДЕЛА БЕЗБЕДНОСНЕ АНАЛИТИКЕ

У складу са претходном опсервацијом и одређењем појмова „модел" и „теоријски модел", у овом делу дисертације се делови праксе, као што су обавештајна аналитика, криминалистичко-обавештајна аналитика и друге врсте аналитике, које само носе заједнички именитељ „безбедносна аналитика", обједињују у целовит модел безбедносне аналитике, којим се оптимизује процес аналитике безбедности државе и грађана на стратегијском нивоу. Тај модел, као теоријски, требало би да омогући његову примену и проверу у пракси, са функционалног и структурног аспекта посматрано. *Теоријски модел безбедносне аналитике* приказан је на Слици 16.



Слика 16. *Теоријски модел безбедносне аналитике*

Извор: *Обрада ауторке дисертације*

Са претходне слике уочавамо четири кључна сегмента теоријског модела безбедносне аналитике, која ћемо описати у даљем тексту. Ти сегменти су: 1) сектори безбедности, 2) процедуре рада аналитичара, 3) стандарди који се користе у безбедносној аналитици и 4) знање/доктрина. Преко наведених сегмената теоријског модела, као његове *структуре*, треба да опишемо функционисање процеса безбедносне аналитике.

2.1 Сектори безбедности

Ово истраживање примарно је усмерено на националну безбедност, односно безбедност државе и њених грађана. У том смислу, у теорији је најраспрострањенија напред наведена дефиниција безбедности коју је дао Арнолд Волферс (Arnold Wolfers) , односно њен објективно-субјективни аспект. Овај Волферсов (објективно-субјективни) приступ безбедности искоришћен је у бројним теоријским радовима, али и службенм документима држава. Тако, на пример, у Републици Србији је појам „национална безбедност“ први пут дефинисан у неком службеном документу тек 2019. године, где

стоји: „Национална безбедност Републике Србије јесте објективно стање заштићености њених националних вредности и интереса од свих облика угрожавања, те субјективан осећај безбедности грађана Републике Србије“ (Стратегија националне безбедности, 2019).

Из претходне дефиниције посебно подвлачимо синтагму *од свих облика угрожавања*.

Дуго је основни облик угрожавања националне безбедности био **рат**, поиман као оружани сукоб, војна претња. Потврда претходног става јесте и прво помињање израза „национална безбедност“ Волтера Липмана (Lippman Walter, 1943), који каже: „Једна нација је безбедна све док не мора да жртвује суштинске вредности уколико жели да избегне рат, а ако је нападнута способна је да их одбрани победом у једном таквом сукобу“.

Науке о безбедности, рудиментарно препознатљиве по називу „студије безбедности“, појављују се након Другог светског рата (Вилијамс, 2012). У том смислу, за време Хладног рата, у групи тзв. критичких теорија безбедности или теорија социјалног конструктивизма, појављује се Копенхашка школа безбедности као део Института за истраживање мира – КОПРИ, из Копенхагена (Данска). Та школа је допринела прво теоријском, а касније и практичном проширењу појма безбедности, из чисто војног у друге секторе безбедности, као што су: политички, економски, социјетални (друштвени) и еколошки сектор. Приступ проширењу појма безбедност прихватила је научна теорија, а примењен је и у бројним службеним документима држава света чија је проблематика национална безбедност.

Пре Првог светског рата безбедност се везивала за појам суверене државне власти, на њену заштиту уз помоћ војске и полиције. Дакле, референтни објект безбедности била је држава. Након Првог светског рата све више се говори о концепту међународне безбедности, а након Другог светског рата међународна безбедност долази у фокус, али и синтагма „национална безбедност“ улази у међународни дискурс. Након краја Хладног рата, који је са собом носио нестанак ривалства између два блока у војном, оружаном и нуклеарном смислу, долази до шире перспективе када је безбедност у питању. Смањењем оружаних и војних претњи фокус се преноси на претње невојног карактера. Такође, долази и до промена у науци, које се последично одражавају и на схватање појма безбедност.

Завршетак Хладног рата и парадигматска промена у друштвеним наукама довели су до продубљења и обогаћивања концепта безбедности. Концепт се проширио (Слика 17) са чисто војне на остале димензије друштва, попут политике, екологије, економије итд. Тако и држава престаје да буде једини референтни објект безбедности, већ се она почиње посматрати кроз безбедност појединца, група, региона па и кроз међународне оквире.

Међу оним мислиоцима који су проширивали студије безбедности и који су такође потекли из мировних студија, посебно велики утицај имали су припадници Копенхашке школе безбедности. Они су комбиновали проширени концепт безбедности (секторска анализа) са постструктуралистичком концептуализацијом безбедности (теорија секуритизације), као и са неким елементима неореализма, поготово у теорији регионалних безбедносних комплекса (Ејдус, 2012).

Слика 17. *Концепт безбедности: нивои и сектори безбедности*

Извор: *Обрада ауторке дисертације*

Свакако, како смо већ навели, постоји у теорији и другачији приступ анализи националне безбедности. Како смо истакли, професор Љубомир Стајић националну безбедност рашчлањује на спољну и унутрашњу компоненту, које заједно чине интегралну безбедност државе (Стајић, 2021). Међутим, и анализа компоненти (унутрашња + спољна = интегрална безбедност), недвосмислено захвата секторе безбедности. У току истраживања је провераван приступ одређењу националне безбедности, што ће бити приказано у трећем делу дисертације – *Резултати истраживања*.

У овом истраживању, као први сегмент теоријског модела безбедносне аналитике узимају се *сектори безбедности*, како их је утврдила Копенхашка школа безбедности, а којима треба да се обухвати национална безбедност, нарочито јер су ти сектори научно доказани. Општа и начелна шема сектора безбедности приказана је у Табели 12.

Табела 12. *Сектори безбедности*

СЕКТОР	ОДНОСИ	РЕФЕРЕНТНИ ОБЈЕКТ	ПРИМЕР ПРЕТЊЕ
Политички	Односи ауторитета	Организациона стабилност социополитичког реда	Револуција. Ширење марксистичке идеологије након Другог светског рата.
Војни	Односи моћи	Територијални интегритет државе	Инвазија Немачке као претња европским земљама 1939-1945.
Економски	Трговински односи	Економски поредак	Крах берзе 1929. Светска економска криза 2008.
Социјетални	Односи колективних идентитета	Колективни идентитет	Културни империјализам. Страх Француске од америкanизације. Страх Срба од губитка Косова.
Еколошки	Односи човека и природе	Цивилизација и/или биосфера	Глобално загревање. Цунами. Подизање нивоа мора. УВ зрачење.

Извор: *Ејдус, 2012: 116.*

2.1.1 Политички сектор безбедности

Политика је основна, а по неким ауторима и једина функција државе (Лукић, 1979). Политички сектор безбедности, према ставовима теоријског творца професора Берија Бузана, као и његових сарадника (1998), примарно се исказује као „социополитичка кохезија унутар једне државе, односно легитимитет који њене установе уживају код грађана“ . У том смислу, политичке претње могу да буду унутрашње и спољне. Поред

наведеног, а у анализи ставова Копенхашке школе о политичком сектору безбедности, како то наводи Филип Ејдус (2012), „политичке претње безбедности могу да буду *намерне* и *структурне*. Међу њима се издваја *тероризам*, који има велику политичку, а малу аналитичку моћ“ (стр. 151-153).

Намерне претње безбедности у политичком сектору односе се на активности једног субјекта (друге државе, држава) на расцепу неке друге државе или нације. Типичан пример јесте настојање неких држава да Косово постане самостална и независна држава. *Структурне претње* политичког сектора настају више из природе ситуације, него ли стварне намере. Типичан пример ове врсте претњи јесте отпор према регионалним интеграцијама, какав је имала Француска према Унији педесетих година и Велика Британија у другој деценији овог века. Такође, у структурну врсту претњи политичког сектора може се сврстати и однос Србије према чланству у НАТО.

Тероризам, као појава, споран је од самог дефинисања тог појма, преко идентификовања ко је терориста и шта су терористичке активности, до праксе супротстављања тој пошасти у савременим међународним односима у свету, али и у Европи. Европа је и у 20. веку и данас била подручје испољавања терористичких активности. У прошлости, у Европи су деловале организације означене као терористичке, као што су, на пример, Црвене бригаде, Баден-Мајхов група, Ирска републиканска армија, ЕТА, Баска и друге, док у овом веку кључна претња од тероризма долази од муслиманских терористичких организација, ИСИЛ, Ал-Каида, Муслиманска браћа, Хамас, Хезболах и друге.

> „У периоду 1970-2015. године у Европи су се догодила 18.803 терористичка акта, у којима су убијена 10.573 лица. Дакле, у просеку, преко 350 терористичких аката годишње (Гудовић, 2019). Посебну латентну и реалну претњу безбедности Европе представљају ‚страни терористички борци’, где се примарно мисли на грађане неких европских држава који су путовали на ратом захваћено подручје у Ираку и Сирији и прикључивали се терористичким организацијама. Највећи број тих ‚страних терористичких бораца’, кад је Европа у питању, јесу са Косова и Метохије, из БиХ и Белгије. Према истраживању Британског савета из 2018. године, а у односу на милион становника, из Белгије су на ратиште биле 44, из БиХ 68, а са Косова и Метохије чак 170 особа“ (Азиновић, 2018).

Политички сектор безбедности посебно се исказује као опасност која настаје због сукоба интереса како у држави тако и у међународним односима. У том смислу, Кузмановић и Благојевић (2021) истичу:

> „Обухват синтагме ‚политичка димензија’ веома је широк, пре свега због раширености, практичности, еластичности и дијалектичности појма политике. Мотиви, као чиниоци који

покрећу појединце или групе на деловање, играју велику улогу у обликовању интереса и циљева јер су засновани на потребама“ (стр. 102**)**.

Сукоби интереса у политици могу да проузрокују кризе, као снажне исказе угрожавања безбедности. У складу с наведеним, Миланко Зорић (2010) као највеће узроке политичке кризе наводи:

„1) борба ривалских сила, група великих сила и војних савеза и пактова за стицање и прерасподелу колонија и протектората, интересних сфера и зона утицаја,
2) борба за освајање туђих територија и за стицање државне територије анексијом, мирном и оружаном окупацијом и на друге начине,
3) геополитичко надметање или борба за запоседање и контролу извора енергената и стратегијских минералних сировина (нафта и земни гас, металне и неметалне сировине) и других природних богатстава у страним земљама, за контролу транснационалних нафтовода и гасовода и међународних водотока, канала и мореуза и других важних стратегијских објеката широм света, као и борба за стицање иностраних тржишта ради пласмана сопствене робе и услуга и истискивање противника;
4) конфронтација и борба за контролу и надзор над светским (и међуконтиненталним, континенталним и регионалним) копненим и поморским комуникацијама, трговачким путевима и саобраћајним коридорима и важним стратегијским правцима и објектима на територијама страних држава;
5) надметање и дубока политичко-идеолошка размимоилажења између великих сила и војних блокова и борба за геополитичко преуређење света, за прерасподелу моћи и снаге у своју корист, за геополитичку превласт и монополски положај у светским (и трансконтиненталним, континенталним и регионалним) оквирима и сузбијање и изолација ривалских сила, односно борба за стицање, одржавање и проширивање светске хегемоније или доминације и за наметање новог система међународних односа;
6) борба за опстанак и развој неке државе или групе држава угрожене или нападнуте од стране неке друге државе, групе држава и војног блока или неке међународне организације“ (стр. 304).

2.1.2 Војни сектор безбедности

Ма како посматрали мноштво претњи по човека, његове заједнице и околину, војна претња, рат (оружана борба) и даље остаје најдрастичнији облик угрожавања због могућности избијања ратова ширих размера, који са собом носе масовне људске жртве, огромна материјална разарања и деструкције свих врста. На тлу Европе започела су два светска рата у прошлом веку, која су завршена агресијом (ратом) НАТО на СР Југославију (1999). У складу с наведеним, као референтни објект у овом сектору безбедности истраживачи Копенхашке школе виде *сувереност*, односно *територијални интегритет државе*. На основу тога, кључна претња безбедности јесте угрожавање територијалног интегритета државе од неке друге државе или групе држава. У складу с наведеним, долази до војних криза.

О узроцима међународне војне кризе, Миланко Зорић (2010) пише:

„Најзначајнији војни узроци међународних политичких и војно-политичких (и ратних), па и економских криза јесу следећи: 1) нападачки рат, инвазија и други акти оружане агресије једне државе, групе држава, војног савеза, мултинационалне коалиције и неке међународне организације против друге државе, групе држава и војног савеза и коалиције, 2) спољна агресија или иностранa војна интервенција у унутрашњи сукоб у кризној држави или групи држава (унутрашњи рат, герилско ратовање, оружана побуна, устанак, револуција и контрареволуција, масовни сепаратистички тероризам), 3) већи гранични и погранични сукоби и разни инциденти, разбуктавање територијалних спорова и сукоба, ескалација територијалних претензија и ревизионистичких захтева и територијална освајања; 4) војнопоморска и ваздухопловна блокада неке острвске и друге државе или њених појединих острва и прекоморских територија и ескалација сукоба до локалног рата; 5) стварање, помагање и ангажовање незаконитих војних и параполицијских формација, а пре свега сепаратистичко-терористичких организација и масовног сепаратистичког тероризма у кризној држави или групи држава у садејству и савезништву са појединим страним државама и војним савезима и с неким међународним терористичким организацијама и агресија неког војног блока или коалиције против неке државе, те разне тајне операције и субверзивне акције“ (стр. 309).

Војни притисак се испољава као претња употребе силом, бојкот извоза наоружања или опреме из неке земље и санкције (забрана) на увоз наоружања и опреме у неку земљу. Типичан пример овог облика војне кризе на глобалном нивоу настао је 1962. године, приликом распоређивања руских ракета средњег домета на Куби[16]. Та политичко-војна криза између СССР и САД, интересантно, касније је употребљена у теорији за стварање синтагме „кризни менаџмент“ (Беденик-Османагић, 2010).

Бојкот и санкције, као изрази војне кризе, присутни су у историји, а највидљивији су управо данас, у току рата у Украјини, или шире – сукоба колективног запада и Русије. Тренутна војна криза између Русије и НАТО прети да прерасте у рат глобалних размера, Трећи светски рат, који због поседовања снажних ефектива нуклеарног оружја с обе стране може да произведе несагледиве последице по планету Земљу.

Погранични сукоби су честа појава војних криза, које настају због нерешених отворених питања између суседних земаља. Карактеришу се мањим оружаним облицима

[16] У затегнутим односима између САД и СССР-а шездесетих година прошлог века, користећи затегнуте односе САД и Кубе, а поводом распоређивања нуклеараних ракета у Турској и Италији, СССР је распоредио ракете средњег домета на Куби. Шпијунски авион САД, који је снимио распоред совјетских ракета, совјетски ПВО је срушио. Дошло је до војне блокаде Кубе од стране САД, док је СССР покренуо своје ратне бродове ка том региону. Дошло је до јаке војне кризе, која је претила да се сваког часа прелије у велики сукоб САД и СССР. На срећу, сукоб је решен дипломатским путем. Шире у: **Стојановић, Д.** (2015). *Рађање глобалног света 1880-2015: ваневропски свет у савременом добу*. Београд: Удружење за друштвену историју.

војски у пограничном појасу, које, најчешће, не прерастају у ширу употребу војне силе. Типични погранични сукоби често се догађају између Индије и Пакистана, као и Индије и Кине.

Војна интервенција јесте израз војне кризе која прераста у једнострану примену војне силе неке државе или коалиције на другу државу, при чему та друга држава не пружа снажнији или никакав отпор. Типичан пример војне интервенције јесте интервенција оружаних снага СССР-а и неких социјалистичких земаља чланица Варшавског уговора у Чехословачкој 1968. године[17].

Агресија је најдрастичнији облик војне кризе који настаје због сукоба непомирљивих интереса држава и коалиција, када оружане снаге државе или коалиције, са или најчешће без објаве рата, оружано нападају другу државу (ређе коалицију). Изузетно је изражен проблем правне регулативе агресије у међународним односима после Другог светског рата. Наиме, тај појам није регулисан Повељом УН из 1945. године. Бројни покушаји након доношења Повеље да се дефинише агресија углавном су били неуспешни.

Стална латентна војна опасност по глобални светски мир јесте трка у наоружавању, посебно *пролиферација оружја за масовно уништење*. Ова опасност нарочито долази до изражаја у условима рата између Русије и Украјине, који је почео 2022. године, а у који су се, на страну Украјине, умешале западне земље, на челу са САД.

2.1.3 Економски сектор безбедности

Економска снага је једна од кључних полуга укупне моћи сваке државе, то јест, економска и војна снага производе политичку моћ. Иако постоје и други чиниоци укупне моћи, економска моћ је неизостављив елемент свих пројекција те моћи. Изворно, према ставовима професора Бузана (1998), економски сектор безбедности поима се као „приступ ресурсима, финансијама и тржиштима неопходним за одржавање прихватљивог нивоа благостања и моћи државе“.

[17] У тадашњој социјалистичкој Чехословачкој, доласком Александра Дубчека на чело комунистичке партије и државе у јануару 1968. године започете су реформе и покушај увођења „социјализма са људским ликом" – увод у период скоро па романтичног назива Прашко пролеће. Руководство Совјетског Савеза било је против реформи и Прашко пролеће је угушено у ноћи између 20. и 21. августа, уласком трупа Варшавског пакта у Праг. Доступно на:https://www.bbc.com/serbian/lat/svet-53867079, 4. 7. 2024.

Наведеној Бузановој одредници економског сектора безбедности неопходно је додати податке о *енергетској безбедности*. Наиме**,** енергетска безбедност јесте кључна полуга економског сектора безбедности, тако да се у појединим теоријским радовима, али и званичним стратегијама, издваја чак и као посебан безбедносни сектор – *енергетска безбедност.* При томе, примарни аспект промишљања енергетске безбедности јесте располагање (доступност) енергентима. Шире посматрајући разне аспекте енергетске безбедности, *Азијско-пацифички центар за енергетику* (APERC) дефинише четири главне димензије енергетске безбедности: 1) расположивост, 2) приуштивост, 3) прихватљивост и 4) доступност (Ren & Sovecool, 2014).

Бери Бузан и сарадници (1998) из Копенхашке школе безбедности посебно се осврћу на аспекте економске безбедности, именујући их као: 1) способност производње добара и услуга за потребе одбране, 2) скопчано са првим, то је настојање другиx држава да осујете способност наведену у тачки један (бојкот, санкције…) или је помогну (подршка запада косовским снагама безбедности), 3) способност да се одржи ниво развоја потребан за унутрашњу безбедносну стабилност и међународни положај државе; 4) економска безбедност појединца, односно његов приступ храни, води, другим производима и запослењу и 5) глобална економска, социјална и еколошка стабилност.

До снажних поремећаја у економском сектору безбедности могу да доведу економске кризе. У најзначајније узроке међународних економских криза Миланко Зорић (2010) убраја:

1) „повећање производње и смањење потрошње, рецесија и други крупни поремећаји у светској привреди, те криза акумулације капитала и структуралне противречности начина производње,
2) монополски и олигополски положај и глобална доминација гигантских транснационалних корпорација (или мегакорпорација) и мултинационалних компанија и банкарске суперолигархије у светској привреди, као пут невојног освајања света и њихова снажна конкурентска борба,
3) систем неравноправних међународних економских (и политичких и геополитичких) односа и дубоке противречности између групе најразвијенијих капиталистичких земаља и земаља у развоју или неразвијених земаља;
4) крупни финансијски проблеми, снажни монетарно-валутни и берзански поремећаји, финансијски крах и хиперинфлација у неким великим и средњим земљама у развоју које располажу важним природним богатствима и изворима енергената и које имају значајан геоекономски положај у свету и ескалација тих унутардржавних и међудржавних криза у велике међународне кризе;
5) хегемонистички економски интереси и циљеви неких великих и регионалних сила, војних савеза и коалиција, борба за освајање или овлађивање изворима нафте и земног гаса и стратешких сировина у страним земљама и за контролу њихових цена и путева транспорта,

као и борба за освајање светског тржишта ради пласмана сопствених производа и услуга и истискивања конкурената;
6) погрешна макроекономска, монетарна и финансијска политика појединих великих држава или групе држава, неке регионалне економске организације или неке међународне економске институције и
7) негативан утицај економско-трговинске и укупне глобализације света по моделу диктираном из једног центра“ (стр. 301).
8)

2.1.4 Друштвени сектор безбедности

Изворно, истраживачи Копенхашке школе безбедности овај сектор именовали су као *социјетални сектор безбедности*. Принципијелно посматрано, социјетални сектор безбедности према Копенхашкој школи односи се на *колетивни идентитет друштва и појединих група унутар њега*, а мање на државу (Форца, 2024). С обзиром на то да ни *колективни идентитет* није експлицитно дефинисана категорија, то се у литератури више среће одредница да социјетални сектор нешто није, више него шта јесте. Тако, Филип Ејдус (2012) пише: „Социјетални сектор није *цивилна заштита*, на пример од природних непогода; није *социјална заштита и сигурност* за запосленост, здравље и не односи се на *физичку егзистенцију* грађана који живе у једној држави“ (стр. 178).

У својим каснијим радовима истраживачи Копенхашке школе су еволуирали ка конкретнијем одређењу социјеталног сектора безбедности. Тако, Бузан је тврдио да је колективни идентитет дефинисан традиционалним културним обрасцима. С друге стране, Оле Вивер (1993) има другачији приступ, тврдећи да се „социјетални сектор безбедности тиче великих самодовољних идентитетских група које су способне да се репродукују независно од државе“. Према његовом схватању, „идентитети који су најподеснији за мобилизацију и секуритизацију јесу етно-национални и религијски“ (стр. 23). У каснијим својим анализама, наведеним етно-националним и религијским групама Вивер (2008) је додао и „род“, односно специфичне друштвене групе унутар једне шире заједнице (раса, племе, сексуална оријентација и др). Заједно, пак, Вивер, Бузан и Де Вилде су идентификовали четири групе социјеталних претњи: *миграције, хоризонтална надметања, вертикална надметања и депопулизација* (Ејдус, 2012: 128).

Миграције представљају премештања популације из једног у друге крајеве света. Принципијелно, постоје добровољне и присилне миграције. По безбедност посебно су опасне присилне миграције, које се догађају услед ратова, природних несрећа, али и других услова који угрожавају животе већих група становништва и присиљавају их да

напусте своја пребивалишта. На пример, према подацима Високог комесаријата за избеглице (УНХЦР) за 2023. годину, у свету је око 117,3 милиона људи присиљено да напусти своја места пребивалишта. Од тога, 68% је интерно расељено (унутар државе), док је око 43,4 милиона лица изван својих земаља (https://www.dw.com/sr/svetski-dan-izbeglica-raseljavanje-dosti%C5%BEe-novi-maksimum/a-69418850).

Хоризонтална надметања, како их појашњавају истраживачи Копенхашке школе безбедности, представљају евидентну бојазан од утицаја страних култура на популацију унутар једне државе. С друге стране, *вертикална надметања* јесу реална опасност од сукоба друштвених група унутар једне државе, а најчешће се испољавају као сецесионизам. Типичан пример овог облика социјеталне претње јесте настојање албанске популације на Косову и Метохији да се одвоји од Републике Србије. Међутим, постоје сличне тенденције у бројним деловима Европе и света (Форца, 2024).

Депопулација је делом у непосредној вези са миграцијама и представља негативну последицу исељавања (емиграције) становништва неке државе, али не присилно, него добровољно (потрага за бољим животом). Међутим, до депопулације долази и природним путем, односно када је морталитет већи од наталитета у једној земљи. Кад је Европа у питању, њен југоисточни део, коме припада и Република Србија, склон је депопулацији, док је северозападни део под притиском повећања броја становника. Према истраживању 85% земаља југоисточног дела Европе има тренд депопулације, а 37% земаља северозападне Европе бележиће пораст становника (H-Alter, 2023).

Претходно описани аспект друштвеног сектора безбедности односи се на један његов део – *социјеталну безбедност*. Реч је о поимању друштва (*societal*) као референтног објекта безбедности. „Социјетална безбедност се односи на способност друштва да очува своје суштинске особине услед променљивих околности и упркос могућим или стварним претњама“ (Hough, 2004: 106). Ова безбедност је угрожена онда када заједница претњу доживи као претњу која угрожава њен идентитет. Идентитет је дефинисан као скуп идеја и пракси које одређене појединце идентификују као припаднике једне социјалне групе. „Нације су апстрактне, замишљене заједнице, а национални идентитет најзначајнији је референтни објекат социјеталне безбедности” (Андерсон, 1991).

Други аспект друштвеног сектора безбедности окренут је ка појединцу (*social*) и управо обухвата оне делове које је „избегавала“ Копенхашка школа:

запосленост/незапосленост, здравље, поштовање људских права; стандард живота; сиромаштво; заштита, лична безбедност и друге. С друге стране, у односу на безбедност појединца, говоримо и о заштити личних података сваке особе. Тако, професор Срђан Благојевић (2019) истиче:

> „Проблем управљања безбедношћу има више аспеката, што га чини веома комплексним. Што је обимнији и комплекснији софтвер који користи, повећава се и његова рањивост. Ову чињеницу користе хакери, злонамерни компјутерски стручњаци, те налазе ове осетљиве тачке и користе их у циљу личне промоције, остваривања користи или из пуке обести. Када говоримо о личним подацима, говоримо, у ствари, о појединцу који се тим подацима може идентификовати. У данашњем свету се прикупљају огромне количине личних података. Неке организације их користе за своје потребе, а неке их преносе трећим лицима из најразличитијих разлога. Овај тренд експоненцијално расте заједно са развојем сложених информационих технологија за обраду и анализу великих база података“ (стр. 25).

У складу с наведеним, говори се о *социјалној безбедности*. У овом домену најизразитије претње безбедности појављују се као разне врсте криминала, посебно организовани криминал и корупција, али и друге.

Оба аспекта друштвеног сектора безбедности, заједно посматрано, односе се на концепт људске безбедности, то јест 1) ширем поимању људске безбедности, на нивоу друштвених група и друштва у целини (*социјетет*) и 2) примарном поимању људске безбедности на нивоу појединца (*социјала*), које се мултипликује на друштво као целину.

2.1.5 Еколошки сектор безбедности

Постоје у литератури забележени ставови да је изворни творац сектора безбедности професор Бери Бузан (1991) највећу пажњу поклањао управо еколошком сектору, речима: „Ако нема здраве животне средине, неће бити ни нас“. Тако, према Бузану, референтни објект безбедности, у овом случају јесте *биодиверзитет* (*животна средина)*.

Међутим, у теорији нема консензуса о томе шта подразумева еколошка безбедност. Бројни аутори су се окушали у дефинисању тог појма, од чега ћемо издвојити нека виђења. Џон Бернет (John Barnett, 2001) под еколошком безбедношћу сматра „способност нације или друштва да одоли оскудицама животне средине, ризицима и нежељеним променама у животној средини или напетостима у евентуалним сукобима” (стр. 15). Елизабет Чалецки (Elizabeth L. Chalecki, 2002) еколошку безбедност дефинише као

„релативну безбедност јавности од еколошких опасности изазваних природним или људским деловањем“. У домаћој литератури, а на основу страних извора, Вера Арежина (2010) даје једну ширу дефиницију еколошке безбедности: „Еколошка безбедност подразумева веома сложен процес супротстављања угрожавању из било ког извора било које врсте и било које компоненте природне целине, укључујући и људско друштво, при чему се остварује неки степен заштићености од опасности по егзистенцију, потребе и интересе“ (стр. 172).

Колин Стивенс (Colin Stevens) као типичне примере угрожавања еколошке безбедности наводи: климатске промене, губитак биодиверзитета и загађење земље, воде и ваздуха (Форца и Жупац, 2025).

Дакле, еколошка безбедност је угрожена деловањем природе, али и несавесним деловањем човека. Професор Форца (2022) најчешће деловање човека на угрожавање животне средине убраја:

- „драстичне промене климе (велика оштећења озонског слоја и нагомилавање загађујућих материја у атмосфери које стварају ефекат стаклене баште),
- деградирање великих површина рударским и другим делатностима,
- угрожавање биодиверзитета са већ неповратно изгубљеним многим врстама;
- исцрпљивање ресурса и велика загађеност животне средине због њиховог трошења;
- непрекидно уништавање читавих шумских и других екосистема;
- немогућност да се савладају све веће количине опасног, отровног и осталих отпадних материја;
- оштећење људског здравља и појава нових болести;
- нагомилане количине нуклеарног и другог разорног оружја које би могле више пута да потпуно униште живот на планети;
- недостатак воде за пиће за 2/3 људи;
- проблем пренасељености, уз то недостатак хигијенског становања и недовољно хране за већи број људи на Земљи“ (стр. 209).

У оквир еколошког угрожавања нарочито су значајне последице које настају услед природних несрећа и катастрофа, какве су земљотрес[18], поплава[19], суша[20], шумски пожари[21], цунами[22] и друге.

[18] 1) Последице по животну средину: биолошке контаминације услед разарања водоводних и канализационих постројења и ремећења активности у комуналној хигијени; 2) Битне промене карактеристика станишта и значајних еколошких фактора - затрпавање језера, настајање водопада, промене токова река као последице катастрофалних земљотреса и друго. Шире у: **Цветковић, В., Милојковић, Б. и Стојковић, Д**. (2014). Анализа геопросторне и временске дистрибуције земљотреса као природних катастрофа. *Војно дело, 66*(2), *166-185*.

2.1.6 Оправданост секторског приступа безбедности

У овом питању намера је да се утврди оправданост коришћења секторског приступа безбедности, који је развила Копенхашка школа безбедности, у смислу његовог поимања као сегмента теоријског модела безбедносне аналитике. Као потврду исправности опредељења за секторски приступ безбедности, навешћемо примере из праксе, јер је чињеница да се идентификацијом изазова, ризика и претњи безбедности баве све државе, али и међународне организације.

„Почетком 21. века тадашњи генерални секретар УН Бутрос Гали, са групом дипломата, покушао је да утврди јединствену листу изазова, ризика и претњи којом се баве све владе држава у свету. Тако, према резултатима Панел-истраживања под називом *Безбеднији свет* (2002), идентификовано је шест група претњи којима се баве светске владе: 1) *економске и друштвене претње* (укључујући сиромаштво, заразне болести и економско уништавање), 2) *унутардржавни сукоби* (укључујући грађански рат, геноцид и друга масовна недела), 3) *међудржавни сукоби*; 4) *нуклеарно, хемијско и биолошко оружје*; 5) *тероризам* и 6) *међународни организовани криминал"* (Вилијамс, 2012: 46). Дакле, уочавамо да се идентификоване претње у целини односе на секторе безбедности, како их је утврдила Копенхашка школа безбедности.

С друге стране, чињеница је да све државе света идентификују изазове, ризике и претње по сопствену безбедност. Најчешће, идентификација изазова, ризика и претњи објављује се у документу који носи назив *стратегија националне безбедности*. Професор

---

[19] На пример: Велика поплава у Кини – 1931. године. Услед циклонских олуја десила се поплава у којој су се излиле три реке. Око 1.000 људи је изгубило живот у меоменту изливања река. Након тога, дошло је до појаве тифуса и колере, од којих је страдало око три милиона особа. Доступно на: https://www.prakticnaekologija.rs/2021/04/13/poplave-posledice-na-sredinu/, 4. 7. 2024.

[20] Еколошке последице се пре свега односе на нарушавање животне средине.

[21] Последице шумских пожара манифестују се дуги низ година након појаве пожара и то на: биолошку разноврсност (долази до губитка који је ненадокнадив); нестајање ретких, угрожених и рањивих биљних и животињских врста (чиме се утиче на смањење специјског и генетског диверзитета); промену пејзажа и лепоту предела (предеони диверзитет); земљиште (мењају се физичке и хемијске особине земљишта, као и микробиолошки састав); климу и микроклиму и водни биланс (грубо ремећење хидролошког режима, смањење залиха воде и појаве поплава). Шире у: **Цветковић, В., Милојковић, Б. и Стојковић, Д.** (2014). Анализа геопросторне и временске дистрибуције земљотреса као природних катастрофа. *Војно дело, 66*, (2), 166-185.

[22] Цунами је комбинација земљотреса и поплава изазваних великим таласима и померањима морске воде. Директне последице су примарно по људске животе, које се мере и десетинама хиљада погинулих (Јапан, 2011), као и економске штете, изражене у стотинама милијарди долара (Јапан, 2011). Секундарне последице, међу којима су и еколошке катастрофе, настају под дејством описаним за поплаве и земљотресе.

Форца је у својој монографији *Теоријски и упоредни аспект анализе стратегије националне безбедности Републике Србије* анализирао 33 стратегије националне безбедности страних држава и Републике Србије (Форца, 2022). Из те анализе изнећемо само примере како изазове, ризике и претње безбедности идентификују стратегије држава из окружења (Табела 13).

Табела 13. *Изазови, ризици и претње у стратегијама националне безбедности*

ИЗВОР	ИЗАЗОВИ, РИЗИЦИ И ПРЕТЊЕ БЕЗБЕДНОСТИ
Стратегија националне сигурности Републике Хрватске, 2017.	Оружана агресија (мало вероватна); Нерешена питања разграничења с појединим суседним државама; Политичко и обавештајно деловање према Хрватској од стране држава које су сукобљене с НАТО и ЕУ; Хибридно деловање; Тероризам (мало вероватан, али велике последице); Екстремизам појединаца и група унутар Хрватске; Корупција; Организовани криминал; Кибернетичке претње; Неповољни глобални економски трендови, Осетљивост на поплаве и природне несреће и пораст сиромаштва; Неповољна демографска структура; Енергетска зависност; Климатске промене; Нарушавање околине; Заостала минско-експлозивна средства; Природне и људским деловањем изазване несреће.
Стратегија националне безбједности Црне Горе, 2018.	Оружана агресија (мало вероватна); Тероризам и насилни екстремизам; Пролиферација конвенционалног и наоружања за масовно уништење; Сајбер претње ; Хибридне претње ; Организовани криминал; Угрожавање јавне безбедности; Угрожавање економске и енергетске безбедности; Илегалне миграције; Обавештајно деловање; Угрожавање или уништење елемената критичне инфраструктуре; Безбедност мора, подморја и морског дна; Природно и вештачки изазване несреће и катастрофе; Недостатак природних ресурса и деградација животне средине.
Резолуција о стратегији националне безбедности Републике Словеније, 2019.	Хибридне претње ; Информационо-сајбер претње ; Обавештајна делатност страних актера; Војне претње ; Кризна жаришта; Тероризам и насилни екстремизам; Недозвољене активности у области конвенционалног оружја, оружја за масовно уништење и нуклеарне и ракетне технологије; Тешки и организовани криминал; Илегалне миграције; Климатске промене; Глобални финансијски, економски, технолошки и друштвени ризици; Угрожавање јавне безбедности; Природне и друге катастрофе; Оскудица природних ресурса и деградација животне средине и Здравствено-епидемиолошке претње .
Стратегија националне безбедности Републике Србије, 2019.	Оружана агресија на РС; Сепаратистичке тежње у РС; Противправно једнострано проглашена независност територије АП КиМ; Оружана побуна; Тероризам; Пролиферација оружја за масовно уништење; Етнички и верски екстремизам; Обавештајна делатност страних субјеката; Организовани криминал; Наркоманија; Масовне илегалне миграције; Проблеми економског развоја РС; Проблеми демографског развоја РС; Епидемије и пандемије заразних болести,; Енергетска безбедност РС; Недовршен процес разграничења држава бивше СФРЈ; Елементарне непогоде и техничко-технолошке несреће; Климатске промене; Високотехнолошки криминал и угрожавање информационо-комуникационих система.

Извор: *Форца, 2022.*

У складу са наведеним примерима из праксе, односно приступом генералног секретара УН, као и у стратегијама националне безбедности држава (претходна Табела), може се закључити да појединачно идентификовани изазови, ризици и претње, кореспондирају генерализовано приказаним секторима безбедности, како их је утврдила Копенхашка школа безбедности. У том смислу, а посебно због тога што се ради о теоријском моделу безбедносне аналитике, опредељење за секторски приступ безбедности може се сматрати методолошки и сазнајно коректним.

Коректност опредељења за секторе безбедности додатно потврђују и следеће чињенице:

1) Хибридне претње су недвосмислено облик угрожавања држава у савременим међународним односима. Међутим, те претње не обухватају врло снажне облике угрожавања какви су природне несреће и катастрофе и пандемије и епидемије заразних болести.
2) Сектори безбедности обједињавају државоцентрични и друштвеноцентрични приступ безбедности.
3) Компоненте безбедности државе су спољна и унутрашња, заједно посматране као интегрална безбедност. Интегрална безбедност, имплицитно, акцептира се кроз секторе безбедности.

2.2 Процедуре рада аналитичара

Безбедносна аналитика је практична вештина заснована на науци (Форца и Аночић, 2018). При томе, процедуре које се користе у раду безбедносних аналитичара заснивају се на практичном раду. У практичном раду аналитички процеси се одвијају кроз више фаза и кроз устаљене процедуре. Оно што је значајно за праксу, а уједно и описано у литератури су обавештајни циклус (обавештајна аналитика) и полицијско-обавештајни модел (криминалистичко-обавештајна аналитика). С обзиром на то да су ове процедуре детаљније описане у првом делу, овде ћемо навести њихове основне карактеристике ради целовитог сагледавања теоријског модела безбедносне аналитике.

Обавештајна (војна) аналитика се одвија у оквиру обавештајног циклуса, о коме, у смислу фаза (корака) који га чине, постоје различита виђења. У домаћој обавештајној пракси , као и у НАТО обавештајној доктрини, кораци (фазе) обавештајног циклуса су: 1) издавање задатака (наређења), 2) прикупљање података, 3) производња обавештајних информација – аналитика и 4) достављање обавештајних информација корисницима. Дакле, фаза (корак) „производња обавештајних информација“ именован је као аналитика.

Пре него што дође до издавања задатка, постоје одређене околности из окружења које доводе до сазнања да постоји обавештајни проблем на који треба усмерити пажњу. Политичко руководство у сарадњи са обавештајним структурама усмерава рад обавештајних субјеката. Форца наводи да се фаза издавања задатака састоји од: 1) одлучивања о обавештајним захтевима, 2) планирања процеса прикупљања података, 3) издавања захтева и наређења за прикупљање података и 4) континуираног праћења продуктивности прикупљачких органа и агенција (Форца и Аночић, 2018). Ова фаза треба да резултира прецизно дефинисам обавештајним захтевима политичког и/или војног руководства и планом прикупљања података обавештајног руководства.

Наредна фаза обавештајног циклуса је она у којој обавештајне службе применом различитих обавештајних метода и коришћењем свих обавештајних извора прикупљају како сирове (необрађене) податке тако и оне које могу, а неретко и морају, бити хитно достављене политичком, војном или обавештајном руководству. Ова фаза подразумева прикупљање података из отворених (јавних) и тајних извора. Напретком у технологијама, посебно у области електронских комуникација, службе безбедности су почеле интензивно да се ослањају на прикупљање података пресретањем комуникација, где се не прикупља само садржај комуникација већ читав низ других података, попут, на пример, с ким је комуницирано и колико често, као и време, место и дужина трајања комуникације, који се најчешће збирно називају метаподаци. У ове податке спадају и они који се односе на употребу интернета и друштвених мрежа (Петровић, 2020).

Производња обавештајних информација – *аналитика* је трећа и кључна фаза у обавештајном циклусу. Ова фаза се често назива и фаза обраде података, где сирови податак или више њих након обраде може да постане аналитичка информација. Ово је, практично, први корак (фаза) обавештајне аналитике, као дела обавештајног циклуса. Принципијелно, овај корак (фаза) састоји се од следећих активности: 1) оцена поузданости извора и тачности податка, 2) разврставање и упоређивање података и информација и 3) слагање података и информација у базу.

„*Аналитичка информација* је више од информације, реч је о синтези података и информација који конституишу знање, с намером да се оно искористи за одређено (конкретно) поступање (потребу) корисника (на пример, решавање проблема, откривање потенцијалне прилике за деловање, избегавање проблема и сл.)“ (Ђурђевић и Милић,

2020: 90). Дакле, ова фаза обавештајног циклуса се завршава израдом обавештајног производа који може бити у различитим формама. „Продукти такве обраде су разни документи – обавештајне информације, анлитичке и динамичке обраде, стратегијске информације, процене и слично“ (Бошковић, 1996: 127).

Обавештајни аналитичар на разне начине утврђује вредност опипљивог и податка заснованог на уверењу. Разврставање и упоређивање података и информација јесте корак у обавештајној аналитици који следи након провере поузданости извора и тачности података-информација. Смештање података и информација у базу јесте корак обавештајне аналитике, након што су подаци разврстани и упоређени са претходним.

Закључивање и процењивање – анализа, тумачење и процена информација је кључна фаза (корак) обавештајне аналитике која треба да резултује обавештајно-аналитичким производом, који ће обавештајна служба да користи у свом раду и/или који доставља доносиоцима одлука у систему (националне) безбедности. У даљем, описаћемо неке практичне процедуре рада безбедносних аналитичара.

2.2.1 Intelligence-led policing (ILP) / Полицијско- обавештајни модел (ПОМ)

Примена полицијско-обавештајног модела је с временом еволуирала, тако што су га у пракси полицијске организације прилагођавале и развијале сходно својим потребама, због чега у савременим условима не постоји његова јединствена стандардизована форма. Упркос томе, суштина његове примене у раду полиције остала је непромењена, тако да подразумева подршку у доношењу одлука стратешких и оперативних управљачких група, кроз обједињене обавештајне функције и базе података из више различитих организационих јединица полиције, што доприноси усмеравању ресурса на приоритете дефинисане у стратешким и оперативним плановима.

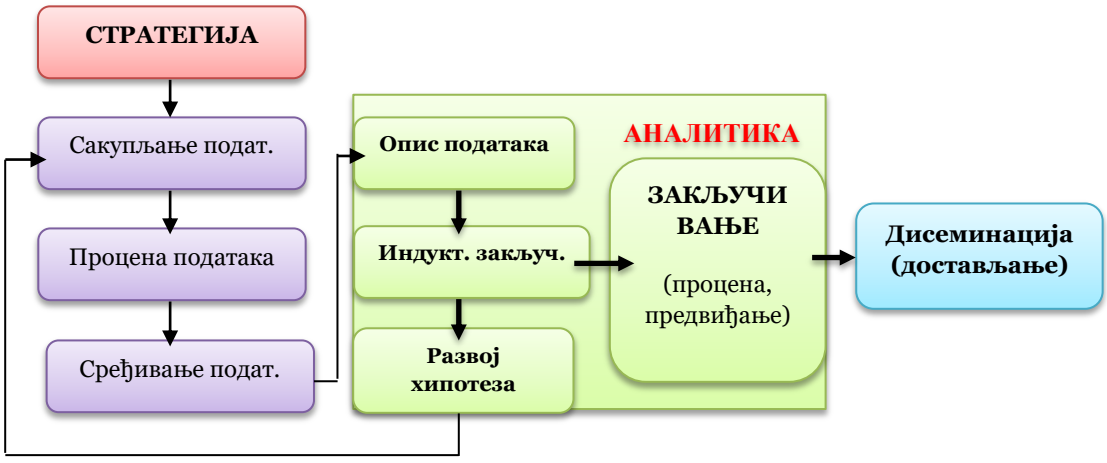
Такође, овакав модел претпоставља сарадњу различитих делова система безбедности једне државе. Дакле, податке морају да укрштају и размењују и војска и полиција и сви релевантни делови цивилног сектора (становништво, удружења, различите агенције, приватници итд.) како би могло да се делује проактивно у оперативном раду полиције, што јесте филозофија овог модела рада. Дакле, полиција не може да делује самостално, већ јој је потребна подршка и осталих сектора како би се дошло до кључних информација благовремено. Такође, инфромације се морају размењивати на различитим нивоима од

локалног до националног нивоа, а по потреби информације се морају размењивати и са другима путем међународних организација.

У делу ПОМ-а „криминалистичко-обавештајни послови“ најзначајнија фаза јесте *аналитика* (Слика18), која је описана у документима полиције и примењује се у пракси.

Слика 18. *Фазе криминалистичке аналитике*
Извор: *МУП Србије, 2017 (обрада ауторке дисертације)*

У раду крим-аналитичара у страним земљама користи се један практичан модел именован као ANACAPA (Слика 19). Овај модел практикован је и у раду полиције у Републици Србији.



Слика 19. *ANACAPA аналитички модел*

Извор: *Манојловић, 2008 (обрада ауторке)*

Аналитички процес (Слика 19) је серија активности или процедура које воде до најпрецизнијег и најнеоспорнијег закључка који се може извести из доступних информација. Информација је прикупљена, процењена и сређена (уређена и похрањена). Аналитички део процеса почиње повраћајем одговарајућих података и организовањем истог тако да је једноставнији за разумевање. Овај корак, **опис података,** помаже за идентификацију информација које недостају и у фокусирању на напоре за наредно прикупљање информација (назначено стрелицом од описа података до прикупљања података). Такође пружа темеље за примену индуктивног расуђивања у развијању једне или више хипотеза о кључним аспектима криминалне активности.

Хипотезе се тестирају понављањем циклуса прикупљања података, проценом података, сређивањем података, описом података и индуктивним расуђивањем. Сваки пут када се циклус понови, уже се фокусира на специфичне врсте информација које су неопходне да потврде или оповргну хипотезе и води ка добро подржаном изведеном закључку. Крајњи циљ процеса јесте да пружи такав изведени закључак који ће дати предвиђање или процену на основу којих се може поуздано деловати (Муратбеговић, 2014).

Процес (процедуре) рада безбедносних аналитичара су доста познате у теорији и пракси, те ћемо фокус ставити на методе и технике које аналитичари користе у том процесу.

2.2.2 Методе и технике у безбедносној аналитици

У склопу процедура приказаних у претходном питању, искуствено, постоји изузетно обухватан спектар метода и техника које се користе у разним врстама безбедносне аналитике. С обзиром на општеприхваћен став да је безбедносна аналитика струка (практична делатност) заснована на науци, то се и у њеној реализацији примењују и научне (методологија) и ненаучне методе (методика). Истакнуто је у претходном тексту, анализи појединих врста безбедносне аналитике, да се, када је реч о научним методама, предлаже употреба врло широког спектра тих метода. У разним државама класификација научних метода је различита, па је готово немогуће набројати све научне методе које се у

безбедносној аналитици користе. Стога, само као пример, наводимо како неки аналитичари из праксе виде примену научних метода у безбедносној аналитици (Табела 14).

Табела 14. *Научне методе у безбедносној аналитици*

ИЗВОР	НАУЧНЕ МЕТОДЕ
Форца Божидар и Аночић Бранислав, 2018.	Статистичка, компаративна, моделовање; дедукција; индукција; абдукција[23]; анализа; синтеза; посматрање; испитивање; прогностичке (Делфи, студија случаја); анализа садржаја; операциона истраживања.
Michael W. Collier, 2005.	Бејсианова (Bayesian) статистичка анализа, симулације, стабло вероватноће; процес аналитичке хијерархије; Делфи, алтернативне сценарије/будућности и „Локвудов аналитички метод за предвиђање"…
Даниловић Нељо, Манојловић Драган, Гајић Дејан, 2023.	1) Општенаучне методе, пре свега, хипотетичко-дедуктивна, статистичка и метода моделовања, 2) основне аналитичко-синтетичке методе сазнања и 3) остале методе за прибављање података, посебно метода испитивања, применом техника разговора (интервјуа) са информатором и методом посматрања, применом технике са и без учествовања у криминалном догађају, као и биографском методом.
Tyler Wall, 2024.	1. Квантитативне (статистичка, математичко моделовање), 2. квалитативне (анализа садржаја, студија случаја, испитивање у фокус групама), 3. општенаучне и логичке (анализа и синтеза, компаративна, хипотетичко-дедуктивна); 4. савремени приступи (2025): (Behavioral Analytics; предиктивна аналитика и мрежна анализа и граф модели).
Саша Мијалковић, Вера Арежина, 2024.	1. Квалитатовне методе (посматрање и интервју с фокус групама), 2) квантитативне методе (експеримент и посматрање) и 3) микс методе.
Даниловић Нељо, Манојловић Драган, 2024.	1. Општенаучне (хипотетичко-дедуктивна, статистичка, моделовање, аналитичко-дедуктивна и аксиоматска) и 2. методи за прикупљање података (посматрање, испитивање, експеримент, анализа садржаја, студија случаја и биографска метода).[24]

Извор: *Обрада ауторке дисертације*

У складу с наведеним, у даљем тексту примарно ћемо се осврнути на тзв. ненаучне (практичне) методе и технике, које се користе у разним врстама безбедносне аналитике.

[23] Термин „абдукција" потиче од латинске речи „abducere", што зачи „одвести", те се у филозофском речнику сматра као силогистички начин закључивања. Абдуктивни метод мишљења и закључивања подразумева поступак при коме се друга премиса третира као вероватна, док и прву премису треба узети са резервом. То подразумева да обавештајни аналитичар за сваки проблем истраживања поставља најмање две хипотезе као потенцијални одговор на истраживачко питање. Шире у: **Форца, Б., Аночић, Б.**, (2018), оп. цит., стр. 134.

[24] Биографска метода је посебна врста методе анализа садржаја. **Даниловић, Н., Манојловић, Д.**, (2024), *Аналитичка истраживања у безбедности,* Универзитет МБ, Београд, стр. 161.

На пример, у криминалистичкој аналитици неке од најчешће описиваних у литератури су: метода мрежне анализе, метода анализе телефонског регистра, метода анализе тока догађаја, метода анализе токова, метода визуелне криминалистичке анализе, метода анализе претње, метода анализе рањивости, метода анализе обрасца злочина и друге методе. Такође помињу се и метода предвиђања и симуловане истражне радње у криминалистици и десетине других метода (Шире у: Манојловић, 2008). Која ће се конретно метода користити у истрази зависи од природе предмета истраге, али и постављеног циља. Тако се, на пример, метода мрежне анализе најчешће примењује онда када треба истражити повезаност између различитих чланова једне криминалне организације, хијерархијску структуру или повезаност с другим организацијама и погодна је за истраживање мрежа нарко-мафије, организованог криминала, тероризма и слично.

„*Метода анализе телефонског регистра* подразумева приказ криминалистичко-аналитичких података из телефонских рачуна, записа и појединачних података регистра бројева. Ти криминалистичко-аналитички подаци односе се на шифре области и бројеве телефона који су позивани, време, датум, локацију, усмерење и трајање позива. Сви наведени подаци се похрањују у криминалистичко-аналитичкој бази података, како би се пружила аналитичка знања о телефонској комуникацији. Анализа телефонског регистра прихваћена је у пракси и законодавствима више земаља“ (Ђурђевић и Радовић, 2012: 327). Користи се у истрагама везаним за организовани криминал, криминал белог оковратника, насиља и слично.

Метода анализе догађаја се, на пример, користи када постоји низ догађаја који воде ка одређеној криминалној активности. Овом методом укрштају се различити подаци везани за различите догађаје, жртве, починиоце, временске и друге околности, како би се дошло до информација које недостају. Догађај може бити приказан у две различите форме графикона, као графикон тока догађаја или као временски низ. Графикон догађаја приказује след догађаја, тако да време догађаја и односи између повезаних догађаја јасно буду утврђени. Он представља неопходни аналитички алат код сложених предмета истраге и састоји се од кратког описа догађаја који се представља симболима, као што су кругови или правоугаоници. Опис догађаја треба да буде кратак, не дужи од три или четири речи.

- Повезивање линијама користи се ради представљања веза између догађаја. Представља пут, тј. низ догађаја у којима један догађај води ка другом.

- Стрелице на свакој линији показују редослед догађаја, тј. ток догађаја кроз време. Датум и /или време у погледу сваког догађаја повезани су на неки начин са описом догађаја, у оквиру симбола догађаја, близу симбола или су повезани са симболом (Ђурђевић и Радовић, 2012).

Методом анализе претњи утврђује се постојање претњи, док се методом анализе рањивости приказују информације о потенцијалним жртвама претње и идентификују области које могу да утичу на изложеност особа и објеката претњама. Тако се анализом претњи могу идентификовати терористичке претње, на пример, а метода анализе рањивости се може користити када је потребно, на пример, заштити личност која ужива одређени имунитет, јер се овом методом долази до слабости. Метода анализе образаца злочина се користи када треба истражити низ злочина који се понављају и тако даље.

„*Метода предвиђања* је посебно значајна за предиктивну функцију криминалистичке аналитике која треба да води спречавању кривичних дела која се још нису догодила, а њен основ лежи у обавештајној делатности. Такође, у оквиру истражних радњи, а тиме и у оквиру криминалистичке аналитике, може да се користи и једна специфична метода која се назива *симулованим истражним радњама.* Суштински (посебна), доказна симулована радња/послови/делтаности и тестирање интегритета су идентичне истражне методе које се заснивају на креирању надзираног, фингираног амбијента, са циљем да се у њему провери и/или утврди спремност одређеног лица на предузимање незаконите радње“ (Маринковић и Тасић, 2023: 50).

2.2.2.1 Сруктуриране технике аналитике

Колијер је након терористичких напада Ал-Каиде на објекте у Њујорку и Вашингтону написао текст који смо раније навели. У том тексту, Колијер (2005) тврди да „*оперативни аналитичари ЦИА не познају довољно методе и технике у раду*. У складу с наведеним, у САД је отпочела обухватна активност на бројним универзитетима и научним институтима да се утврди скуп научних метода и техника, као и програми оспособљавања, неопходни за доградњу и изградњу оспособљености безбедносних аналитичара.

У складу с претходно наведеним, а полазећи од тога да се савремени свет знатно променио у односу на хладноратовски период и да је улога обавештајне аналитике за доносиоце одлука данас значајнија него икада, те да је улога обавештајног аналитичара да да одговор на питање шта је оно што следи, а не шта нам је познато, Хауер и Персон

(2015) су у својој књизи обрадили више од педесет аналитичких техника. Као илустрацију, навешћемо само неке.

Технике се крећу од једноставнијих, које аналитичари могу и самостално да практикују, до оних компликованијих, које су погодније за групни рад попут брејнсторминга. Такође, неке од наведених техника су погодније за бизнис и финансије, док се друге могу користити у борби против тероризма и стратешким анализама.

Ови аутори на почетку сугеришу да постоје два начина на која могу да размишљају они који доносе одлуке. Један начин је брз, интуитиван и заснован на претходном знању и искуству и често се одвија несвесно. Због тога, иако је овај начин размишљања често ефикасан, он зна да буде и пристрасан. Други начин размишљања је аналтички, спор и заснован на емпиријским и квантитативним методама, а циљ овог начина размишљања је да се избегне пристрасност, што је посебно значајно у раду безбедносних аналитичара. Структурне анлитичке технике које они описују дају предност другом начину размишљања и имају за циљ да смање пристрасност и друге грешке које могу настати у ослањању на интуитивно размишљање.

„Циљ ових техника није да замене интуитивно расуђивање већ да омогуће један шири оквир за размишљање. Аналитичке методе су важне, али сам метод је далеко од довољног да осигура аналитичку тачност или вредност. Метод се мора комбиновати са стручношћу и радозналим и маштовитим умом. А ови, заузврат, морају бити подржани и мотивисани организационим окружењем у којем је анализа рађена“ (Heuer & Pherson, 2015: 28).

„Разне истражне комисије које су пратиле изненађење терористичким нападом од 11. септембра 2001, а затим погрешне анализе о ирачком поседовању оружја за масовно уништење, повећале су притисак за више алтернативних прилаза обавештајној анализи“. (Исто, 30) С временом су се, наравно, ове технике развијале и унапређивале у правцу мултисекторске сарадње између различитих актера, али и кроз технолошко увезивање подржано савременим софтверима. „Отприлике половина описаних техника овде је претходно уграђена у материјалаима за обуку које користе Одбрамбена обавештајна агенција, Канцеларија за Обавештајно-аналитичко одељење у Министарству унутрашње безбедности или у другим обавештајним агенцијама“ (Исто, 32).

Структурне технике аналитике ови аутори групишу у осам фамилија и то на следећи начин:

- распадање и визуализација (decompozition and visualization),
- генрисање идеја (idea generation),
- сценарији и индикатори (scenarios and indicators);
- стварање и тестирање хипотеза (hypothesis generation and testing);
- процена узрока и ефеката (assesment of cause and effect);
- анализа изазова (challenge analysis);
- менаџмент конфликата (conflict management) и
- подршка одлукама (decision support).

„Аутори сматрају да сви аналитичари треба да буду обучени да користе основне технике о којима се овде дискутује јер су често потребне и широко применљиве у различитим типовима анализа – како у стратешким и тактичким анализама, обавештајном и криминалистичком ангажовању, тако и за сајбер и бизнис анализе“ (Heuer & Pherson. 2015: 51). Приказаћемо неке од поменутих техника које су и сами аутори издвојили.

1) Структурни брејнсторминг (Structured brainstorming)

Структурни брејнсторминг спада у групу техника које се називају генератори идеја и подразумева постојање групе и тимски рад аналитичара. Тим аналитичара је обично ефективнији него појединац у стварању нових идеја или у синтези више већ постојећих идеја. Ово је можда и најчешће коришћена техника у раду америчких обавештајних аналитичара, која се углавном примењује на почетку аналитичког процеса за подстицање релевантних информација или увида из мале групе стручних аналитичара. Не односи се само на окупљање групе и њихову дискусију већ постоје правила и процедуре који се морају испоштовати. Циљ овакве групе може бити да направи листу релевантних променљивих, хипотезе, кључне актере и томе слично.

Пракса је показала да се највећи ефекат постиже онда када постоји могућност записивања или снимања самог процеса како би постојала могућност и касније допуне резултата брејнсторминга. Забелешке овакве врсте морају бити по унапред припремљеној форми и такве да буду разумљиве свим учесницима сесије. Такође, постоји могућност и виртуелног брејнсторминга, када није могуће због географске удаљености или других разлога групу окупити да сарађује лицем у лице.

„Поента брејнсторминга је да се што више идеја изнесе и да сваки члан групе има слободу да изрази своје идеје, без обзира на функцију и позицију коју има у обавештајној служби. Такође, постоји облик брејнстормига који се фокусира више на постављање питања него на давање одговора. Питања почињу речима: ко, шта, како, када, где и зашто. Мозгањем сваке од ових речи, једне по једне, генерише се што више питања о истраживању одређене теме“ (Heuer & Pherson, 2015: 121).

„Брејнсторминг обично излаже аналитичара већем спектру идеја и перспектива него што би он могао да генерише сам, а ово проширење ставова обично резултира бољим аналитичким производима. Да би био успешан, брејнсторминг мора бити фокусиран на одређени проблем и генерисање коначног писаног производа. Структурни брејнсторминг је техника која захтева модератора, делимично и зато што учесници не могу да разговарају током брејнсторминг сесија“ (Heuer & Pherson, 2015: 123).

„Модератор или вођа групе треба да представи фокално питање, објасни и спроведе основна правила, држи састанак на правом колосеку, стимулише дискусију постављајући питања, бележи идеје и резимира кључне налазе. Учесници треба да буду охрабрени да изразе сваку идеју која им се појави у главу. Чак и идеје које су изван могућег, јер могу да стимулишу друге идеје, које су изводљивије. Група би требало да има најмање четири и не више од дванаест учесника. Оптималан број је од пет до седам учесника, а ако има више од дванаест људи, групу би требало поделити на две“ (Исто, 124).

Постоје правила која је неопходно испоштовати како би се ова техника спровела адекватно:

- Пожељно је да се тема која је у фокусу брејнсторминга најави унапред и да постоји могућност достављања предлога и идеја и пре саме сесије.
- Унапред треба испланирати време сесије и узети у обзир да је потребно око сат времена да се учесници сместе и опусте како би се дошло до заиста креативних идеја.
- Ниједна идеја се не сме критиковати, колико год била неуобичајена или неизводљива.
- Само једна особа може говорити, а сваки учесник би требало да добије прилику да говори.
- Потребно је укључити аутсајдере, то јест људе који немају исто знање и перспективе везано за тему о којој се дискутује у односу на остатак групе.
- Потебно је пратити дискусију и забележити значајније резлтате.
- На крају сесије треба сумирати закључке и то доставити свим учесницима како би могли и касније да их допуне.

Брејнсторминг се обично користи у идентификовању потенцијалних осумњичених или за проналажење различитих путева истраге. Ова техника се може поново користити касније, у аналитичком процесу, како би се тим извукао из „аналитичке колотечине“, тако

што стимулише креативније размишљање које може резултирати новим траговима или новим правцима у истрази.

2) *Матрица унакрсног утицаја (Cross-impact matrix)*

„Ако брејнсторминг идентификује листу релевантних променљивих, покретачких снага или кључних играча, следећи корак би требало да буде стварање унакрсне матрице која се користи као помоћ групи да визуализује, а затим дискутујте о односу између сваког пара променљивих, покретачких снага или играча. То је једноставна, али ефикасна вежба учења која је нова за већину обавештајних аналитичара“ (Heuer & Pherson, 2015: 51). „Помаже аналитичарима да се носе са сложеним проблемима када је ‚све везано за све остало'. Коришћењем ове технике аналитичари и доносиоци одлука могу систематски да испитају како сваки фактор у одређеном контексту утиче на све друге факторе за које се чини да је повезан“ (Исто, 136).

Пожељно је да се ова техника користи на почетку пројекта, када се група аналитичара упознаје са проблемом и покушава да посложи комплексну ситуацију. Такође, ова техника може да се користи када је ситуација која је предмет аналитике стабилан, али је потребно да се прате различити фактори, који могу да угрозе ту стабилност или када се деси изненадни догађај, где се јавља потреба да се процене све његове импликације. Заправо, матрица унакрсног утицаја је користан алат који се може применити у неком тренутку у скоро свакој студији која настоји да објасни актуелне догађаје или прогнозира будуће исходе.

Ова техника функционише тако што окупите групу аналитичара који су упућени у различите аспекте теме. Група треба да сачини листу променљивих (варијабли) или догађаја који би вероватно имали неки ефекат на питањ које се проучава. Координатор пројекта затим креира матрицу и ставља листу променљивих или догађаја на левој страни матрице и исте променљиве или догађаје на врх. Матрица се затим користи за разматрање и записивање релације између сваке променљиве или догађаја и сваке друге променљиве или догађаја. „На пример, да ли присуство променљиве 1 повећава или умањује утицај променљивих 2, 3, 4 итд.? Или, да ли појављивање догађаја 1 повећава или смањује вероватноћу догађаја 2, 3, 4 итд.? Ако једна променљива утиче на другу, позитивна или негативна величина ефекта се може забележити у матрицу уношењем великог или малог

‚+' или великог или малог ‚–' у одговарајућој ћелији (или тако што уопште не прави ознаке ако нема значајаног ефекта). Терминологија која се користи за описивање сваког односа између пара променљивих или догађаја је да се он ‚побољшава', ‚инхибира' или ‚невезано'" (Heuer & Pherson, 2015: 137).

Одређене комбинације између варијабли могу да укажу на то да може доћи до изненађујуће брзих промена и такође оне могу омогућити да се правци таквих промена предвиде. На Слици 20 је приказан пример матрице унакрсног утицаја.

	Variable 1	Variable 2	Variable 3	Variable 4	Variable 5	Variable 6
Variable 1			+		−	
Variable 2			-	+	+	+
Variable 3	+	-		+		-
Variable 4		+			+	-
Variable 5	−	+		+		
Variable 6	-	+	−	-	-	

Variables 2 and 4 in the cross-impact matrix above have the greatest effect on the other variables, while variable 6 has the most negative effect.

Direction and magnitude of the effect:
+ strong positive
+ positive
neutral
- negative
− strong negative

Слика 20. *Пример матрице унакрсног утицаја аутора Хауера и Персона*

Извор: *Ричардс & Рандолф, 2015.*

3) Провера кључних претпоставки (Key Assumptions Check)

Провера кључних претпоставки спада у групу техника која се назива процена узрока и ефеката. Аналитичка процена је увек заснована на комбинацији доказа и претпоставки, а ово је једна од најчешће употребљаваних техника која захтева да аналитичари експлицитно набрајају и доводе у питање најважније радне претпоставке које се односе на њихову анализу.

„Свако објашњење тренутних догађаја или процена будућег развоја захтева тумачење непотпуних, двосмислених или потенцијално обмањујућих доказа. Да би попунили те празнине, аналитичари обично праве претпоставке о стварима као што су релативне политичке снаге, намере или способности друге земље, начин на који владини процеси обично функционишу у тој земљи, веродостојност кључних извора, валидност претходних анализа на исту тему, присуство или одсуство релевантних промена у контексту у којем се активност дешава“ (Heuer & Pherson, 2015: 52).

Ова техника се спроводи углавном на почетку аналитичког процеса. У неким случајевима, уколико није урађена на почетку процеса, може се спровести и касније, пре доношења и достављања закључака. Чак је понекад и пожељно уколико је ова техника урађена на почетку процеса да се понови пре састављања извештаја да би се проверило да ли су претпоставке и даље на месту или би их требало мењати.

„Процес спровођења провере кључних претпоставки је релативно концептуално једноставан, али често изазован у пракси. Један од изазова је то што аналитичари који учествују морају да буду отворени за могућност да би могли да погреше. Оно што помаже је да се у овај процес укључи неколико високоцењених аналитичара, који су генерално упознати са темом, али немају претходну посвећеност било ком скупу претпоставки о питању које је по среди. Треба имати на уму да се многе ‚кључне претпоставке’ претворе у ‚кључне неизвесности’ (Heuer and Pherson, 2015: 228).

Када окупљена група аналитичара састави листу претпоставки, треба поставити следећа питања:

- Зашто сам уверен да је та претпоставка тачна?
- У којим околностима би та претпоставка могла да буде неистинита?
- Да ли је то могла да буде истина у прошлости, али да данас више не буде истина?
- Колико је поуздано да је та претпоставка валидна?
- Ако се испостави да је неважећа, колики би то утицај имало на анализу?

Након одговора на ова питања, претпоставке се сврставају у једну од следећих категорија:

- У суштини солидно.
- Коректно, са неким мерама предострожности.
- Неподржано или упитно – „кључне неизвесности“.

Након тога врши се ревизија листи претпоставки, где се одбацују оне претпоставке које нису одрживе. Такође, након овог процеса треба размотрити да ли кључне неизвесности отварају потребу за поновним прикупљањем података и покретањем новог аналитичког процеса везаног за нову тему.

4) Индикатори (Indicators)

„Индикатори спадају у групу техника које се називају *сценарији и индикатори*. Индикатори су приметне или потенцијално приметне радње или догађаји који се прате да би се открила или проценила промена током времена. На пример, они се могу користити за мерење промена према непожељном стању, као што су политичка нестабилност, предстојећа финансијска криза или предстојећи напад. Индикатори такође могу да укажу на пожељно стање, као што су економске или демократске реформе. Посебна вредност индикатора је у томе што стварају свест која припрема ум аналитичара да препозна најраније знаке значајних промена који би се иначе могли занемарити. Међутим, развијање ефективног скупа индикатора је теже него што изгледа“ (Heuer & Pherson, 2015: 52).

Индикатори се често користе заједно са техником сценарија и њихов задатак је да укажу на то који сценарио има највећу вероватноћу да се оствари. Ова техника се користи како би аналитичари успели да препознају рана упозорења за неки будући догађај. Такође могу да се користе и као потврда неке постојеће опсервације.

„Индикатори се могу пратити да би се добили тактичка, оперативна или стратешка упозорења о неком будућем развоју који би, ако би до њега дошло, имао велики утицај. Идентификација и праћење индикатора су основни задаци анализе, јер су главно средство за избегавање изненађења. Класична примена предиктивних индикатора је тражење раног упозорења непожељних догађаја, као што је војни напад или нуклеарна проба стране земље. Такође се користе за мерење промена тачака ка непожељном стању, као што је политичка нестабилност или економско успоравање или ка пожељном стању, као што су економске реформе или потенцијал за раст тржишта. Аналитичари могу да користе ову технику кад год је потребно праћење одређене ситуације за надгледање, откривање или евалуација промене кроз време“ (Heuer & Pherson, 2015: 170-171).

Код ове технике потребно је прво направити листу индикатора. Затим је потребно проверити листу и одбацити индикаторе који су дуплирани или слични. Потом се сваки индикатор који је остао на листи преиспитује кроз пет критеријума: да ли постоји могућност њихове опсервације и прикупљања, да ли је валидан, поуздан, стабилан и да ли је јединствен. Кључно је, дакле, да индикатори могу да се мере и посматрају у будућности, као и у садашњости и да се односе само на мерење једне ствари (појма). Напослетку се врши мониторинг или праћење индикатора, како би се уочили евентуални промене и одступања. Вредан индикатор је онај који кроз време није само компатибилан са једним сценарием или хипотезом, већ је супротан са свим осталим сценаријима или хипотезама који су креирани.

„Свака листа индикатора која се користи за праћење да ли се нешто десило, дешава се или ће се десити подразумева бар један алтернативни сценарио или хипотезу: да се то није десило, да се не дешава или да се неће десити. На пример, размотрите индикаторе противникове припреме за војни напад, где могу постојати три хипотезе: нема напада, напада и лажна намера да нападне са циљем присиљења на повољан споразум. Скоро сви показатељи скорог напада такође су у складу са хипотезом о нападу. Аналитичар мора да идентификује индикаторе способне за дијагностиковање разлике између истинске намере напада и намере напада. Мобилизација резерви је такав дијагностички индикатор. Толико је скупа да се обично не предузима осим ако не постоји јака претпоставка да ће резерва бити потребна“ (Heuer & Pherson, 2015: 174).

5) Анализа конкурентских хипотеза (Analysis of Competing Hypotheses)

Анализа конкурентских хипотеза спада у групу техника које се називају стварање и тестирање хипотеза. Научни процес подразумева посматрање, категоризацију, формулисање хипотеза и потом њихово тестирање. Генерисање и тестирање хипотеза је суштина функционисања структуриране анализе. Потенцијална објашњења прошлих или будућих догађаја су хипотезе које треба доказати прикупљањем и обрадом података. Може се рећи да се у овом процесу примењује научни метод у анализи обавештајних података.

Ова техника захтева да аналитичари почну са низом вероватних хипотеза, а не са једном највероватнијом хипотезом. Аналитичари затим узимају сваку релевантну

информацију, једну по једну и процењују њену доследност или недоследност са сваком хипотезом. Идеја је да се оповргну хипотезе уместо да се потврде (Heuer & Pherson, 2015). Највероватнија хипотеза је она којој се најмање информација супротставља, а не она која има највише информација које јој иду у прилог.

Анализа конкурентских хипотеза је примерена за скоро сваку анализу где постоје алтернативна објашњења за оно што се десило, што се дешава или ће се вероватно десити. Користи се када је пресуда или одлука толико важна да не можете себи да приуштите да погрешите. Користи се када вам осећај у стомаку није довољно добар, а када вам је потребан систематски приступ да се спречи да будете изненађени непредвиђеним исходом. Користи се за контроверзна питања, када је пожељно идентификовати прецизне области неслагања и оставити ревизорски траг да су релевантне информације разматране и како су различити аналитичари дошли до својих различитих закључака. Посебно је ефикасна када постоји снажан проток података за апсорбовање и процену. На пример, погодан је за решавање питања о техникалијама хемијских, биолошких, радиолошких и нуклеарних арсенала, као што су: „За који систем наоружања је овај део највероватније увезен?“ или „Који тип ракетног система Земља X увози или развија?“ (Heuer & Pherson, 2015).

Иако ова техника не изискује пуно времена за спровођење (довољан је један дан припреме и један дан за спровођење), ипак је потребна много већа ментална агилност од уобичајене праксе тражења доказа који поткрепљују једну хипотезу за коју се већ верује да је највише вероватна.

6) Шта-ако анализа (What-If Analysis)

У спровођењу шта-ако анализе, аналитичар замишља да се десио неочекивани догађај и онда анализира како је то могло да се деси и разматра потенцијалне последице. Овакав вид вежбања ствара свест која припрема аналитичара да препозна ране знаке значајне промене и може да омогући доносиоцима одлука да планирају унапред за ту непредвиђену ситуацију. Ово може бити тактички начин да се доносиоцима одлука укаже на могућност да су можда погрешили. Ова техника би требало да буде у алату сваког аналитичара. То је важна техника за обавештавање доносилаца одлука о догађају који би

могао да се деси, чак и ако се чини мало вероватно у овом тренутку. Најприкладније је када је нешто од следећих услова присутно:

- Ментални модел је усађен у аналитичара или заједницу корисника да се одређени догађај неће десити.
- Питање је веома спорно или унутар аналитичке заједнице или међу доносиоцима одлука и нико се не фокусира на то какве акције треба да буду разматране да би се спречио овај догађај.
- Постоји уочљива потреба да се други усредсреде на могућност да се овај догађај може заиста десити и да се размотре последице ако до тога ипак дође.

„Шта-ако анализа је логичан наставак након провере кључних претпоставки која идентификује претпоставку која је од критичног значаја за важну процену, али о којој постоји нека сумња. У том случају, у шта-ако анализи може да се замисли да је супротно од ове претпоставке тачно. Анализа би се онда фокусирала на то како би могло да дође до овог исхода и какве би биле последице“ (Heuer &d Pherson, 2015: 270).

Ову технику може да користи аналитичар као појединац, али је као и све друге технике погоднија и плодоноснија у тимском раду или групи. Сама метода укључује и елементе других техника попут сценарија или креирања индикатора.

У овом раду су приказане само неке од техника како би се уочио оквир рада америчких обавештајних аналитичара. На основу онога што су поменути аутори изнели може да се закључи да су ово тенике које стимулишу иновативно размишљање, изван кутије, да су погодне за самосталан али и групни рад, с тим да је групни рад увек плодоноснији и да је кључна ствар код аналитичких техника и алата предвидети будуће догађаје на основу постојећих података.

Оно што су Хауер и Персон изнели у својој књизи не осликава детаље рада обавештајних аналитичара у САД, али даје један оквир о томе које би вештине требало да има обавештајни аналитичар, уз напомену да се ове технике могу научити и савладати кроз обуке, а једном кад их савлада аналитичар ће увек моћи да их користи уз мало уложеног времена. То даље имплицира да адекватан аналитички процес ипак захтева обучене и припремљене аналитичаре, што није или је ретко пракса у обавештајним службама.

Примарни задатак безбедносне аналитике јесте да обрађује податке и информације како би креирала обавештајни производ који ће помоћи државним руководиоцима у процесу доношења одлука. Међутим, сам аналитички процес умногоме зависи од

окружења и околности у којима се спроводи. „Постоји широк спектар етикета које би се могле прикачити обавештајним аналитичарима и које сугеришу подједнако широк спектар вештина и атрибута потребних онима који су запослени као аналитичари“ (Corkill et al., 2015). Тако треба поменути и групу аутора са Безбедносног истраживачког института из Аустралије (Security Research Institute at Edith Cowan University, Perth, Australia) која је направила табелу вештина и атрибута безбедносних аналитичара анализирајући постојећу литературу (Табела 15).

Табела 15. *Компарација особина безбедносних аналитичара по различитим ауторима*

АУТОР	**СПОСОБНОСТИ, ВЕШТИНЕ, АТРИБУТИ И КАРАКТЕРИСТИКЕ**	**ОКРУЖЕЊЕ**
(Clauser, 2008; Clauser & Weir, 1976)	**Карактеристике:** способност расуђивања, тачност, интелектуална искреност, отвореност, скептицизам, одвојеност, стрпљење, марљивост, истрајност, машта.	Национална безбедност
(Katter et al., 1979)	**Карактеристике**: разумевање сложених концептуалних модела, генерисање концептуалних модела, знање, памћење, ментална флексибилност.	Војска
(Fischl & Gilbert, 1983)	**Атрибути:** способност расуђивања на високом нивоу, индуктивно резоновање,интелектуална флексибилност, вештина писања, меморија, интелектуална радозналост,намерност, међуљудске вештине, мотивација за постигнућима,самодисциплина, истрајност.	Одбрана
(Schneider, 1995)	**Атрибути:** интелектуална радозналост, памћење, брза асимилација информације, упорност, доношење пресуда **карактеристик**е: широк спектар интересовања, развијена истраживачка способност, искуство, иницијатива самоуправљање, дисциплиновано, интелектуална храброст **вештине**: писање вештине, вештине усмене комуникације.	Спровођење закона
(Wing, 2000)	**Карактеристике:** знање, предвиђање, радозналост, иновација, одлучност, интуиција, логика, машта, надахнуће.	Војска
(Wolfberg, 2003)	**Атрибути:** иновација, синтеза, учење, испитивање, образац препознавање, прилагођавање неизвесности, визуелно размишљање, експериментирање, метафоре, нелинеарно систематско размишљање.	Национална безбедност
(Moore, Krizan & Moore, 2005)	**Способности**: комуникација, сарадња, размишљање, **Карактеристике**: незасито радознао, самомотивисан, фасциниран слагалицама, изложен аха размишљању, похлепно посматра, читапрождрљиво, заузима променљиве перспективе,ствара креативне везе, разигран, осећај за хумор, осећајза чудо, интензивно се концентрише, **Знање**: циљ, заједница, политика, купац, вештине ресурса: критично резоновање, писменост, рачунарска писменост, страни језик, истраживање, манипулација прикупљањем информација, пројектно управљање, визуелизација.	Национална безбедност
Allen, D. M. (2008).	**Атрибути**: редослед информација, препознавање образаца, образложење, **Вештине**: техничка стручност, циљно знање, аналитичке технике, претражне и организационе способности, способност синтезе података, индуктивно резоновање, изражавање идеја.	Одбрана

(Quarmby & Young, 2010)	**Атрибути:** комуникација, сарадња, критичко размишљање, **Вештине:** креативност, стручност, процесна експертиза, дисциплинска стручност, генеричко знање.	Усаглашавање и управљање
(Richards, 2010)	**Вештине:** критичко размишљање, креативност, расуђивање, комуникација.	Национална безбедност
(Evans & Kebbell, 2011)	**Атрибути:** размишљање, коминикација.	Спровођење закона
Corkill, (UnPub)	**Атрибути:** способност дијагнозе и контекстуализације проблема, комуникација, самосвест.	Спровођење закона

Извор: *Коркил и сар., 2015.*

2.3 Стандарди и стандардизација

Трећи значајан сегмент теоријског модела безбедносне аналитике јесу *стандарди и стандардизација.,* Стандарди и стандардизација обухватају секторе безбедности и процес рада аналитичара.

Стандард, у општем смислу, дефинише се као критеријум и норма. Стандард је поновљиви, усаглашени, договорени и документовани начин на који је потребно нешто радити. Стога, стандарди садрже техничке спецификације и друге прецизне критеријуме дизајниране да се доследно користе као правило, смерница или дефиниција. Помажу у поједностављењу живота и повећању поузданости и ефикасности многих добара и услуга које користимо. „*Стандард* се, уопште, у документима међународних организација одређује као документ којим се утврђују захтеви, спецификације, правила, смернице или карактеристике које треба конзистентно следити и испунити да би се обезбедило да материјал, производи, процеси, услуге, заиста могу служити за њихову основну намену. Стандарди треба да се заснивају на провереним резултатима науке, технологије и искуства, а ради постизања оптималне користи за друштво" (Драгишић и Радојевић, 2014). Готово је немогуће побројати све врсте стандарда који се утврђују у разним областима[25].

У основи, *стандардизација* процеса описује успостављање скупа правила која регулишу начин на који људи у организацији треба да испуне одређени задатак или низ задатака. Тако, најпознатији вид стандарда су ISO (International Organization for

[25] На пример, ако узмемо само стандарде из области безбедности поризвода, у Србији је донет *Правилник о утврђивању листе српских стандарда у заштити безбедности производа*. Тај правилник обухвата 73 српска стандарда у заштити безбедности производа која су усклађена са европским стандардима у тој области. Види: *Службени гласник РС,* бр. 47/2023.

Standardization) стандарди. У том смислу, стандардизација је оквир споразума кога се морају придржавати све стране у организацији (компанији) како би осигурале да се сви процеси који су повезани са стварањем (призводња, услуге и др.) одвијају у складу са постављеним смерницама (*Службени гласник РС,* бр. 47/2023).

На пораст свести о значају доношења међународних стандарда из области безбедности утицали су пораст броја, сложености, непредвидивости и последица кризних и ванредних ситуација у свету: тероризам, елементарне непогоде, техничко-технолошке несреће и катастрофе итд. Осим развијања система раног упозорења, јавно-приватног партнерства и мреже за ублажавање последица кризних ситуација, евидентна је потреба да се применом стандарда омогући заштита профита компанија и наставак пословних активности у условима изазваним кризама. Међународни стандарди из домена друштвене безбедности, које су до сада донела и усвојила национална тела за стандардизацију, покривају углавном области управљања у ванредним ситуацијама и континуитетом пословања, а у последње време област стандардизације простире се и на остала питања безбедности лица, имовине и пословања: унутрашња безбедност од разних облика терористичког и криминалног угрожавања, спречавање превара, приватна безбедност.

Међу најпознатије ISO стандарде убрајају се:

- Квалитет: ISO 9001,
- Заштита животне средине: ISO 14001,
- Енергија: ISO 50001;
- Безбедност и здравље на раду: ISO 45001, SCC;
- Информациона безбедност: ISO 27001;
- Управљање кризним или ванредним ситуацијама: ISO 22301;
- Управљање ризицима: ISO 31000 и бројни други (Форца и Жупац, 2025).

У складу са наведеним међународним стандардима, у Србији се доносе српски стандарди (SRPS) за конкретну област. Тако, на пример, само за стандард у области безбедности информација ISO 27001 у Србији је донето 25 српских стандарда (https://iss.rs/sr_Cyrl/project/show/iss:proj:104420).

С обзиром на то да безбедносна аналитика не функционише као јединствена делатност, већ се одвија у оквиру својих врста (обавештајна, криминалистичко-обавештајна и др.), може се закључити да не постоје јединствени стандарди за безбедносну аналитику као целину. У том смислу, као примери за изградњу стандарда

теоријског модела безбедносне аналитике послужиће утврђени стандарди у појединим секторима безбедности, односно у моделима рада аналитчара.

2.3.1 Стандарди у појединим секторима безбедности

Генерално, примена ISO стандарда би требало да олакша одрживи развој на локалном, државном па и глобалном нивоу. У том смислу стандардима се инсистира на одређеним процедурама и утврђеним параметрима како би се на глобалном нивоу подигао квалитет живота у економском, социолошком и еколошком погледу. Одређени стандарди имају за циљ да олакшају живот за све становнике планете, али се они, нажалост, не поштују једнако у свим земљама. Безбедност као изузетно значајна област за функционисање државе у савременим оквирима није довољно стандардизована, али се стандарди у овој области могу посматрати кроз секторски приступ. Тако имамо, на пример, економску, људску и еколошку безбедност, где постоје утврђени стандарди.

2.3.1.1 Стандарди у економској безбедности

„Економски односи који се успостављају у процесу производње и расподеле, као најважнији друштвени односи, одређују друштвено и политичко уређење земље, квалитет живота становништва, степен развоја националног система безбедности, економску и политичку моћ земље у међународним односима, што их чини битном детерминантом националне безбедности“ (Дашић и Тркља, 2017: 312). Када је у питању економска безбедност, међународни систем стандардизације може умногоме допринети подизању општег квалитета живота људи. Међународни стандарди у области економије промовишу одрживи развој и продуктивно запошљавање уз поштовања одговарајућих услова рада и права радника. Значајни су стандарди који се односе на област банкарства, финансијског пословања и финансијских услуга.

Посебну пажњу треба обратити на ISO 22301 (Безбедност и отпорност – Систем менаџмента континуитетом пословања – Захтеви). Његова примена значајно доприноси економској стабилности заједнице. Припремљеност за суочавање са незгодама које могу утицати на ток процеса, али и опстанак ентитета, јесте добар мотив за примену

организационих принципа пословања, који су подлежни оцењивању (оверавању) независних тела. Истовремено, ако размишљате стратешки, пословни систем ће инсистирати на примени принципа пословне стабилности, отпорности система на сметње, што значи бољи безбедносни посао. У овом контексту постоји додатни мотив за компаније да се придржавају принципа који су саставни део ISO/TC 22318 (Друштвена безбедност – Систем менаџмента континуитетом пословања – Смернице за континуитет ланца снабдевања), чиме се обезбеђује опстанак и континуитет њиховог прихода (Ђорђевић и Кековић, 2023).

„ISO 22301, систем менаџмента континуитетом пословања даје оквир за идентификацију потенцијалних спољних и унутрашњих претњи које могу угрозити организацију. *Континуитет пословања представља способност организације да настави испоруку производа или услуга на прихватљивим, унапред дефинисаним нивоима након инцидента*. Имплементацијом овог стандарда предузеће се осигурава од потенцијалних инцидената, смањује вероватноћу да се инцидент појави. Односи се и на приватни и на јавни сектор. Овим стандардом се дефинише План континуитета пословања, а на руководству је да га стално ажурира и унапређује“ (Ђорђевић и Кековић, 2023: 1029).

Стандард ISO 22301, између осталог, идентификује и управља тренутним и будућим претњама, омогућује проактивни приступ смањењу утицаја на пословање приликом појаве инцидената, омогућава одрживост пословања у кризним ситуацијама; умањује време застоја током инцидената и убрзава време опоравка; испуњавање обавеза усклађености са законском регулативом; уштеду трошкова кроз спремност на реаговање у ванредним ситуацијама; постизање финансијских и оперативних користи које могу произаћи из примене захтева овог стандарда.

Док је ISO/TC 22318 техничка спецификација којом се обезбеђују смернице за методе за разумевање и проширење принципа БЦМ-а садржаних у ISO 22301 и ISO 22313 у оквиру менаџмента ланцем снабдевања. Ова техничка спецификација је генеричка и примењива на све организације (или њене делове), без обзира на тип, величину и природу посла. Примењива је за снабдевање производима и услугама, интерно и екстерно (https://iss.rs/sr_Cyrl/project/show/iss:proj:59131).

Примена поменутих стандарда није значајна само за предузећа и компаније који функционишу у оквиру једне заједнице већ би могли да допринесу и економској

стабилности државе, а тиме и националне безбедности. *Дакле, све набројано може се применити и на аналитички сектор и процес безбедносне аналитике.*

2.3.1.2 Стандарди у еколошкој безбедности

Када је реч о савременим концептима безбедности, посебна пажња се посвећује животној средини и еколошкој безбедности. Животна средина је одраз и политичког и економског стања у једној држави те је свест о потреби заштите животне средине већа у развијенијим државама, за разлику од оних мање развијених. Стога се значај животне средине све више апострофира на глобалном нивоу, како би се подигла свест о значају овог аспекта безбедности, јер загађење животне средине и природних ресурса може и озбиљно угрозити здравље и безбедност људи на одређеној територији. „Наиме, животна средина представља све оно што нас окружује, све оно са чиме је директно или индиректно повезана човекова животна и производна активност. Животна средина, као и односи који настају деловањем људи на природу, има свој реални друштвени, правни, економски, политички, као и безбедносни аспект“ (Матијашевић-Обрадовић и Обрадовић, 2014: 260).

За област екологије најзначајнији је ISO/TC 207 (Еколошки менаџмент), који се фокусира на стандардизацију у области менаџмента животне средине. Циљ ове комисије је умрежавање економских и институционалних актера који могу допринети промени негативних трендова изазваних климатским променама и тиме допринети одрживости наше цивилизације. Комплементаран томе јесте ISO/TC 331 (Биодиверзитет), који развија стандарде, успоставља принципе и смернице који могу допринети одрживом развоју кроз очување постојећег природног фонда флоре и фауне. Стандарди ISO/TC 146 (Квалитет ваздуха), ISO/TC 147 (Квалитет воде), ISO/TC 190 (Квалитет земљишта); ISO/TC 276 (Биотехнологија); ISO/TC 297 (Сакупљање отпада и управљање транспортом) такође доприносе у истом правцу (Ђорђевић и Кековић, 2023). И стандард ISO/TC 207 (Еколошки менаџмент) је фокусиран на системе управљања животном средином, ревизију, верификацију/валидацију и сродна истраживања, обележавање животне средине, евалуацију еколошких перформанси, процену животног циклуса, климатске промене и

њихово ублажавање и прилагођавање, еко-дизајн, ефикасност материјала, економију животне средине и финансирање животне средине и климе (Исто).

„Серија стандарда ISO 14000 представља практично средство за организовање активности које могу имати утицаја на животну средину. Ови стандарди обезбеђују оквир за праћење климатских промена кроз квантификацију гасова са ефектом стаклене баште и примере добре праксе“ (Ђорђевић и Кековић, 2023: 1034). *Систем менаџмента животном средином* ISO 14001 је међународни стандард који захтева од организација да се баве питањима животне средине која су битна за њено пословање, као што су загађење ваздуха, питања отпадних вода, управљање отпадом, загађење земљишта, ублажавање и прилагођавање климатским променама, коришћење ресурса и ефикасност. Као и сви стандарди система менаџмента, ISO 14001 укључује потребу за сталним побољшавањем система организације и приступа проблемима животне средине. Стандард је ревидиран са кључним побољшањима, као што су повећан значај управљања животном средином у оквиру процеса стратешког планирања организације, већи допринос руководства и снажнија посвећеност проактивним иницијативама које повећавају перформансе животне средине. Овај стандард се може применити на било коју организацију која жели да успостави, имплементира, одржава и унапређује животну средину и свој систем менаџмента у складу са изјавом о Политици животне средине (Исто).

2.3.1.3 Стандарди у друштвеном сектору безбедности

Што се тиче личне безбедности грађана, она се не може посматрати одвојено од осталих сектора безбедности, јер на људску безбедност утичу и квалитет ваздуха и политичка стабилност једне државе. Међутим, постоји више стандарда који доприносе томе кроз промоцију добре праксе у области одрживе изградње, заштите приватности и безбедности саобраћаја. Међу њима ћемо да издвојимо два стандарда која су значајна за људску безбедност, али која могу бити значајна и за безбедносну аналитику. То су ISO 22341 (Безбедност и отпорност) и ISO 27001 (Заштита и безбедност информација).

Везано за ISO 22341 постоје и смернице за смањење криминалитета кроз дизајн окружења и то је ISO 22341:2021. Овај документ пружа смернице организацијама за успостављање основних елемената, стратегија и процеса за спречавање и смањење

криминала и страха од криминала у новој или постојећој изграђеној средини. Препоручује се успостављање контрамера и акција за третирање криминалних и безбедносних ризика на ефектан и ефикасан начин коришћењем еколошког дизајна. У оквиру овог документа, термин „безбедност“ се користи на широк начин да обухвати све апликације специфичне за криминал, сигурност и безбедност, тако да је применљив на јавне и приватне организације, без обзира на врсту, величину или природу (https://www.iso.org/standard/50078.html).

.

> „Општи принципи и оквир за процес превенције криминалитета кроз дизајн окружења успостављени су 2022. године унутар документа Превенција криминалитета – урбано планирање и дизајн зграда – CEN 14383 (Prevention of crime – Urban planning and building design – CEN 14383) као првог европског стандарда за смањење криминалитета и страха од криминалитета путем урбаног планирања. CEN стандарди из серије 14383, а посебно кровни стандард Урбанистичко планирање (ENV 14383-2:2003 замијењен TR 14383- 2:2007 и TS 14383-2:2022), засновани су на идејама Ц. Џејкобс и О. Њумана о превенцији криминалитета и страху од криминалитета. Рад на овом стандарду започео је 1995. године, а отприлике 25 година касније, резултат је не само комплетна серија европских стандарда CEN 14383 него и приручник SafePolis (2008) и свјетски ISO стандард о CPTED-у (ISO 22341:2021). Приручник SafePolis је креиран као практично објашњење смерница у стандарду TR 14383-2. Овај стандард пружа смернице и стратегије за CPTED, за процес ‚корак по корак', укључујући све релевантне актере за урбано планирање и смањење криминалитета. Стандард и приручник нуде практично знање о томе како спречити криминалитет, страх од криминалитета и антисоцијално понашање кроз урбани дизајн и планирање. За стандард TR 14383-2 каже се да је ‚једини стандард за превенцију криминалитета у Европи од Римског царства' (COST Action TU1203, 2014: 50), а исто важи и за ревизију TS 14383-2:2022 (Van Soomeren, 2022)“ (Ступар, Т. и Ступар, Д., 2024: 60).

Стандард који може бити од посебног значаја за безбедносну аналитику и који дефинитивно треба уврстити у теоријски модел безбедносне аналитике, а који такође може допринети и спречавању тероризма јесте ISO/IEC 27001:2013. Овај стандард представља систем менаџмента безбедности информација и односи се на процес заштите и употребе информација у различитим организацијама, приватним и јавним компанијама.

> „ISO 27001 је усредсређен на заштиту поверљивости, целовитости и расположивости података у организацији. То се постиже препознавањем који се потенцијални проблеми могу догодити подацима (тј. процена ризика), те дефинише што треба предузети да се такви проблеми спрече (тј. третман или обрада ризика). Дакле, темељна филозофија ISO 27001 се заснива на управљању ризицима, препознавању и системској обради ризика. Типови информација на које се односи ISMS – Систем управљања менаџментом безбедности информација су писане информације, штампане информације, информације у електронским форматима, информације послане поштом, информације послане електронском поштом, фото, аудио, видео-информације – аудио-визуелне информације“ (https://iso.org.rs/iso-27001/).

Овај стандард има 10 поглавља где су објашњени кораци које организације треба да предузму како би руковале информацијама на адекватан начин. Мере које је потребно имплементирати су у форми правила, процедура и техничких решења, а циљ је да се креира документ посебно за сваку организацију или институцију који треба да садржи прописе којима би се спречавало нарушавање безбедности информација, тзв. политика безбедности информација. *На основу наведеног, може се закључити да би организације које се баве безбедносном аналитиком као процесом обраде података свакако требало да имају такав документ и да поштују овај стандард.*

Такође, са аспекта друштвене безбедности, значајно је поменути и стандард ISO 22311:2017 Друштвена безбедност – видео-надзор – излазна интероперабилност. Такође, овај стандард би било пожељно уврстити у модел безбедносне аналитике. Углавном се користи за потребе друштвене безбедности и у њему се утврђује уобичајени излазни формат фајла који се добија из система за видео-надзор (појединачна опрема или системи великих размера) помоћу медијума за складиштење података или путем мреже, да се омогући крајњим корисницима приступ садржају дигиталног видео-надзора и да могу да обављају неопходну обраду. Средства за размену података нису део овог стандарда. Будући да снимање видео-надзора често обухвата снимање грађана, овим стандардом су обухваћени и захтеви у вези приватности, употреби снимака и њиховом располагању. На основу горенаведених техничких стандарда, обухваћене су следеће компоненте формата:

- видео,
- аудио,
- метаподаци:
- описни (локација, идентификатор камере, итд.),
- динамички (датум, време, пан, нагиб, зум, идентификациони резултати итд.),
- инкапсулација/паковање излазног фајла;
- подаци/приступ безбедности и интегритет;
- одредбе о приватности;
- информативни подаци о презентацији корисницима (https://iss.rs/sr_Cyrl/project/show/iss:proj:59127).

2.3.1.4 Стандарди у политичком сектору безбедности

„Концепт људске безбедности подразумева активну улогу грађана у креирању политике државе у којој живе. Демократско одлучивање је једно од највећих друштвених

достигнућа и у том смислу ISO систем подржава одрживи развој и политичку стабилност кроз промоцију добре праксе и подстичући грађански активизам. Због своје развијености и универзалности, као и правно обавезујућег карактера, стандарди Уједињених нација се могу сматрати најважнијим међународним стандардима. У области политичких права и слобода у ужем смислу, ови стандарди обухватају три централна права: право на учествовање у јавним пословима, право на равноправан приступ јавним службама и право на слободне, поштене и истинске изборе“ (Трипковић, 2004: 98).

„Технички комитет ISO/TC 309 (Управљање организацијама) формализује добру праксу, која пружа широку ефикасност управљања из конкретних упутстава за систем организације, кроз систем контроле корективних механизама у форми притужби и узбуњивача. Инсистирање на родној равноправности као кључном сегменту демократских достигнућа доприноси остваривању политичких права и стабилности заједнице. Стандард ISO 26000 (Водич о друштвеној одговорности) доприноси отклањању родне пристрасности и обезбеђује равноправан положај жена и мушкараца у погледу запошљавања, напредовање у каријери и приход у оквиру пословних система и институција“ (Ђорђевић и Кековић, 2023: 1037).

За политичку стабилност значајан је и ISO 37004:2023 Управљање организацијама – Модел зрелости управљања – Смернице. Овај документ даје смернице за процену успостављања услова управљања и за примену принципа управљања с обзиром на кључне аспекте праксе ISO 37000. Он поставља концепт зрелости управљања и његово мерење и обезбеђује оквир за мерење зрелости управљања, повезану скалу зрелости управљања и модел зрелости управљања. Овај документ је применљив на све типове и величине организација без обзира на њихову локацију (https://isme.me/sr_ME/project/show/iso:proj:65037).

2.3.1.5 Стандарди у војном сектору безбедности

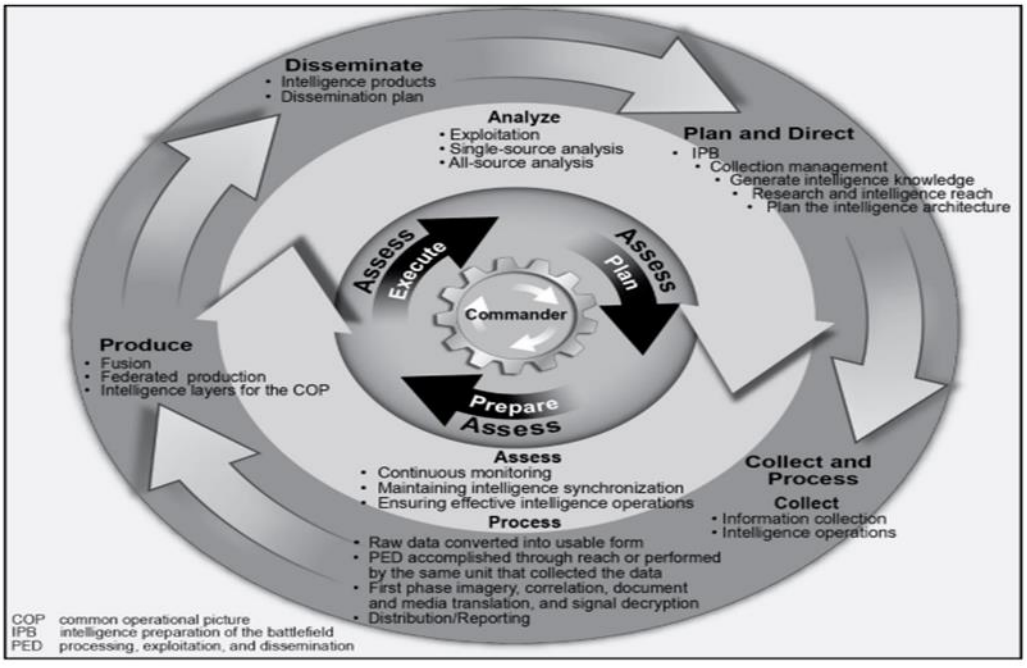
Најстарији, односно рудиментарни приступи аналитици настали су у војсци (оружаним снагама), те се отуда и одомаћио општи израз „обавештајна аналитика“. Такође, у војсци, кад је у питању општа организација рада команди/штабова, па и у обавештајној делатности, развијене су стандардизоване оперативне процедуре – СОП

(Standard Operating Procedures – SOP). Taj pristup standardizaciji operativnih procedura rada u vojsci presликan je u brojne civilne organizacije i masovno se primenjuje u praksi.

Kad je Republika Srbija u pitanju, kao i države iz njenog bližeg i šireg okruženja u Evropi, činjenica je da se u vojsci (oružanim snagama) primenjuje SOP po modelu standardizacije u NATO, a koji se primenjuje i u zemljama članicama programa Partnerstvo za mir. Tako, u NATO, a time i vojskama članica programa Partnerstvo za mir, primenjuju se standardi pod opštim nazivom STANAG (Standardization Agreement) (https://outsource.contractlaboratory.com/nato-stanag/).

> „STANAG (Standardization Agreement) je NATO dokument koji definiše standarde za vojne i tehničke operacije radi poboljšanja interoperabilnosti među nacijama članicama. Ovi sporazumi pokrivaju široku lepezu tema, kao što su komunikacije, logistika, kompatibilnost opreme i procedure obuke. Pridržavajući se STANAG-a, zemlje NATO-a mogu efikasnije i delotvornije da sarađuju, obezbeđujući spremnost i jedinstvo u kolektivnoj odbrani“ (https://outsource.contractlaboratory.com/nato-stanag/).

Posebni NATO standardi primenjuju se i u obavештajnoj delatnosti. U tom smislu, obavештajni ciklus (Intelligence) u okviru operacija i operativnog rada ima iste faze (koraке) kao što je to navedeno u prvom delu rada (Slika 21).



Слика 21. *Обавештајни циклус по НАТО стандарду*

Извор: *НАТО АЈП-2.7, 2021.*

Сврха савезничке заједничке публикације 2.7 (АЈП-2.7) је да успостави заједничку доктрину савезника да води команданте, штабове и снаге ангажоване у операцијама JISR у оквиру НАТО. Ова публикација документује стандарде, принципе и основне процедуре особља неопходне за успешно планирање, усмеравање и извођење JISR операција које обезбеђују благовремено и ефикасно доношење одлука (Allied Joint Doctrine-AJP-2.7, 2021).

Заједничка обавештајна служба, надзор и извиђање (JISR), скуп интелигенције и оперативне способности да синхронизује и интегрише планирање и операције свих могућности прикупљања са обрадом, експлоатацијом и дистрибуцијом добијене информације као директну подршку планирању, припреми и извршењу операција (Исто).

„JISR процес је процес координације кроз који прикупљање обавештајних података дисциплинује, могућности прикупљања и активности експлоатације пружају податке, информације и појединачне изворе обавештајне делатности за решавање захтева за информацијама или обавештајним подацима у намеран, ад хок или динамичан временски оквир за подршку планирању и извршењу операција. JISR процес се састоји од пет корака: *издавање задатка, прикупљање података и информација, процесуирање, коришћење и ширење (дисеминација)"* (Исто).

2.3.1.6 Студија случаја: Стандарди америчке обавештајне заједнице

У складу с претходно наведеним, а као студија случаја, приказаћемо примену стандарда у оквиру *америчке обавештајне заједнице*. У овом истраживању, као студија случаја, за пример је узета Обавештајна заједница САД, јер се у њему посебно истиче изградња **обједињеног модела безбедносне аналитике**, коју *Обавештајна заједница* развија након терористичких напада Ал-Каиде на објекте у Њујорку и Вашингтону 11. 9. 2001. године.

Америчка обавештајна заједница (Intelligence Community – IC) је скуп агенција и организација у САД које се баве обавештајним радом. Оне прикупљају, обрађују и размењују обавештајне податке, те у састав ове шире поставке обавештајне делатности улазе Централна обавештајна агенција (ЦИА), Федерални истражни биро (ФБИ), Агенција

за националну сигурност (НСА), али и Војна обавештајна агенција (ДИА), Министарство унутрашње безбедности, Министарство финансија, Агенција за заштиту животне средине и друге организације и институције које могу бити значајне за одређене обавештајне задатке. Улога Обавештајне заједнице је да пружи благовремену, дубинску, објективну и релевантну обавештајну информацију о активностима, способностима, плановима и намерама страних сила, организација, особа и њихових агената, како би информисале о питањима и догађајима значајним за одлуке о националној безбедности. Обавештајна заједница не даје препоруке у вези са политиком (https://www.intelligence.gov).

Обавештајна заједница такође прикупља, анализира и дистрибуира информације које се односе на обавештајне активности које су стране силе, организације, особе и њихови агенти усмерили против Сједињених Држава; предузима мере за заштиту од таквих непријатељских активности; спроводи тајне акције и специјалне активности и извршава друге обавештајне активности које може да наложи председник (Исто).

Обавештајну заједницу координише директор националне обавештајне службе (ДНИ). Његова улога је да повезује рад свих ових агенција олакшавајући размену информација између њих. Такође, његова улога је и да обезбеди да се обавештајни подаци користе у складу са законом. Поред тога, постоји и Обавештајни савет (Intelligence oversight), који штити права грађана и бави се етичким и другим стандардима у обавештајном раду.

Дакле, ова заједница чини један шири концепт обавештајног рада обухватајући различите специјализоване агенције које деле информације и сарађују са јасним циљем заштите националне безбедности САД. Обухвата различите аспекте обавештајног рада, попут националне и војне безбедности, борбе против тероризма, контраобавештајне делатности и друге значајне области. Наведено представља пример безбедносне аналитике који покрива различите секторе безбедности уз координацију рада различитих служби, организација и агенција са циљем заштите укупне безбедности на стратешком нивоу поштујући њихове различите процедуре, али уз уважавање одређених стандарда.

Америчка обавештајна заједница је и прописала одређене стандарде који морају бити испоштовани у аналитичким процесима и одредила директора ДНИ као одговорног за праћење њиховог поштовања у пракси. На основу Закона о националној безбедности из 1947. године, са изменама, Закона о реформи обавештајних служби и превенцији

тероризма из 2004. године и других регулатива Канцеларија директора националне обавештајне службе (ОДНИ) је даље кодификовала ове стандарде у Директиви Обавештајних заједница (ИЦД), Аналитички Стандарди. ІСИЦ аналитички стандарди су установљени 2007. године, а ДНИ их је ревидирао, ревалидирао и одобрио у јануару 2015. године (https://www.intelligence.gov).

У овом документу наводи се следеће:

Сви ІС аналитички производи треба да буду у складу са следећи пет аналитичких стандарда, укључујући девет стандарда аналитичког заната.

1) **Објективност**: Аналитичари морају да обављају своје функције са објективношћу и са свесношћу о сопственим претпоставкама и размишљањима. Они морају користити технике размишљања и практичне механизме који откривају и ублажавају пристрасност. Аналитичари треба да буду опрезни у погледу утицаја постојећих аналитичких ставова или одлука и морају размотрити алтернативне перспективе и супротне информације. Анализа не треба да буде превише ограничена претходним закључцима када нови развојни догађаји указују на потребу за изменама.

2) **Независност од политичких разматрања**: Аналитичке процене не смеју бити изобличене нити обликоване за промоцију одређеног циља, публике или политичког става. Аналитички судови не смеју бити под утицајем преференција за одређену политику.

3) **Правовременост:** Анализа мора бити достављена на време како би била корисна за кориснике. Аналитички елементи имају одговорност да буду стално свесни догађања од обавештајног интереса, активности и распореда корисника, као и обавештајних захтева и приоритета како би пружили корисну анализу у правом тренутку.

4) Заснована на свим доступним изворима обавештајних информација: Анализа треба да буде информисана свим релевантним информацијама које су доступне. Аналитички елементи треба да идентификују и решавају кључне празнине у информацијама и сарађују у активностима прикупљања и са пружаоцима података како би развили стратегије приступа и прикупљања.

5) Спроводи и показује стандарде аналитичког заната, специфично:

Исправно описује квалитет и кредибилитет основних извора, података и методологија. Аналитички производи треба да идентификују основне изворе и методологије на основу којих су закључци засновани и користе дескрипторе извора у складу са lCD 206, Захтевима за изворе за објављене аналитичке производе, како би описали факторе који утичу на квалитет и кредибилитет извора. Ови фактори могу укључивати тачност и потпуност, могућност обмане, старост и актуелност информација, као и техничке елементе прикупљања, приступ изворима, валидацију, мотивацију, могућу пристрасност или стручност. Препоручује се коришћење сажетка извора, како је описано у lCD 206, како би се пружила свеобухватна процена снага и слабости извора и објаснило који су извори најважнији за кључне аналитичке закључке.

Исправно изражава и објашњава несигурности повезане са главним аналитичким закључцима, Аналитички производи треба да означе и објасне основе несигурности повезаних са главним аналитичким закључцима, специфично вероватноћу настанка догађаја или развоја и поверење аналитичара у основу овог закључка. Степени вероватноће обухватају читав спектар, од ретких до готово извесних. Поверење аналитичара у процену или закључак може бити засновано на логици и доказима који их подржавају, укључујући количину и квалитет изворног материјала и њихово разумевање теме. Аналитички производи треба да напомену узроке несигурности (нпр. тип, актуелност и количину информација, празнине у знању и природу проблема) и објасне како несигурности утичу на анализу (нпр. до ког степена и како закључак зависи од претпоставки) (https://irp.fas.org/dni/icd/icd-203.pdf).

2.4 Знање/доктрина

Четврти део теоријског модела безбедносне аналитике јесте *знање*, тј. *доктрина*. Овај део обједињава претходна три дела модела у теоријско-практичном и практичном смислу. У теоријско-практичном смислу, знање је основа теоријског модела, које се акцептира у: 1) знању о безбедности, 2) знању о процесу/процедурама рада безбедносних аналитичара и 3) знању о стандардима који се у аналитици примењеују. У практичном смислу, укупно наведено знање исказује се као *доктрина,* односно као скуп утврђених и систематизованих ставова о теоријском моделу безбедносне аналитике.

2.4.1 Знање

Знање (сазнање) је продукт процеса сазнавања. Сазнавање као процес може да се одвија на више начина. Према теорији логике, знање може да буде здраворазумско и научно.

Здраворазумско знање се заснива на чулном искуству и спонтаном разумском закључивању, у коме је елементарна логика присутна, али није доведена до свести, није „научена из књига“. Здраворазумско знање се разликује од мита, магије и религије по томе што не прихвата ништа на веру, већ само оно што се може чути, видети, дознати од стварних сведока догађаја. Ово сазнање је отклон од празноверја и сујеверја и искорак ка науци (Форца и Аночић, 2018).

Научно сазнање карактеришу већа критичност и систематичност. На пример, посматрајући Сунце и звезде ми чулима доживљавамо привид да се они окрећу око Земље, док се, у ствари, Земља окреће око њих. Служећи се различитим методама и инструментима научници су дошли до сазнања да су небеска тела, поготово планете и Месец, знатно другачији од онога што се голим оком види. Дакле, „потребно је нагомилано искуство генерација, потребна је читава једна технологија посматрања и експериментисања да бисмо превазишли почетне заблуде здраворазумског знања и дошли до научног сазнања. То је природан пут којим се наука развија“ (www.ef. .rs/Downland/metodologija_nir/02%20logika.pdf).

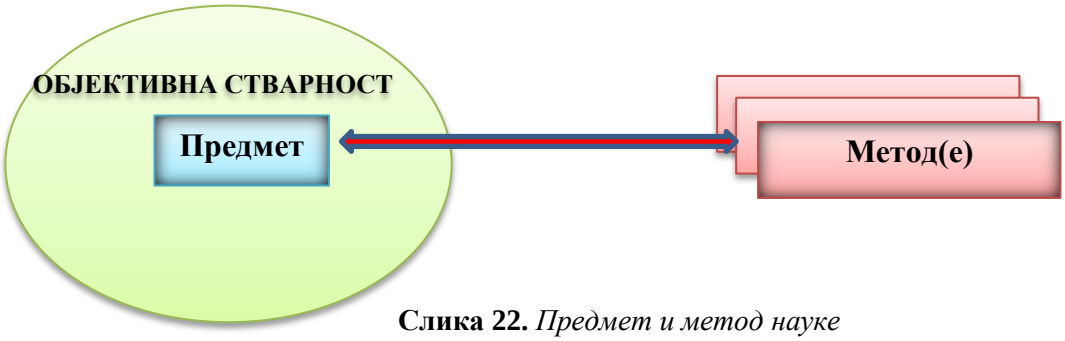
Од значаја за ово истраживање јесу ставови професора Даниловића и Милосављевића, који су објављени у наведеном делу *Основи безбедносне аналитике*. Према Даниловићу и Милосављевићу, сазнање може да буде: 1) лично – искуствено, 2) комбинација лично-искуственог и прихватања туђих сазнања (посебно оних која су проверена), 3) продукт образовања (општег и стручног) и 4) продукт системског и критичког проучавања објективне стварности, који има научни или стручни (оперативни) карактер (Даниловић и Милосављевић, 2008).

Из наведених ставова Даниловића и Милосављевића уочава се да знање (сазнање) може да буде *искуствено* и *теоријско* (образовно), при чему теоријско сазнање може да буде научно, коришћењем *научних метода и научне методологије* и стручно, коришћењем *методике* неког (оперативног) рада, у коме се долази до сазнања. Стручно сазнање може, али не мора, да се заснива на науци.

У складу са наведеним, потребно је чинити дистинкцију између начина сазнавања применом научних метода и методологије и коришћењем методике, што значи да је потребно разликовати *научну методологију* и *методику*.

Да бисмо утврдили разлику између научне методологије и методике, неопходно је да се осврнемо на свет који нас окружује и начин спознаје објективне стварности. Објективна стварност постоји мимо наше воље и, приципијелно, чине је друштвене и природне појаве, као и психички процес њихове спознаје. У том смислу, први задатак науке јесте да утврди истину о објективној стварности. Тако, општи циљ свих наука (науке у општем смислу) јесте научна спознаја објективне стварности. У оквиру скупа наука, разне науке (научне дисциплине) истражују део објективне стварности, трагајући за истином. Стога, како

истиче Славомир Милосављевић, свака наука има свој **предмет** (као део објективне стварности) и **метод(е)** помоћу којих тај предмет истражује (Слика 22).



Слика 22. *Предмет и метод науке*

Извор: *Милосављевић, 2008 (обрада ауторке дисертације)*

У складу са наведеним (Слика 22.), у Даниловић и Милосављевић (2008) Милосављевић закључује: „Општепознато и општеприхваћено је да се свака наука и научна дисциплина састоје из два (научна) дела, **предмета** који одређена (дакле, дефинисана и конституисана) наука сазнаје научним истраживањем (теоријским и емпиријским), чију суштину, облике, односе и везе, узроке и последице, зависности и посебности, квалитативне и квантитативне одредбе настоји да опише, објасни и прогнозира. Да би то успешно остварила, свака наука развија сопствени **метод** истинитог научног сазнања".

Због специфичности структуре и квалитативних одредаба предмета, свака наука развија и проучава свој *метод*. Посебна наука, која је истовремено и структурни део сваке посебне науке и научне дисциплине, која проучава методе, технике, инструменте и поступке, нужне и довољне за постизање истинитог научног сазнања о предмету науке, назива се *методологија*. Њену структуру чине: 1) **логички део** – којим се у оквирима одређеног логичког система (двовалентног, тровалентног, поливалентног) обезбеђује смисленост и логичност сазнања, 2) **епистемолошки део**, као нужни скуп научних сазнања о предмету науке односно предмету истраживања. Разлог за настанак и развој овог дела методологије је у простој чињеници да је свако сазнавање, па и научно предметно, да беспредметног сазнавања нема. Унутар овог дела могу се констатовати два слоја: а) валидна и поуздана сазнања о предмету – која су битни чиниоци одговарајуће теорије, б) битна – научно верификована сазнања о начинима стицања истинитог научног сазнања. То у ствари чини битни *теоријски фонд* од кога се приступа даљем научном истраживању, 3) **научно-стратешки део** у методологији проучава: а) примењивост

одређених метода концептуализације и пројектовања истраживања и реализације истраживања одређених делова предмета, као и функционисање тих метода, б) међузависност померања граница сазнања о предмету и граница сазнања у методологији (Даниловић и Милосављевић, 2008).

С друге стране, појављује се израз **методика**. Милосављевић је става да у нашој теорији и пракси методика није у потпуности ситуирана (позиционирана), осим у педагогији и социјалном раду. У том смислу, Милосављевић пише: „Наше схватање методике је повезано са разликовањем научног, стручно-професионалног, стручно-аматерског – хоби рада и дилетантског рада. Научни рад – рад у науци подразумева обављање задатака научног истраживања, било да се ради о откривању новог, потврди старог, већ познатог (хеуристичка и верификаторна истраживања), било да се ради о истраживању појава, закона одигравања и сл. које указује на могућности њихове примене у пракси (примењена и развојна истраживања)“ (Даниловић и Милосављевић, 2008).

Ближе се одређујући према безбедносној аналитици, Даниловић и Милосављевић (2008) о односу научне методологије и методике пишу:

> „Међутим, научна сазнања и научне методе се примењују и у свакодневном животу, истина на лаички нестручан, али и на стручан начин у оквирима одређених струка и занимања. Методика је једна од подграна методологије која се непосредно бави истраживачко-инструктивним радом који одређене научне методе, нарочито прибављања и обраде података, прилагођава потребама извршавања одређених задатака струке. Ово је нарочито очигледно у сваком облику евиденције (израда и попуњавање разних образаца; у раду безбедносних служби узимање изјава и саслушања у полицији је *испитивање* – благо, неутрално или оштро; посматрање приликом праћења (ухођења) итд. Постојање стручног рада који захтева одређено образовање и обуку стручњака, подразумева извесна специфична правила, методе и технике струке. Тако, методика посредује између методологије наука и праксе радног делања у струци“.

Сличан, али ипак другачији приступ односу научног и стручног (искуственог) сазнавања приказали су Форца и Аночић у свом (наведеном) делу *Безбедносна аналитика*, посебно у смислу коришћења метода. Наиме, Форца и Аночић су на бази теорије и праксе примарно аналитичког рада у обавештајној и криминалистичко-обавештајној аналитици дали шири аспект примене научних метода, али и методских поступака, који нису научно верификовани. Тако, на пример, говорећи о аналитичком раду у обавештајно аналитици, Форца и Аночић (2018) закључују:

„Производи обавештајне аналитике могу да буду описни, објашњавајући и прдвиђајући (прогностички). Најпогоднije методе при изради *описних* аналитичких докумената су: дескриптивна метода; метода посматрања; историјска метода; метода студије случаја. *Објашњавајући* аналитички документи су погодни за израду применом следећих врста метода: квалитативне (анализа докумената, анализа разговора и друге методе анализе садржаја); компаративне; квантитативне (статистичке методе, анкете, тестови). *Проценске (предвиђајуће) анализе* захтевају велики број посебних методских поступака који се користе у научним истраживањима ради доношења закључака о исходу неког процеса или појаве. Све методе које се могу применити у поступку израде предвиђајућих аналитичких докумената спадају у једну од следеће три категорије општих логичких метода: индукција; дедукција; абдукција“ (стр. 133).

С друге стране, при анализи рада аналитичара у криминалистичко-обавештајној аналитици, Форца и Аночић наводе читав низ метода (поступака) које нису научно признате као методе, али се често користе. Тако, на пример, наводе се следеће ненаучне методе (поступци): Дрво релевантности; Морфолошка кутија, Анализа телефонских разговора; Анализа догађаја и бројне друге (Форца и Аночић, 2018).

У складу с наведеним, Форца и Аночић (2018) износе следеће податке:

„Питању метода који се користе у безбедносној аналитици разни аутори приступају изузетно разнолико, што је последица поимања самог процеса аналитике. Тако, једни под методом посматрају метод рада безбедносних аналитичких служби (Термиз и Милосављевић, 2008), описујући цео процес, од прикупљања, преко сређивања и анализе, до чувања и коришћења података. Други говоре о методима прикупљања података, анализирајући само примену научних метода (Даниловић и Милосављевић, 2008). Код појединих аутора, у сфери криминалистичке аналитике, говори се о типологији метода које се непосредно примењују у процесу криминалистичко-аналитичког рада и, пре свега, имају практичан аспект (Манојловић, 2008). Поједини аутори се осврћу само на прогностику и анализирају примену само научних метода у том процесу“ (стр. 117).

Врло је илустативан пример анализе односа научних приступа сазнавању и рада аналитичара у САД (ЦИА), који су спровели амерички експерти након терористичких напада на Њујорк и Вашингтон 11. 9. 2001. године. Наиме, да би дефинисали какав треба да буде безбедносни аналитичар, експерти у САД су извршили компарацију 1) сазнања до којих долази аналитичар и 2) научног приступа истраживању појава и процеса. Према америчким експертима, аналитичар до сазнања долази на начин приказан у Табели 16.

Табела 16. *Извори сазнања за аналитичко закључивање*

Извор сазнања	Опис
Ауторитет	Експерт или неко са ауторитетом (родитељ, наставник или супервизор) нуди сазнање и њему се верује без поговора.
Вера	Сазнање се прихвата без чврстих доказа (религија, идеологија, митови).

Здрав разум	Логично сазнање добијено од других – „једноставно, то сви знају“.
Интуиција	Сазнање које имамо без свесног објашњења истог. Оно долази из унутрашњих логичних уверења или имплицитног повезивања чињеница.
Рационализам	Сазнање добијено кроз виши ниво логичног резоновања (постављање теорије) и засновано на људској способности да резонује независно од актуелног искуства у стварном свету.
Емпиризам	Сазнање генерисано из искуства и систематског посматрања појава и процеса, нпр. прикупљање података помоћу пет чула.
Наука	Комбинација рационализма и емпиризма.

Извор: *Колијер, 2005.*

С друге стране, према амаеричким експертима, научни приступ истраживању и сазнању има следеће кораке:

1. Постави истраживачки проблем или питање,
2. Стекни увид у расположиве податке и сазнања,
3. Постави теоријски оквир (модел);
4. Дефиниши истраживачке хипотезе;
5. Креирај замисао истраживања;
6. Спроведи прикупљање података;
7. Спроведи анализу података и
8. Подели ново сазнање корисницима (Collier, 2005)

Упоређујући рад аналитичара (оперативаца) и научни приступ у сазнавању, амерички експерти су закључили да њихови аналитичари, у суштини, „не познају научне методе“. У том смислу, уследила је широка акција ангажовања америчких факултета и института у формирању начина оспособљавања обавештајних аналитичара у примени савремених научних метода (Collier, 2005).

Чињеница је да се у теорији и пракси води полемика по питању да ли је безбедносна аналитика наука (теорија) или пракса. Мишљења су подељена, једни придају већи значај научним методима у раду аналитичара, док се други више приклањају искуству и практично утврђеним поступцима. Озбиљне анализе, пак, указују на то да је безбедносна аналитика практична делатност заснована на науци. Однос научних и ненаучних метода у безбедносној аналитици је 70%:30% (Форца и Аночић, 2018).

Из приказа претходна три сегмента теоријског модела безбедносне аналитике, недвосмислено се може закључити и потврдити став који су изнели Форца и Аночић, да се у безбедносној аналитици примењују научна и практична (искуствена) знања (сазнања).

2.4.2 Доктрина

Посебан аспект изградње теоријског модела безбедносне аналитике јесте *доктрина,* што ћемо образложити у наредном тексту.

Реч *докрина* потиче из латинског језика (*doctrine*) и изворно значи: учење, наука, догма. Представља скуп темељних начела, теорија, веровања или учења која се прихватају као истинита унутар одређене области. Служе као смерница за деловање. *Речник српскохрватског књижевног језика* за реч доктрина даје две групе значења 1) „правила и начела једне науке, идеологије“ и (2) „учење, идеологија“ (Сивачек, 2006).

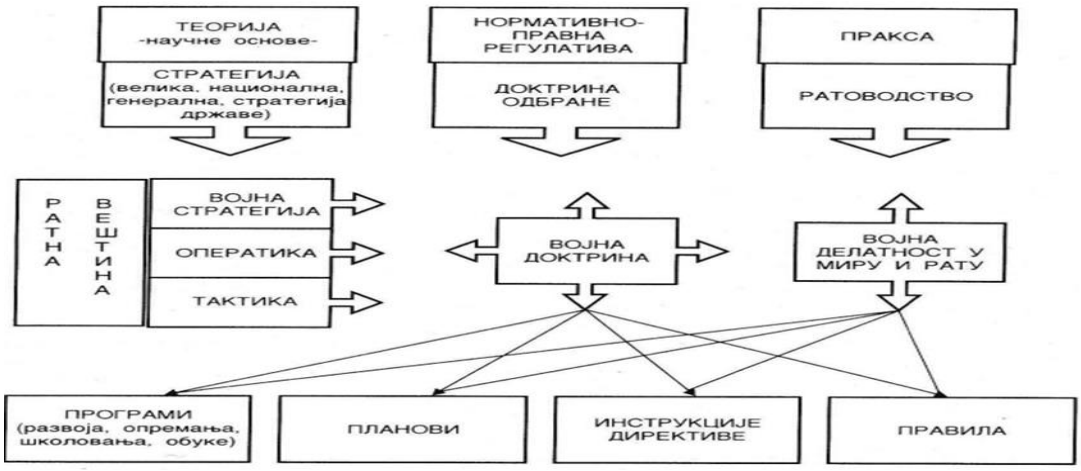
Савремена теорија под доктрином не подразумева науку, већ теорију струке, односно норме практичне делатности у разним сферама људске делатности. Иако би се, принципијелно посматрано, доктрина могла анализирати у разним сферама људске делатности, у савременим условима тај појам захваћен је, пре свега, у оружаним снагама (војсци) (Форца, 2017).

У складу са претходном опсервацијом знања (сазнавања), у односу научног и стручног знања, Душан Вишњић (1995) у војној сфери пореди однос војне стратегије и доктрине и каже: „стратегија је наука (делатност стратегиста) и практична делатност стратега (команданата), док је доктрина искључиво теорија струке, на науци заснована. У том смислу, стратегија говори о општем аспекту предметне области (нпр. оружана борба, у општем смислу), док доктрина даје ставове о конретној области (оружана борба у доктрини Војске Србије, стр. 5). Потврду Вишњићевих ставова о односу војне стратегије и доктине налазимо у класификацији докумената у оружаним снагама западних земаља, пре свега у САД и Великој Британији. Наиме, у појашњењу тих докумената се истиче да је „доктрина скуп принципа по којима се руководе оружане снаге у реализацији одређене стратегије. Тако, једна је војна стратегија, а доктрина постоји читав скуп, од тзв. нулте (*capstone*), преко неколико нивоа (кључне – *keystone*, операционализоване), до тактика, техника и процедура“ (Форца, 2014).

Међутим, на западу, где се често користи израз „доктрина“, исти се употребљава у општем и конкретном смислу. Тако, за укупни фонд теорије струке неке области се каже – *доктрина*, именујући чија (америчка, француска, српска…). Такође, у политичкој пракси се врло често употребљава израз „доктрина“, који појашњава приступ председничке администрације ка неком спољнополитичком питању. У том смислу, врло је позната тзв.

Монроова доктрина, по којој се предлаже да САД више не дозволе да нека европска држава господари државама Северне и Јужне Америке. Та доктрина је настала за време председника САД Џејмса Монроа (1817-1825), а обзнањена је након ослобађања држава Јужне Америке од шпанске колонизације (Пророковић, 2018).

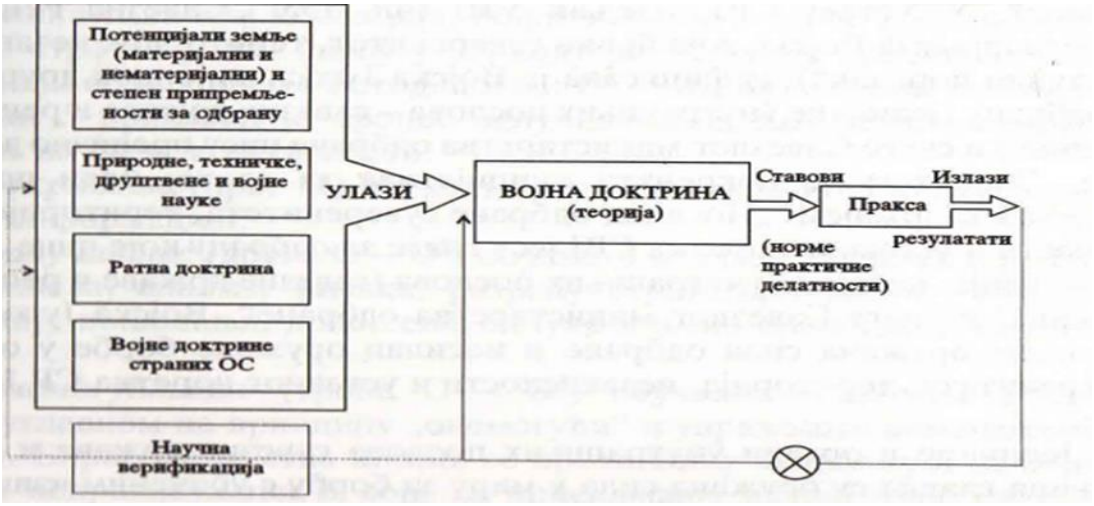
У нашој теорији и пракси доктрина се задржала само у војној сфери, док се у осталим делатностима само спорадично помиње. Скраја прошлог и почетком овог века коришћен је израз „војна доктрина“ до 2010. године, када је званично усвојена *Доктрина Војске Србије.* Поимање војне доктрине, тежишно, подразумевало је теорију струке. У том смислу, Митар Ковач (2021) користи ставове Душана Вишњића и пише: „Војна доктрина је интегрално, на поузданим знањима засновано, повезано изложено програмско становиште о свим основним питањима војне делатности. Она (војна доктрина) јесте опште упутство војне струке, опште правило војног деловања у миру и рату“ (стр. 44). Тај свој став Ковач врло сликовито исказује и појашњава (Слика 23):



Слика 23. *Однос теоријских и доктринарних садржаја*

Извор: *Ковач, 2001: 45*

‚Слично Ковачу, Спасоје Мучибабић (2021), пишући о Доктрини Војске Југославије, истиче „да она (доктрина) подразумева дефинисање ставова за *практичну делатност* Војске“ (стр. 125). Дакле, војна доктрина је теорија струке, што и сликовито показује Слика 24.



Слика 24. *Војна доктрина као систем*

Извор: *Мучибабић, 2001: 112*

Како смо истакли, 2010. године у Србији је усвојен документ под називом *Доктрина Војске Србије,* која је дефинисана на следећи начин: „Доктрина Војске Србије је основни документ у којем се дефинишу општа опредељења о војној делатности, организовању, припремама, употреби и обезбеђењу Војске Србије у миру, ратном и ванредном стању“ (Доктрина Војске Србије, 2010).

Из наведене дефиниције уочавамо да се под војном доктрином подразумева теорија струке о војној делатности у миру, ратном и ванредном стању. Такође, уочавамо да се користи израз „основни документ“. Наиме, у приступу изради војне доктрине у Србији примењена су искуства земаља чланица Партнерства за мир, оперативни домен израде нормативних аката у НАТО, где доктрина није само један документ. У том смислу, доктринарна документа према *нивоу општости* деле се на 1) доктринарна документа првог нивоа (*основна*) и 2) другог нивоа (*изведена*). *Основна* доктринарна документа су 1) главна и (2) функционална (кључна), а изведена доктринарна документа су правила, упутства и тактички приручници (Генералштаб Војске Србије, 2012). У даљој класификацији, главна доктринарна документа су: Доктрина Војске Србије, Доктрина КоВ, Доктрина РВ и ПВО, а кључна јесу: Доктрина операција и тзв. функционалне доктрине, које доносе управе Генералштаба из своје надлежности (Доктрина обавештајне

делатности, Доктрина планирања, Доктрина логистике... до Доктрине цивилно-војне сарадње).

Уважавајући наведено о изразу „доктрина“ и „војна доктрина“, применићемо опште ставове на питање теоријског модела безбедносне аналитике. У том смислу, доктрину у домену безбедносне аналитике повезујемо са претходна три њена сегмента (сектори безбедности, процедуре и стандарди) и дефинишемо на следећи начин: *Доктрина безбедносне аналитике јесте целовит национални приступ опису, објашњењу и предвиђању угрожавања безбедности државе и грађана Републике Србије. Представља скуп знања и вештина потребан за аналитику сектора безбедности, утврђених процедура и стандарда. Она је динамична и мења се у складу са променом теорије и праксе изазова, ризика и претњи, као и усавршавања процедура и стандарда у аналитици.*

Овако утврђена дефиниција доктрине безбедносне аналитике захтева мало детаљније објашњење.

Прво, доктрина безбедносне аналитике је целовит национални приступ угрожавању безбедности државе и грађана, што подразумева аналитику на стратегијском (стратешком) нивоу у систему националне безбедности. Принципијелно посматрано, такве приступе имају савремене државе и интеграције. На пример, NIM (Национални обавештајни модел) у Великој Британији или ECIM у Европској унији, преко модела SOCTA, а посебно приступ Обавештајне заједнице у САД, што је већ описано. У складу са карактером аналитике у било којој области, тај приступ у доктрини безбедносне аналитике *описује, објашњава и предвиђа* изазове, ризике и претње (изворе, облике и носиоце) угрожавања националне безбедности. Описивање подразумева информације о томе шта се и када догодило. Објашњење подразумева виши ниво аналитике, тражењем разлога – како и зашто се нешто догодило или догађа. Највиши ниво доктрине безбедносне аналитике јесте предвиђање како и зашто ће се нешто (угрожавање) догађати у будућности. Такав целовит национални приступ доктрине треба да стратегијском нивоу управљања системом националне безбедности[26] испоручи релевантан скуп информација о угрожавању државе и грађана потребних за њихов рад, односно предузимање мера за супротстављање

[26] Системом националне безбедности Републике Србије управљају: Народна скупштина, председник Републике, Влада и Савет за националну безбедност. Види: *Стратегија националне безбедности Републике Србије*, *Службени гласник РС*, бр. 94/2019.

угрожавању безбедности. На описани начин, доктрина безбедносне аналитике, поред захвата безбедносног амбијента у коме се налази држава и грађани, врши утицај на доносиоце одлука у смислу предузимања мера и активности за супротстављање угрожавању националне безбедности.

Друго, да би стратегијском нивоу управљања системом националне безбедности испоручила релевантан скуп информација о угрожавању националне безбедности, доктрина безбедносне аналитике мора да обухвати изузетно широк и дубок скуп знања (сазнања) како научних (теоријских) тако и стручних (искуствених), којима располажу безбедносни аналитичари. Та знања (сазнања) примарно се односе на секторе безбедности, процедуре рада и примену стандарда (стандардизација) у раду аналитичара. Као таква, доктрина безбедносне аналитике је теорија струке, заснована на науци, што подразумева да се уобличава у скуп за одређено време релевантних упутстава, правила и процедура рада.

Треће, доктрина безбедносне аналитике није догма. Она је отворени систем знања и вештина, који се мења у складу са променом основних чинилаца на којима је заснована. Дакле, мења се у складу са теоријско-практичним променама у погледу сектора безбедности, процедура рада аналитичара и усвршавања и коришћења стандарда у том раду. У том смислу, поред развоја теорије и праксе на националном нивоу, доктрина безбедносне аналитике користи и најбоља страна искуства и решења.

2.4.2.1 Организационо-функционални аспект доктрине безбедносне аналитике

У ранијем тексту више пута смо, с разлогом, истакли став признатог експерта Мура, који каже да је „обавештајна аналитика *знање, активност и организација*“. У складу с наведеним, у овом питању фокус је на организационој јединици у управљању системом националне безбедности која би била надлежна да за стратегијски ниво спроводи безбедносну аналитику. У том смислу, послужићемо се научним ставовима о пројектовању система.

У пројектовању организационих система, полазећи од њиховог циља (сврхе), прво се одређују функције које ће тај систем да обавља, а затим се тим функцијама додељује

структура која ће да их обавља (Форца, 2022). Доктрину безбедносне аналитике, условно, можемо посматрати као систем у којем конкретне организационе структуре обављају одређене функције у процесу аналитике. У том смислу, за приказ организационо-функционалног аспекта доктрине безбедносне аналитике послужићемо се у теорији познатом и често примењиваном IDEF0 методологијом (Слика 25).

Слика 25. *Начелна шема примене IDEF0 методологије*

Извор: *Форца, 2003.*

IDEF0 је акроним енглеских речи „**I**cam **DEF**inition for Function Modeling“, где је ICAM акроним од речи „Integrated Computer Aided Manufacturing“. Долазак до IDEF0 имао је свој краћи историјат (Форца, 2003).

Нагли развој информационих технологија скраја прошлог века утицао је и на њихову примену у пословању (бизнису). С друге стране, дошло се до сазнања да примена информационе технологије не може бити ефикасна уколико се и сами пословни системи, тј. организације не преобликују, како би се искористили могући потенцијали стратегијске примене ИТ. Као резултат тога, појавио се концепт „реинжињеринга пословних процеса“ – BPR (Business Process Reengineering), те концепт „управљања пословним процесима“ – BPM (Business Process Management). Након тога, развиле су се познате методе моделовања организације, међу којима се истичу: IDEF (скуп интегрисаних метода), UML (објективно усмерена методологија) и ARIS (интегрисана методологија) (Bogati, Vuk, 2012: 93–99).

IDEF методологија обухвата скуп интегрисаних модела, који су дефинисани као засебни стандарди, а настала је у оквиру Агенције за одбрамбене информационе системе (DISA – *Defense Information Systems Agency*) у оквиру Министарства одбране САД. Развијала се од IDEF0 методе до већег броја, означених од 1 до н. IDEF0 метода је дизајнирана за моделовање доношења одлука, акција и активности организације, односно система. Национални институт за стандарде и технологију САД (National Institute of Standrads and Tecnology, USA) усвојио је IDEF0 методу као стандардну методу моделовања. Покровитељство над овим стандардом преузео је Институт за електронско инжењерство, а прихватила га је и Међународна организација за стандардизацију (International Organization of Standards – ISO). Од 1993. године усвојена је као стандард у САД, а методологију у усавршеном типу **IDF X** (1-9) примењују чланице НАТО (Bogati, Vuk, 2012).

IDF методологија је слична **BSP** (Business System Planning) методи, али са већом детаљизацијом и конкретизацијом захтева који требају да се испуне да би се дефинисао и утврдио неки процес (активност) у организацији. Наиме, полазећи од чињенице да активности, саме по себи, не дају потпун одговор шта све треба урадити да би се неки процес заокружио, у овој методологији (шема) посебно се анализирају улази, излази, ресурси и контрола сваке активности, то јест процеса, као што је то приказано на претходној слици. **Активност** је именовани *процес*, функција или догађај, који траје у временском периоду и даје препознатљиве резултате. **Улаз** су информације које активности користе (могу их обрађивати или само трансформисати) да би се добили излази из активности. **Излаз** су информације које активности производе. Тако, свака активност мора имати бар један излаз јер активност која нема излаз највероватније није ни требало да се дефинише. **Контрола** одређује како, када и да ли треба нека активност да се деси. Свака активност мора имати бар једну контролу, која представља правила, законе, упутства, процедуре или стандарде. **Механизам** представља ресурсе које активност користи. То су, најчешће, људи, опрема или неки други ресурси (Исто).

У складу са наведеним за IDF0 методу, као и њен приказ на претходној слици, закључујемо:

- **Процес** који реализују безбедносни аналитичари има свој улаз, излаз, контролне механизме и ресурсе.

- **Улаз** у процес чине подаци и информације сакупљени из разних извора и на различите начине о изазовима, ризицима и претњама безбедности из утврђених сектора безбедности.
- **Излаз** из процеса треба да чини релевантан скуп поузданих информација о изазовима, ризицима и претњама, који се доставља стратегијском нивоу управљања системом националне безбедности, у утврђеној форми.
- **Контролни механизми** за процес јесу: закони, одлуке, правила, упутства, методе и стандарди.
- **Реусрс** за реалаизацију процеса представља организациона целина безбедносних аналитичара, која располаже научним и практичним знањима и вештинама и примењује одговарајуће методе и стандарде.

У тако описаној примени IDF0 у теоријском моделу безбедносне аналитикике (доктрини безбедносне аналитике), поставља се питање: *Ко чини организациону целину безбедносних аналитичара?* Да бисмо дали конзистентан одговор, односно предлог, који је проверен у истраживању, неопходно је мало детаљније појаснити процес управљања системом националне безбедности Републике Србије.

2.4.2.1.Управљање системом националне безбедности Републике Србије

Република Србија је самостална и независна држава од 2006. године. Након доношења Устава Републике Србије (2006) успостављене су све државне функције међу којима и функција „одбране и безбедности“. Наиме, у Уставу је у надлежности Републике Србије, између осталих, утврђена и: „уређује и обезбеђује одбрану и безбедност Републике Србије и њених грађана“ (Устав, 2006). Дакле, надлежност Републике Србије (функција) у Уставу је утврђена као „одбрана и безбедност“. Ово истичемо с јер се у каснијем доношењу закона и других прописа појављује несклад по питању дистинкције „одбране“ и „безбедности“. Наиме, чињеница је да су након Устава у сфери одбране донети Закон о одбрани, други закони и подзаконски акти, међу којима и Стратегија одбране Републике Србије. Међутим, кад је безбедност у питању, после Устава нема Закона о безбедности (Закон о систему националне безбедности), већ је највиши акт Стратегија националне безбедности Републике Србије. Тако, о систему националне безбедности Републике Србије основне одредбе налазимо у документу Стратегија националне безбедности.

Међутим, чињеница је да Устав Републике Србије не познаје документ *Стратегија националне безбедности,* али познаје *Стратегију одбране*. Професор Форца је става да се највероватније ради о „инерцији“, јер је у Државној Заједници Србије и Црне Горе

постојао документ Стратегија одбране (*Службени лист СЦГ*, бр. 55/2004), а није Стратегија националне безбедности (Форца, 2022). У том смислу, како истиче Форца, требало је прво неким правним актом утврдити документ *стратегија националне безбедности Републике Србије*, чиме би се створиле правне претпоставке за његово доношење. Тако, Законом о одбрани из 2007. године, први пут је утврђен документ Стратегија националне безбедности Републике Србије (*Службени гласник РС*, бр. 116/2007). Након две године (2009), Народна скупштина је, у складу са Законом о одбрани, усвојила прву Стратегију националне безбедности Републике Србије. (*Службени гласник РС*, бр. 88/2009).

Поред наведених чињеница о начину усвајања прве стратегије националне безбедности у Републици Србији, чињеница је да та стратегија није имала акциони план за спровођење, као што то имају модерне стратегије. С тим у вези, након 10 година (2019), Народна скупштина је усвојила другу по реду (до сада) Стратегију националне безбедности Републике Србије, где је утврђено да ће се усвојити и Акциони план за спровођење стратегије (Стратегија националне безбедности, 2019). Из наведених разлога, основни подаци о систему националне безбедности Републике Србије и управљању тим системом прузети су из Стратегије из 2019.

Систем националне безбедности Републике Србије утврђен је на следећи начин: „Систем националне безбедности представља нормативно, структурно и функционално уређену целину чијом се делатношћу обезбеђују заштита и остваривање националних интереса Републике Србије“ (Стратегија националне безбедности, 2019).

У претходном тескту смо истакли да су у структури система националне безбедности Републике Србије утврђена два дела, *управљачки* и *извршни.* Управљачки део чине: Народна скупштина, председник Републике, Влада и Савет за националну безбедност. На овом месту треба истаћи да су Народна скупштина, председник Републике и Влада институције Републике Србије утврђене Уставом, што није случај са Саветом за националну безбедност.

Врло је интересантна позиција и процес настанка Савета за националну безбедност у Србији. О томе, тадашњи Центар за цивилно-војне односе из Београда изоноси следеће податке:

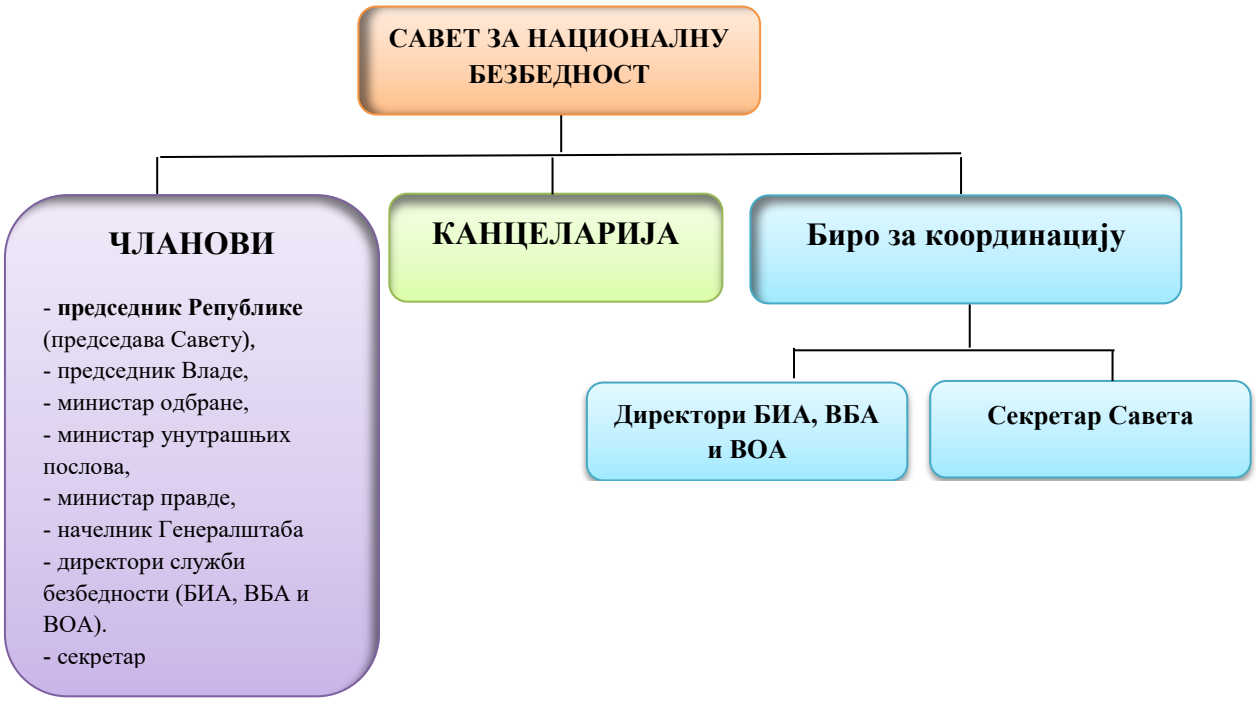
„У Србији је до данас било, додуше неуспешних, покушаја да се формира овако значајно тело. Влада СРЈ је 2000. године основала Савет за одбрану и безбедност, на чије је чело постављен савезни премијер Зоран Жижић, а у чијем саставу се нашао и министар одбране Слободан Краповић. Савезни министар финансија Драгиша Пешић објаснио је да је Савет основан као радно тело Владе, да је саветодавног карактера и да се неће мешати у ингеренције Врховног савета одбране (ВСО). Влада Зорана Ђинђића својевремено је уредбом основала Савет за државну безбедност. Међутим, овај Савет није био дугог века, нити је његово постојање резултирало усвајањем било каквог стратешког документа. Прва влада Војислава Коштунице је у јануару 2006. године уредбом основала један овакав савет ради успостављања боље координације рада тајних служби, као и ради хапшења Ратка Младића. Нажалост, овај Савет се никада није састао. Формирањем Савета друга Влада Војислава Коштунице покушала је да надомести уставне мањкавости. Устав Србије (2006) пропустио је да регулише постојање овог тела. Самим тим, пропуштено је и то да се Уставом устроји и систем безбедности у Србији. Надлежности које Савет има свакако говоре у прилог томе да њихово постојање мора бити регулисано највишим правним актом. Уместо да буде формиран Уставом, Савет је формиран Законом о основама уређења служби безбедности Републике Србије 2007. године“ (Центар за цивилно-војне односе, 2009).

Законске одредбе о Савету за националну безбедност, као и његово виђење у Стратегији националне безбедности (2019) упућују на могућност (потребу) да се у том телу формира организациона целина за безбедносну аналитику, предвиђена овим истраживањем. На овом месту указује се на стратешке и законске одредбе о Савету за националну безбедност.

Према Закону о основама уређења служби безбедности Републике Србије, Савет за националну безбедност чине:

- председник Републике (председава Савету),
- председник Владе,
- министар одбране;
- министар унутрашњих послова;
- министар правде;
- начелник Генералштаба;
- директори служби безбедности (БИА, ВБА и ВОА) и
- секретар (Закон о основама уређења служби безбедности Републике Србије, 2007).

Поред наведених главних чланова Савета за националну безбедност, његова структура дата је на Слици 26.



Слика 26. *Структура Савета за националну безбедност*

Извор: *Обрада ауторке дисертације*

Законом је утврђено (Табела 17) да се Савет за националну безбедност 1) стара о националноја безбедности и 2) усклађује рад служби безбедности.

Табела 17. *Надлежности Савета за националну безбедност*

СТАРАЊЕ О НАЦИОНАЛНОЈ БЕЗБЕДНОСТИ	УСКЛАЂИВАЊЕ РАДА СЛУЖБИ БЕЗБЕДНОСТИ
• разматра питања из области одбране, унутрашњих послова и рада служби безбедности, • разматра међусобну сарадњу органа надлежних за одбрану, органа надлежних за унутрашње послове и служби безбедности и њихову сарадњу с другим надлежним државним органима, као и сарадњу са органима и службама безбедности страних држава и међународних организација, • предлаже надлежним државним органима мере за унапређење националне безбедности; • разматра предлоге за унапређење националне безбедности које му упућују органи надлежни за одбрану, органи надлежни за унутрашње послове, службе безбедности и други надлежни државни органи; • разматра питања из делокруга органа државне управе, аутономних покрајина, општина, градова и Града Београда која су значајна за националну безбедност; • разматра и друга питања која су значајна за националну безбедност.	• разматра обавештајно-безбедносне процене и доноси закључке којима одређује приоритете и начине заштите и усмерава остваривање националних интереса који се спроводе путем обавештајно-безбедносне делатности, • доноси закључке у вези с радом служби безбедности и Бироа за координацију, • доноси закључке којима усмерава и усклађује рад служби безбедности; • доноси закључке којима усмерава сарадњу служби безбедности са службама безбедности страних држава и међународних организација; • доноси закључке којима усклађује делатности државних органа које су посвећене међународној сарадњи у области националне безбедности и одбране; • прати извршавање закључака које је донео; • даје мишљења о предлозима годишњих и средњорочних планова рада служби безбедности; • даје мишљења Влади о предлозима буџета служби безбедности и прати реализацију одобрених буџетских средстава; • даје мишљење Влади о предлогу за постављење и разрешење директора служби безбедности.

Извор: *Закон о основама уређења служби безбедности*, 2007, члан 5

Стратегија националне безбедности 2019, надлежности Савета за националну безбедност утврђује на следећи начин:

„*Савет за националну безбедност* представља тело Републике Србије које разматра питања из области безбедности, одбране, унутрашњих послова и рада служби безбедности. Такође, разматра и координира међусобну сарадњу органа надлежних за одбрану, органа надлежних за унутрашње послове и служби безбедности и њихову сарадњу са другим надлежним државним органима, као и сарадњу са органима и службама безбедности страних држава и међународних организација и обавља друге послове и задатке из области националне безбедности“ (Стратегија националне безбедности, 2019).

Као што је приказано на претходној слици, у оквиру Савета за националну безбедност као организационе јединице, постоје Канцеларија и Биро за координацију. Према наведеном Закону о основама уређења служби безбедности Републике Србије, надлежности Бироа за координацију су утврђене на следећи начин:

„Биро за координацију оперативно усклађује рад служби безбедности и извршава закључке Савета о питањима из своје надлежности.

Биро за координацију посебно:

- утврђује задатке који се извршавају оперативним усклађивањем делатности служби безбедности и служби безбедности и других државних органа и с тим у вези координира њихове активности,
- утврђује начин оперативног усклађивања у појединим случајевима,
- оснива мешовите радне групе за оперативне задатке који се извршавају оперативним усклађивањем делатности и утврђује њихове задатке;
- анализира резултате оперативног усклађивања и о томе по потреби извештава Савет, а најмање једном у шест месеци (Закон о основама уређења служби безбедности Републике Србије, 2007: чл. 11).

Канцеларија Савета за националну безбедност и заштиту тајних података јесте стручна служба Владе. У складу са Законом о тајности података, надлежности Канцеларије су:

1) поступа по захтевима за издавање сертификата и дозвола,
2) обезбеђује примену стандарда и прописа у области заштите тајних података,
3) стара се о извршавању прихваћених међународних обавеза и закључених међународних споразума између Републике Србије и других држава, односно међународних органа и организација у области заштите тајних података и сарађује са одговарајућим органима страних држава и међународних организација;
4) израђује и води Централни регистар страних тајних података;
5) предлаже образац безбедносног упитника;
6) предлаже образац препоруке, сертификата и дозволе;
7) води евиденцију о издатим сертификатима, односно дозволама, као и евиденцију о одбијању издавања сертификата, односно дозвола;
8) организује обуку корисника тајних података у складу са стандардима и прописима;
9) предлаже Влади план заштите тајних података за ванредне и хитне случајеве;
10) опозива тајност податка у складу са одредбама овог закона;
11) после престанка органа јавне власти који немају правног следбеника, обавља послове који се односе на заштиту тајних података;
12) сарађује са органима јавне власти у спровођењу овог закона у оквиру своје надлежности;
13) обавља и друге послове који су предвиђени овим законом и прописима донетим на основу овог закона.

Директор Канцеларије Савета подноси Влади годишњи извештај о активностима у оквиру надлежности Канцеларије Савета (Закон о тајности података, 2009: чл. 87).

Да бисмо још детаљније ушли у решавање проблема организационе јединице која може да буде надлежна за безбедносну аналитику, навешћемо и друге законске одредбе које се односе на угрожавање безбедности.

Прво, према Закону о одбрани Влада „усваја Процену војних и невојних изазова, ризика и претњи безбедности земље, на предлог министра одбране“ (Закон о одбрани, 2015).

Друго, на основу Закона о безбедносно-информативној агенцији БИА, као јединствена контраобавештајна и обавештајна цивилна агенција, надлежна је за следеће послове: 1) заштита безбедности Републике Србије и откривање и спречавање делатности усмерених на подривање или рушење Уставом утврђеног поретка Републике Србије, 2) истраживање, прикупљање, обрада и процена безбедносно-обавештајних података и сазнања од значаја за безбедност Републике Србије, 3) информисање надлежних државних органа о тим подацима, као и друге послове одређене законом (Закон о Безбедносно-информативној агенцији, 2002: чл. 2).

Треће, о Војнобезбедносној (ВБА) и Војнообавештајној (ВОА) агенцији је донет посебан закон – Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији из 2009. године. Према том закону уочава се да су кључне функције (послови, надлежности) ВБА безбедносна и контраобавештајна заштита Министарства одбране и Војске Србије. Те кључне функције ВБА могу се груписати у две главне области 1) општебезбедносна и 2) контраобавештајна (Табела 18), као и друге послове и задатке који су од значаја за одбрану Републике Србије, у складу са Законом.

Табела 18. *Главне области у оквиру функција ВБА*

ОПШТЕБЕЗБЕДНОСНА ОБЛАСТ	КОНТРАОБАВЕШТАЈНА ОБЛАСТ
1) Процена безбедносних ризика.	1) Откривање, праћење и онемогућавање обавештајног деловања и субверзивне делатности других држава, страних организација или лица против МО и ВС.
2) Планирање, организовање и контрола безбедносне заштите снага,објеката и средстава.	2) Планирање, рганизовање и спровођење контраобавештајне заштите тајних података М и ВС.
3) Примена и контрола примене мера заштите тајности података.	3) Прикупљање, анализа и обрада и процена контраобавештајних података из своје надлежности.
4) Безбедност информационих система и рачунарских мрежа, система веза и криптозаштите.	

Извор: *Обрада ауторке дисертације на основу Закна о ВБА и ВОА*

„С друге стране, према Закону о ВБА и ВОА, послови и задаци ВОА предвиђени су у оквиру 12 области које подразумевају, најпре, све фазе обавештајног циклуса – од прикупљања података до обавештавања надлежних органа, сарадњу са домаћим и страним службама и чување података, као и опреме и средстава у складу с прописаним процедурама. Од осталих конкретних задатака, предвиђене су мере заштите лица, објеката и документације Војске Србије у земљи и иностранству, коришћење информационих и других система везе, едукација припадника, вршење безбедносних провера, планирање опремања, унутрашња контрола припадника и други задаци из његове надлежности“ (Машуловић и сар., 2016: 208).

Наведене законске и стратешке одредбе примарно се односе на Савет за националну безбедност и службе безбедности (БИА, ВБА и ВОА). Међутим, оно што представља широк опсег из домена тзв. унутрашње безбедности, осим делом и уопштено дато у надлежностима БИА, није поменуто. У том смислу, чињеница је да се великим делом тих послова бави полиција. Познато је, а што је наведено у првом делу дисертације, да је у Србији уведен Полицијско-обавештајни модел, који, између осталог, обухвата и криминалистичку (криминалистичко-обавештајну) аналитику, кључне претње у домену криминалитета. Такође, у сатаву МУП-а Србије налази се и Сектор за ванредне ситуације, у чијој надлежности јесу претње из тог домена. Међутим, изван наведених врста аналитике остају значајне претње безбедности које долазе од пандемија и епидемија заразних болести.

Све горе наведено указује да у нас не постоји јединствена организациона целина која се бави изазовима, ризицима и претњама у целини, као целином. Стога, са аспекта управљања системом националне безбедности, а који неизоставно мора да обухвати безбедносну аналитику, неопходним се чини 1) донети закон о националној безбедности (или закон о систему националне безбедности) и 2) утврдити организациону целину у систему националне безбедности, чија би надлежност била безбедносна аналитика на стратешком нивоу.

Само као искуство, али и могућност његове примене у сопственој пракси, навешћемо организациони део који се у систему националне безбедности Републике Хрватске назива *Координација*. У Закону о суставу домовинске сигурности састав Координације чине:

потпредсједник Владе Републике Хрватске задужен за националну сигурност, као предсједник Координације за систем домовинске сигурности; савјетник предсједника Републике Хрватске задужен за националну сигурност; челници средишњих тијела државне управе надлежних за унутарње послове, обрану, ванјске послове, хрватске бранитеље, цивилну заштиту, заштиту околиша, финанције, правосуђе, здравство, море, промет и инфраструктуру; начелник Главног стожера Оружаних снага Републике Хрватске; главни равнатељ полиције; главни ватрогасни заповједник; предстојник Уреда Вијећа за националну сигурност; равнатељ Сигурносно-обавјештајне агенције, равнатељ Војне сигурносно-обавјештајне агенције и равнатељ Завода за сигурност информацијских система (Закон о систему домовинске сигурности, 2017).

У складу са садашњом организацијом и надлежностима организационих делова система националне безбедности Републике Србије логичним се чини да организацијска целина за безбедносну аналитику (нпр. Координациони центар) буде у саставу Савета за националну безбедност. У **Прилогу 4** дата је могућа структура Координационог центра за безбедносну аналитику.

2.5 Примена теоријског модела безбедносне аналитике у супротстављању тероризму

Ослањајући се на све напред наведено може се рећи да теоријски модел безбедносне аналитике израђен на секторском приступу безбедности подразумева сарадњу између различитих чинилаца сектора безбедности (служби, агенција, министарстава итд.) у циљу креирања обавештајних производа на стратешком нивоу који имају значај за националну безбедност. Овај модел обухвата процедуре које имају своје сличности са ПОМ-ом и обавештајним циклусом, с тим да се фазе аналитичког процеса додатно разрађују на следећи начин: постављање аналитичког задатка, прикупљање података у различитим секторима безбедности, обрада података; провера података; архивирање у базама података; размена (између различитих обавештајних и необавештајних организација) и дисеминација односно достављање података политичком руководству. Претпоставка је ослањање на постојеће знање (доктрину) која већ постоји у различитим секторима безбедности. Кроз цео овај процес морају се поштовати потребни стандарди који уједно чине и контролни механизам, а за то је потребно на основу већ постојећих стандарда

прописати и усвојити аналитичке стандарде. Да би све ово могло да се реализује неопходно је креирати координационо тело или угледајући се на *Америчку обавештајну заједницу* одредити координатора ових процеса који би испратио спровођење стандарда у пракси. Резултати стратешке безбедносне аналитике би били обавештајни производи који би садржали податке од виталног значаја за одбрану националне безбедности.

У истраживању за потребе дисертације утврђено је да ће се теоријски модел безбедносне аналитике приказати на примеру супротстављања тероризму. Ово из основног разлога што је тероризам у свим познатим стратегијама националне безбедности држава света препознат као једна од највећих претњи безбедности, како националној, тако и међународној.

2.5.1 Тероризам као претња безбедности

Данас, врло често можемо да чујемо да се у безбедносним расправама и разговорима користи синтагма *изазови, ризици и претње безбедности*. Иако се изазови, ризици и претње користе заједно, ова три термина не означавају исто и то не само у лексичком већ и у научном смислу. Претња је најексплицитнији облик опасности и означава конкретну лошу намеру да се неко или нешто повреди или уништи. Има највећи ниво деструктивности и означава да ће се опасност испољити у кратком року уколико се не спречи адекватном реакцијом. Претња обично долази са позиције силе и *a priori* има негативан контекст. Претња мора такође имати реалну могућност да се испољи.

Данас је тероризам једна од водећих претњи безбедности како појединачним државама тако и целом свету. Чини се да је тероризам у све већој експанзији из дана у дан. Остали су упамћени брутални напади у Паризу, Бриселу, Ници, Берлину, Истамбулу, као и велики број напада који се догодио на Блиском истоку. Можемо рећи да је тероризам пошаст нашег доба и глобална претња која захтева мултидисциплинаран приступ.

„Један од значајних историјских момената који је ставио акценат на савремене безбедносне изазове, ризике и претње је терористички напад на тржни центар у САД 2001. године. Овај терористички напад алармирао је цео свет и може се рећи да је то преломни тренутак од када тероризам постаје највећа глобална претња безбедности од које ниједна држава није безбедна. Од напада на Светски трговински центар терористичке активности

су постајале динамичније, организованије и софистицираније у погледу метода и употребе савремених технологија. Терористичке организације су добиле транснационални карактер и међународни значај тако што су показале да могу угрозити велесиле попут Америке и Русије“ (Андрић и Ковач, 2021: 108).

„Проблем код тероризма је што не постоји општеприхваћена дефиниција како међу стручњацима који се баве овом темом тако и у оквиру међународних организација и између држава. С друге стране, данас се више него икада говори о тероризму. Тероризам је највећа претња безбедности 21. века, али уједно и изазов у економском, моралном и културном смислу. То је сложен феномен који има много појавних облика и који карактеришу динамичност и променљивост. Ипак, оно око чега нема расправе јесте то да је тероризам увек облик политичког насиља“ (Андрић и Ковач, 2021: 110).

„Према Коксу (Cox), савремени тероризам обухвата употребу силе или насиља, пошто сама претња не производи терор, иако многи истраживачи у овом пољу описују тероризам као употребу или претњу насиљем под специфичним околностима у специфичне сврхе“ (Wolf & Frankel, 2007: 255).

Драган Симеуновић дао је своју дефиницију савременог тероризма. Овај аутор наводи следеће:

> „Као вишедимензионални политички феномен, савремени тероризам се може теоријски најопштије одредити као сложени облик огранизованог групног и, ређе, индивидуалног или институционалног политичког насиља обележен застрашујућим брахијално-физичким и психолошким методама политичке борбе којима се обично у време политичких и економских криза, а ретко у условима остварене економске и политичке стабилности једног друштва, систематски покушавају остварити ’,велики циљеви’ на начин непримерен датим условима, пре свега друштвеној ситуацији и историјским могућностима оних који га као политичку стратегију упражњавају“ (Симеуновић, 2009: 38).

„Тероризам је упечатљива политичка појава и он увек настаје са политичким мотивима и увек егзистира у пољу политике и уколико не постоји политичка мотивисаност или политички циљ, не може се говорити о тероризму. Тероризам увек по правилу представља борбу против неке и нечије политике, против неке политичке власти и настојања заснивања сопствене власти и политика се њиме увек бави и то врло интензивно због његове злоћудности“ (Симеуновић, 2009: 66–73).

„Тероризам за собом оставља несагледиве деструктивне последице, које се испољавају кроз три димензије државног живота: људску, безбедносну и економску. Када

је реч о људској димензији, она се манифестује кроз грубо кршење људских права многих како директних тако и индиректних жртава тероризма. Безбедносна димензија, која се односи за угрожавање националне безбедности кроз успоравање и гушење демократизације друштава која пролазе кроз процес транзиције, подривањем демократских тековина и институција, владавине права и конституисањем многобројних социо-економских потешкоћа. Државне институције које су слабе и захваћене корупцијом, као и неодговарајућа законска регулатива, значајно онемогућавају успешно супротстављање овом проблему, а крајњи резултат је унутрашње и спољно угрожавање националне безбедности. Када говоримо о економској димензији, треба рећи да се она односи на ефекте терористичких аката који додатно поспешују негативне и неповољне детерминанте економске транзиције и развоја, а који су само један од услова и узрока његовог настанка“ (Милашиновић и Мијалковић, 2005: 5).

„Модерни тероризам одликују бројни појавни облици, методе, мотиви и тактике деловања, као и последице са којима капацитети појединих држава, органа и институција не могу да се адекватно супротставе, тако да су и директни поводи за особене терористичке акте веома разноврсни, бројни и у великом броју случајева несхваћени. Тероризам услед процеса глобализације, техничко-технолошке и транспортне експанзије, све лакше и несметаније делује изван граница држава и тиме озбиљно урушава не само националну, тј. безбедност конкретне државе, већ и глобалну безбедност“ (Добовшек и Јунг, 2013: 26).

Када говоримо о средствима извршења терористичких напада, она су јако значајна у истражним радњама органа који су задужени за борбу против тероризма. Терористи ће увек изабрати убојитије, застрашујуће и оружје које ће допринети ширењу панике (на пример, биолошко или нуклеарно оружје). Међутим, неће увек имати на располагању идеално оружје. Због тога некада користе неко средство само зато што немају могућност да користе оно које би заправо желели, али пракса је показала да често постоји устаљен образац у коришћењу одређених средстава код исте терористичке организације. На пример, коришћење експлозива или бомби код самоубилачких терористичких напада. У погледу средстава које користе терористи или имају намеру да користе, Симеуновић прави разлику између класичног (конвенционалног), биохемијског и нуклеарног тероризма. Док према методама које користе терористи разликује: класични,

самоубилачки, сајбер и нарко-тероризам (Добовшек и Јунг, 2013), где у последње време, због развоја савремених технологија, изузетно значајан постаје сајбер тероризам.

Сајбер тероризам се сматра кривичним делом, извршеним употребом компјутера и телекомуникационих средстава, које доводи до уништавања и/или прекида услуга како би се створио страх у датој популацији, а у циљу утицања на владу или становништво да се повинује одређеној политичкој, друштвеној или идеолошкој агенди (Пујари, 2016).

„У овом тренутку трошкови ресурса, прикупљања обавештајних података и организовања тако софистицираних операција премашују тренутне могућности оваквих активиста за спровођење софистицираних или ефикасних сајбер напада. Међутим, могуће је регрутовати способније актере из ‚подземног тржишта' за компјутерске експлоатације и на тај начин се лако могу повећати ограничени капацитети сајбер терористе. Стога је вероватно да ће се ниво оваквих претњи променити у наредној деценији2 (Балтазаревић и Балтазаревић, 2023: 179).

Често тежимо да утврдимо просторни распоред терористичких напада, њихове последице, смртност, порекло и финансирање терористичких организација, да ли су реакције на те нападе биле адекватне и оно што је најважније да предвидимо где, када и како би могао да се догоди следећи напад. Предиктивна функција оваквих анализа је разлог што се оне често изводе под претпоставком хитности, штуро и непотпуно. За овакву анализу потребан је значајан број проверених података до којих није лако доћи и то је разлог зашто је потребно сачекати да се такви подаци прикупе. У ту сврху постоји више база података које бележе податке везане за терористичке нападе (Андрић и Ковач, 2021). Ове базе биће описане у даљем тексту.

Борба против тероризма захтева посебну размену података између обавештајних система различитих држава, али и размену оваквих података са међународним организацијама и другим сличним актерима. Проблем настаје у томе што обавештајни субјекти нису увек заинтересовани да такве податке поделе. Такође, често постоје и неправилности у раду обавештајних структура на националном нивоу.

Бановић (2001) сматра да се процедура која се примењује у случају откривања и хватања терористе може класификовати у три фазе, које су међусобно зависне и повезане и настављау се једна на другу у ситуацији да се терористе не ухвати у некој претходној фази и оне осликавају једну специфичну целину у поступку проналажења, откривања и

хватања терористе. Грешке које настану у некој од фаза (попут непроверених и недовољних података на почетку истраге) могу утицати и на остале фазе. То нам говори да цео безбедносни систем мора да ради координирано, повезано и једнако добро, а то у пракси често није случај.

Карактеристика савременог тероризма поред екстремистичких основа су нове методе како врбовања тако и борбе. Бојно поље се све више премешта из реалног у виртуелни свет. Технологије које користе терористи неретко су напредније од оних које користе они који се против тероризма боре. Тако је борцима против тероризма у недостатку обученог кадра или неусклађености система безбедности са новим технологијама често тешко да балговремено дођу до значајних информација о потенцијалним терористичким нападима. Такође треба нагласити да, иако је борба против тероризма међународна категорија, она ипак полази од локалних средина и укључивање локалних обавештајних и полицијских структура је изузетно значајно. Радикалне, превентивне мере нису примењиве свуда, али систем раног упозоравања, који укључује и шире становништво је свакако шанса да се дође до више неопходних информација. Благовремене информације о потенцијалним терористима и планираним нападима су први зид одбране, а када говоримо о информацијама, поред безбедносно-обавештајних структура и становништва у ову битку морају се укључити и медији и различити научно-истраживачки центри.

С обзиром на значај који има тероризам као претња безбедности која представља сложен облик политичког насиља и да се борба против тероризма заснива на обавештајном деловању, он може бити идеалан пример на коме се може приказати теоријски модел безбедносне аналитике.

2.5.2 Општи – теоријски аспект примене теоријског модел безбедносне аналитике у супротстављању тероризму

Теоријски модел безбедносне аналитике, како смо описали, јесте скуп знања и вештина, тј. доктрина. Дакле, знање је база за тај модел. Као база модела, знање – доктрина безбедносне аналитике у домену супротстављања тероризму постаје кључни елемент рада безбедносних аналитичара. У свету су познате и примењене у пракси бројне базе за супротстављање тероризму, од којих ћемо приказати најзначајније, а које се

користе у нашем окружењу и у Републици Србији. Пре тога следи краћи осврт на примену теоријског модела безбедносне аналитике на супротстављање тероризму.

„Обавештајни рад је један од стубова националне безбедности. Покривајући широк дијапазон изазова, ризика и претњи безбедности и одговарајући на захтеве претпостављених, обавештајне службе имају велику улогу у усмеравању одлука политичког, војног и безбедносног руководства. Један од кључних претњи националној безбедности многих држава као облик политичког насиља јесте тероризам. Борба против тероризма може да се води на два фронта, први је превентивно деловање, а други постактивно. Оба начина реаговања на тероризам као угрожавајућу појаву заснивају се на поседовању информација“ (Андрић и Терзић, 2023: 5). Ово, између осталог, подразумева посматрање садржаја снимка и посматрање понашања личности које се појављују на аудио-визуелним снимцима. Такође, и средства јавних информисања могу бити значајан извор обавештајних сазнања. Зато су обавештајне службе заинтересоване за штампу, различите публикације, радио и ТВ емисије, различите извештаје, чак и за научне радове. На пример, пажњу служби безбедности у једном периоду привлачили су научни радови и истраживања на тему атомске енергије или усавршавања ракетног горива, данас би то могли бити радови из области биотероризма. Ово нас наводи на закључак да су подаци из јавно доступних извора тзв. ОСИНТ подаци изузетно значајни за супротстављање тероризму.

Супротстављање тероризму као претњи безбеднсти уз помоћ безбедносне аналитике у теорији описан је у тексту који следи.

2.5.2.1 Свеукупно знање о тероризму и зони интересовања (доктрина)

Знање мора обухватати сазнање из различитих дисциплина. Потребно је познавати и историјат развоја тероризма од његових претеча до савремених облика. С друге стране, потребно је познавати и историјске и културолошке карактеристике одређеног подручја и региона који представља зону интересовања, као и више језика. Затим, потребно је познавати потенцијалне утицаје који се могу преламати на одређеном простору. На пример, припадници неког огранка Исламске државе, који имају повезнице на простору Косова и Метохије, могу обилазити споменике у центру Београда и у на први поглед

туристичком разгледању града могу разматрати на арапском језику где би било идеално поставити експлозивну направу. Дакле, потребно је познавање и других језика и култура. Улазак оваквих лица у државу мора бити испраћен, а да би се то могло спровести на адекватан начин, потребно је поседовати широко знање. Осим свега онога везаног за тероризам од историјских, културолошких, религијских и националних специфичности, безбедносни аналитичар мора бити упознат и са безбедносним окружењем и другим претњама безбедности, као и географским карактеристикама зоне интересовања и региона око ње. Мора адекватно руковати савременим технологијама које су значајне не само са аспекта сајбер тероризма, већ и са аспекта комуникације међу терористима. Потребно је да познаје геополитичка дешавања, социјалне, економске и друге прилике. Дакле, знање мора обухватати све описане секторе безбедности: политички, војни, економски, социјетални и еколошки.

2.5.2.2 Процедуре у супротстављању тероризму

Друштво се против тероризма мора борити свим расположивим средствима, а средства која се користе у тој борби морају се константно унапређивати. Оспособљеност и спремност за реаговање на изазове тероризма се најчешће испољава кроз разноврсне програме организовања, сталним праћењем научних достигнућа из домена друштвених, војних и техничких наука; врхунску, квалитетну обуку и савремено опремање јединица за противтерористичка дејства; подизање на виши ниво система мера за одвраћање терористичких активности и на тај начин настоји учвршћивати и јачати унутрашњу снагу и способност друштва за наставак демократских процеса анализом досадашњих искустава у антитерористичкој делатности.

„Деловање државних органа у сузбијању тероризма треба да буде потпомогнуто укључивањем и ангажовањем грађана и неких њихових удружења и група, тј. субјеката који се појављују као веома битни носиоци превентивних активности и задатака, односно свих оних делатности које су биле у стриктној надлежности државних органа“ (Кривокапић, 2012: 2).

У борби против савременог тероризма користе се устаљене процедуре и у смислу превенције и реакције на конкретан терористички акт. Када је у питању превенција, изузетно је важно сазнати за деловање одређене терористичке организације и припремање теористичког акта. Потребно је спречити да дође до извршења терористичког напада и предупредити га. С друге стране, уколико пак дође до терористичког напада, потребно је извршити његову анализу како би се уочили пропусти који су довели до његовог извршења и како би се евентуално могло предвидети где и када би могао да се догоди следећи напад. Стога је прикупљање и обрада података о теористичким организацијама, лидерима и планираним терористичким активностима суштина ове борбе.

„Држава и њене безбедносне службе су паралелно са развојем у стратегији деловања терористе почеле да раде на прилагођавању у сфери борбе на његовом сузбијању, а са данашњег аспекта модел борбе против тероризма садржи у себи следеће мере: супротстављање нападима терористе формирањем специјалних јединица са задатком ефикасне и правовремене интервенције у случају напада, примена преговарачких техника и метода у талачким ситуацијама, разноврсне облике заштите потенцијалних терористичких циљева, као нпр. дипломатких представништава, војних база, ваздушног саобраћаја, затим размену обавештајних информација држава, модернизовани и софистицирани системи надзора и праћења терористичких активности, са циљем да до напада и не дође, као и ради хватања терористе након извршеног напада, затим формирање јединствене базе података о терористима, борба и сузбијање финансирања терористичких активности“ (Маринковић и Ђурђевић, 2013: 67).

Када је у питању превенција терористичког деловања, безбедносна аналитика може имати кључну уогу. Оне процедуре које се спроводе у пракси до сада не садрже стандардизоване процесе који се односе посебно на област тероризма, већ се подаци прикупљају по принципу обевештајног циклуса.

Обавештајни циклус у борби против тероризма има своје специфичности:

Пријем задатка и планирање:

„Фаза утврђивања обавештајних потреба је фаза у којој непосредно учествује политички естаблишмент. У зависности од стратешких националних интереса и приоритета у спољној политици или неких конкретних спољнополитичких акција, они доносе одлуке о тренутним и дугорочним обавештајним потребама. У том смислу,

политички естаблишмент доноси одлуку о предмету обавештајног истраживања ради прибављања обавештајних сазнања, неопходних за успешно спровођење активности на спољнополитичком плану“ (Крштенић и Матијашевић, 2014: 113).

Тероризам је претња која је препозната на стратешком нивоу. Република Србија препознаје тероризам као претњу по основне вредности на којима почива, као што су владавина права, људска права и демократија, укључујући слободу, мир и безбедност грађана, суверенитет и територијални интегритет, стабилност и безбедност државе и легитимно изабраних власти, као и међународни мир и безбедност међународне заједнице, наводи се у Националној стратегији за спречавање и борбу против тероризма за период 2017-2021. годину (*Службени гласник РС*, бр. 19/2017).

С обзиром на то тероризам је претња која захтева константан обавештајни рад. У том смислу могу се пратити екстремистичке групе, странци који долазе из ратом захваћених подручја или, на пример, мигранти који се последњих година крећу и преко територије наше земље. Дакле, обавештајне службе имају задатак да владају материјом у овој области иако не постоје озбиљне индиције да би могло доћи до терористичког напада. Међутим, када оперативни подаци покажу да је, на пример, појачана активност екстремистичких организација или било која друга активност која може водити ка тероризму, могу се издати посебна наређења у смислу обавештајних задатака.

„Политичко руководство издаје задатке који имају за крајњи циљ спречавање терористичких аката. Естаблишмент који је надлежан за доношење одлука на највишем нивоу упознаје обавештајне стручњаке са својим обавештајним потребама и износи им конкретне захтеве. Захтеви и потребе који су утврђени овим путем представљају улазну информацију за фазу планирања и организовања обавештајног истраживања“ (Крштенић и Матијашевић, 2014: 113).

Овде треба имати у виду да постоје два нивоа издавања задатака, и то 1) задаци које издаје политичко (војно) руководство и (2) задаци које издаје руководство обавештајне службе (Форца и Аночић, 2018). Пријемом задатака везаних за тероризама започиње обавештајни циклус у борби против истог, након чега следи израда плана прикупљања података. У овом плану задаци се даље разрађују у складу са обавештајним снагама, средствима и изворима које обавештајна служба поседује. Потом се задаци додељују различитим изворима и агенцијама, у складу са њиховим могућностима.

Прикупљање информација и података

„Значајна фаза планирања је и одлука обавештајне службе који ће се методи, то јест обавештајне прикупљачке дисциплине/поступци изабрати (једна или више њих), а који ће гарантовати успешно прикупљање правовремених обавештајних информација високог степена тачности, свеобухватности и провереностиˮ(Бајагић, 2015: 169).

„Сви методи прикупљања података, начелно, могу се поделити у следеће категорије:

- обавештајно-оперативним радом,
- применом техничких средстава и
- коришћењем отворених извораˮ (Форца и Аночић, 2018: 149).

Обавештајно-оперативни рад на терену може бити изузетно захтеван, али и значајан када је у питању тероризам, с обзиром на то да се терористичке организације често и саме понашају као обавештајне службе. Иако нема атрибуте институционализованости, обавештајно-безбедносна компонента терористичких организација примењује сличне методе као и обавештајна и безбедносна служба. Разлози њеног постојања и деловања су пружање максималне „информационе и акционе логистикеˮ специјализованим извршиоцима терористичких аката, односно безбедносна заштита терористичке организације од „провалијивањаˮ, пресецања терористичких активности и од хапшења њених припадника (Мијалковић, 2010).

„Због наведеног обавештајни рад у борби против тероризма може имати и особине контраобавештајног рада. У том смислу оперативни контакт или инфилтрација у редове терористичких организација могу бити драгоцени.Терористичке организације се ослањају у великој мери на тајност и анонимност да би извршиле своје верске и политички вођене програме, а прикупљање обавештајних података и експлоатација су најпогоднији за скидање овог критичног слоја заштите чинећи их рањивијим на инфилтрацију, истраге и хапшењаˮ (Hughbank & Githens, 2010: 35).

„Када је реч о примени техичких средства, треба нагласити да велики број терориста поседује обимно и стручно знање када су у питању комуникације путем техничких средстава. Поред тога поседују и потребна техничка средства и изузетно су домишљати

када треба да остваре комуникацију, пренесу поруку или изврше трансакцију новца. Познати су примери где су терористи комуницирали међусобно путем *драфт* порука преко мејла, али и да су користили видео-игре на много сложенији начин него што би се могло претпоставити да су способни. Колико су терористи испратили технолошки напредак говори нам и чињеница да се често окрећу хаковању и сајбер ратовању, за шта је потребна озбиљна умешност“ (Андрић и Терзић, 2023: 8).

Табела 19. *Примери метода прикупљања података у борби против тероризма*

ПРИМЕРИ МЕТОДА ПРИКУПЉАЊА ПОДАТАКА У БОРБИ ПРОТИВ ТЕРОРИЗМА	
Обавештајно-оперативни рад	- праћење, - директан разговор, - провера и претрага терена; - инфилтрација у терористичке организације.
Применом техничких средстава	- прислушкивање, - снимање, - сателитско праћење; - примена технологија за праћење интернет комуникација..
Коришћењем отворених извора	- посећивање верских сајтова који се користе за врбовање нових чланова, - медији, - отворене научне базе података о тероризму.

Извор: *Андрић и Терзић, 2023.*

У пракси се методе прикупљања података најчешће комбинују и до података се долази из више извора, што је најчешће случај и када је тероризам у питању.

Аналитика и израда обавештајних производа

Прикупљени подаци о некој безбедносној појави се често називају „сирови“ или необрађени подаци. Да би податак прешао у информацију мора да прође кроз фазу обраде. Ово је интелектуално најзахтевнија фаза и спада у домен оперативне безбедносне аналитике. Тако Даниловић и Милосављевић наводе да „под оперативном (оперативно-интервентном) аналитиком подразумевамо интелектуалне радње које, у склопу редовних оперативних послова, обављају припадници система безбедности“ (Даниловић и Милосављевић, 2008: 28).

Људски фактор односно рад аналитичара је примаран у овој фази обавештајног циклуса, али он може бити помогнут техничким средствима и базама података. На

почетку ове фазе подаци се сортирају и групишу. Задатак аналитичара је и да оцени извор из ког долази подата његову поузданост и да се одреди поверљивост датог податка. Ово ће аналитичару омогућити да лакше донесе закључке.

Након груписања и сортирања података врши се њихова корелација и анализа. Нови обавештајни подаци се повезују са оним који су постојали пре њиховог прибављања и упоређују са почетном претпоставком. Обрада података је интелектуана радња која се умногоме ослања на способности, знање и интуицију онога ко је спроводи. Крајњи излаз из ове фазе јесте обавештајни производ. „Потребно је истаћи да ‚обавештајни производ', као резултат ове фазе обавештајног циклуса, може имати четири нивоа, и то:

- израда обавештајне информације о догађајима који су се већ одиграли,
- израда обавештајне информације о догађајима и процесима који се управо одвијају и
- израда обавештајне процене о могућем развоју догађаја у будућности" (Форца и Аночић, 2018: 158).

Поред тога што аналитика треба да дође до закључака о томе шта се дешава или шта се већ догодило, може да да одговоре и на питања шта ће се догодити. Поред превентивне и постактивне, има и предиктивну улогу. Ова улога је изузетно значајна када је у питању борба против тероризма јер је од виталне важности предвидети где, када и како би могао да се догоди следећи напад. За тако нешто је потребно да аналитичар који се бави оваквом врстом предикција одлично познаје проблематику тероризма и савремене трендове када је у питању тероризам не само у сопственој земљи већ и у иностранству.

Ова фаза обавештајног циклуса се завршава са израдом обавештајног производа, а то је обавештајна информација или обавештајна процена о терористичким активностима, плановима и слично. Након израде обавештајног производа следи фаза дисеминације, доставе обавештајног производа крајњем кориснику.

Дисеминација обавештајних производа

Достава обавештајних производа до крајних корисника је једна од завршних фаза обавештајног циклуса. Битно је да се производи доставе благовремено, у супротном неће имати вредност. Како би политичко, војно и безбедносно руководство државе донело

адекватне одлуке, оно мора имати не само проверене и тачне информације, већ их мора имати у правом тренутку.

„Начини достављања обавештајне информације и обавештајне процене корисницима могу имати различите форме: писани обавештајни извештај, хитна порука, обавештајни преглед или, углавном у хитним случајевима, усмени извештај политичком лидеру или команданту“ (Форца и Аночић, 2018: 155). Када је у питању тероризам, откривени подаци често могу имати префикс хитности и у том случају се процес скраћује, а претпостављени обавештавају без устаљених поступака. Такође, информације о тероризму до којих се долази током обавештајног циклуса могу бити значајне и за друге државе или иностране обавештајне агенције, али и за домаће органе и институције на локалном нивоу. „Аналитички материјали се сачињавају и за потребе екстерног извештавања и информисања највиших органа власти у Републици, других државних органа, органа локалне самоуправе, али и међународних тела и организација и др.“(Рацић, 2018: 145).

Повратна информација

За обавештајне аналитичаре значајно је да добију повратну информацију о резултатима свог рада, о томе какви су поступци и процедуре предузети након достављања информације и какве даље импликације је она имала на националну безбедност државе. Када је тероризам у питању, посебно је значајно да обавештајни субјекти буду информисани о поменутим ефектима како би могли да отклоне неправилности у свом раду, а да задрже методе које воде ка спречавању тероризма.

„Сазнање да је наша информација била корисна (у најширем значењу тог појма) или да смо, с друге стране, ‚потпуно промашили тему' врло је битно за наш даљи рад и усмеравање како прикупљачких тако и капацитета за израду обавештајних производа“ (Форца и Аночић, 2018: 156). Тако Рацић (2018), на пример, наводи да се улога „Одељења за аналитику (МУП) може препознати и у оцени имплементације самих криминалистичко-обавештајних информација. То би практично значило да је неопходно донети одговарајући методолошки поступак на основу којег би се вршило оцењивање степена имплементације криминалистичко-обавештајних информација и њихових ефеката“ (стр. 146).

На крају можемо додати да су за све активности у току обавештајног циклуса задужени различити субјекти (Табела 20). Како би цео процес био успешан неопходна је добра сарадња између свих актера, а како се види из приложене табеле и њихова сарадња је циклична.

Табела 20. *Активности у склопу обавештајног циклуса и субјекти који их спорводе*

АКТИВНОСТ	СУБЈЕКТ КОЈИ СПРОВОДИ АКТИВНОСТ
Издавање задатака	**Политичко и/или војно руководство**
Пријем задатака и планирање	**Обавештајно руководство, обавештајни штаб**
Прикупљање података	**Оперативци – обавештајци**
Производња обавештајних информација – аналитика	**Безбедносни аналитичари**
Достављање обавештајних информација корисницима	**Обавештајно руководство, обавештајни штаб**
Давање повратне информације	**Политичко и/или војно руководство**

Извор: *Обрада ауторке дисертације*

Када сагледамо ове фазе можемо закључити да се обавештајни циклус у потпуности може применити и на проблем тероризма.

Неке од специфичности обавештајног циклуса у борби против тероризма јесу следеће:

- С обзиром на то да је спречавање тероризма утврђено на стратешком нивоу обавештајне службе у склопу својих редовних активности баве се прикупљањем података о појавама везаним за тероризам и без посебно издатих задатака.
- Тероризам рачуна на фактор изненађења и у те сврхе развија и сопствени обавештајни апарат, није лако благовремено доћи до потребних информација и зато обавештајни циклус неретко може бити скраћен како би се информације хитно доставиле претпостављенима и може имати контраобавештајни карактер.
- Феномен са пуно појавних облика какав је тероризам захтева посебно обучене и аналитичаре са натпросечним познавањем овог феномена.

- Подаци до којих дођу обавештајне службе, а који су везани за тероризам, могу бити предмет међународне сарадње и на тај начин бити уступљени и изван надлежности једне државе.

На крају се може закључити *да је обавештајни циклус у супротстављању тероризму не само применљив, већ и од изузетне важности. Оно где има простора за даљи напредак јесте додатни развој аналитичких метода специјализованих за рад са подацима везаним за тероризам и развој курсева и програма усавршавања за аналитичаре који се баве проблемом тероризма. За то су такође потребни додатни научни напори да се сачини теоријски оквир безбедносне аналитике.*

2.5.2.3 Стандарди у супротстављању тероризму

Модел безбедносне аналитике који би био применљив на супротстављање тероризму мора обухватати и одређене стандарде којих се треба придржавати у том процесу. Борба против тероризма је комплексна због мноштва појавних облика овог феномена. Ти различити појавни облици се не односе само на различите приступе безбедности, већ и на културолошке и верске разлике које могу бити укључене. Тероризам је претња безбедности која се може испољити у свим секторима безбедности (економском, војном, еколошком, социјеталном...). Стога у овај модел безбедносне аналитике треба укључити и стандарде из ових сектора који су већ раније описани. Навешћемо неке од кључних стандарда који се морају поштовати приликом прикупљања и обраде података везаних за терористичке претње:

- ISO 22301 – Систем менаџмента континуитетом пословања који даје оквир за идентификацију потенцијалних спољних и унутрашњих претњи које могу угрозити организацију. Овај стандард везан је за економску безбедност и бави се способношћу организације да настави испоруку производа или услуга на прихватљивим, унапред дефинисаним нивоима након инцидента, то у случају терористичке претње значи креирање плана како одржати континуитет функционисања државе након терористичких напада. Дакле, потребно је предвидети потенцијалне теористичке нападе који би могли доћи споља и изнутра и креирати агенду како такве нападе превазићи и умањити њихове последице како би се омогућио континуитет у функционисању државе.
- У еколошкој безбедности значајан је ISO/TCTЦ 207 (Еколошки менаџмент), који је фокусиран на системе управљања животном средином, као и серија стандарда ISOИCO 14001. Када је теоризам у питању, примена ових стандарда значајна је са аспекта

биотероризма који може озбиљно угрозити и загадити животну средину, а који постаје све присутнији код савременог тероризма.

- Два стандарда која су значајна за људску безбедност, али која могу бити значајна и за безбедносну аналитику у супротстављању тероризму су ISO 22341 (Безбедност и отпорност) и ISO 27001 (Заштита и безбедност информација). Стандард који дефинитивно треба уврстити у теоријски модел безбедносне аналитике, а који такође може допринети и спречавању тероризма јесте ISO/IEC 27001:2013. Овај стандард представља систем менаџмента безбедности информација и односи се на процес заштите и употребе информација у различитим организацијама, приватним и јавним компанијама. Такође, са аспекта друштвене безбедности значајно је поменути и стандард ISO 22311:2017 Друштвена безбедност – видео-надзор – излазна интероперабилност.
- ISO 26000 (Водич о друштвеној одговорности) доприноси отклањању родне пристрасности и обезбеђује равноправан положај жена и мушкараца у погледу запошљавања, напредовање у каријери и приход у оквиру пословних система и институција. Ово је посебно значајно када је у питању превенција тероризма, где би већа друштвена одговорност могла да спречи разлике у друштву које посредно могу бити покретачи или погодно тло за терористичко деловање.
- И напослетку, можда и најзначајни за модел безбедносне аналитике у супротстављању тероризму, могу бити стандарди за аналитичке процесе које је прописала Америчка обавештајна заједница. *Овде се наводе кључни стандарди који треба да буду испоштовани у процесу безбедносне аналитике, а то су: објективност, независност од политичких разматрања, правовременост, заснованост на свим доступним изворима обавештајних информација и томе слично*. Ови принципи свакако морају бити укључени у процес безбедносне аналитике у супротстављању тероризму.

Поред наведених стандарда из различитих области потребно је и извршити додатни процес стандардизације у области безбедносне аналитике како би се јасно поставила како овлашћења тако и ограничења у раду. На пример, зарад борбе против тероризма не сме да трпи људска безбедност. У том процесу морају бити испоштована и права сваког појединца на приватност. С друге стране, пожељно је у процес прикупљања података везаних за тероризам укључити и шире становништво, што је потврдио и концепт полиције у заједници. Овде треба наћи баланс између задирања у приватност, а истовременог мотивисања грађана за укључивање у ове процесе.

2.5.2.4 Базе података – општи аспект

Као посебан елемент модела безбедносне аналитике, а посебно када је тероризам у питању, треба размотрити базе података. Базе података могу бити значајне на два начина за безбедносну аналитику. Као елемент модела безебедносне аналитике могу се односити на посебну фазу складиштења и чувања података. Свака организација која прикупља и

обрађује податке мора имати свој начин архивирања података, како би се њима могло приступити касније. Раније су такви подаци потрхањивани у аналогном облику и у архивима. У савременом контексту такви подаци се чувају у специјализованим дигиталним базама података, софтверским базама података. Овакав облик чувања података омогућава њихову лакшу претрагу, корелацију, проверу и допуну. С друге стране, базе података, посебно научне базе, могу да се користе као отворен извор података. Многи универзитети и научно-истраживачке организације и институције су креирале научне базе података од којих су неке полуотворене (доступне само за научну заједницу), а неке потпуно отворене. Овакве базе података се могу сматрати ОСИНТ подацима од значаја, посебно када је у питању борба против тероризма. Постоји више научних база података које се баве праћењем статистике и трендова везаних за терористичке нападе који су већ описани.

Конкретнији и детаљнији приступ базама података у супротстављању тероризму дат је у каснијем тексту.

2.5.3 Посебан – практични аспект примене теоријског модела безбедносне аналитике у супротстављању тероризму

Суштина теоријског модела безбедносне аналитике који је предмет ове дисертације приказана је у претходном тексту. Шема показује да је основа безбедносне аналитике укупно знање којим треба да овладају безбедносни аналитичари. То знање мора да обухвата како знање из различитих сектора безбедности тако и познавање процедура и стандарда који се односе на безбедносну аналитику. Овако постављена шема делује једноставно, али у реалности је доста сложенија. Додатно када је у питању сложен облик политичког насиља попут тероризма потребно је и додатно знање и познавање овог феномена.

У овој дисертацији говоримо о безбедносној аналитици на стратешком нивоу. Дакле, о аналитици која се бави питањима од значаја за националну безбедност. Таква аналитка представља свеобухват различитих компоненти и сектора безбедности и мора укључивати различите организације и појединце који се баве прикупљањем података. Као резултат рада безбедносне аналитика на стратешком нивоу долазе аналитички производи који се достављају политичком руководству и на основу којих оно предузима даље активности. Све оно што се

дешава у различитим секторима безбедности, а може имати утицај на националну безбедност, мора бити обрађено кроз овај процес. То даље имплицира да је за успостављање безбедносне аналитике на стратешком нивоу неопходна међусекторска сарадња, а посебно сарадња служби безбедности. БИА, ВОА, ВБА, различите агенције и институције од значаја у Републици Србији морају сарађивати по кључним питањима и размењивати информације што у пракси значи да је неопходно одређи се дела информација у корист друге службе како би се дошло до остварења заједничког циља.

У пракси није једноставно остварити наведено из пошто постоји устаљена пракса и систем рада. Такође, не постоји довољно воље да службе уступају своје податке другима. Због тога је неопходно формирати координациони центар за безбедносну аналитику (Види: Графикон 4) за све службе безбедности и све агенције и институције које могу имати значајне податке (МУП, Управа царина, Агенција за спречавање корупције, Министарство спољних послова и слично), који би обједињавао податке и надзирао рад свих ових елемената. Било би то нешто попут Америчке обавештајне заједнице коју смо претходно описали. Да би тако нешто могло да се формира, потребна је политичка воља, реорганизација система безбедности и прописивање пратећих докумената, планова, стратегија и законских аката који би све наведено уредили. Стога је предлог изложен у овој дисертацији, а који је настао на основу реалних потреба, назван теоријски модел безбедносне аналитике.

Како бисмо што реалније приказали те потребе, узели смо пример тероризма. Тероризам је сложен облик политичког насиља који је динамичан, променљив и који се простире подједнако на све секторе безбедности. Тероризам као претња може угрозити подједнако економски и еколошки сектор кроз, на пример, сајбер нападе на народну банку или биотероризам који ће угрозити животну средину. Такође, може угрозити и војни сектор тако што ће извршити низ напада на војне објекте или изазвати друштвену нестабилност кроз учестале нападе на јавне објекте. Тероризам може изазвати и нестабилност у политичком и друштвеном сектору безбедности. Да би држава адекватно одговорила на овакву претњу, мора имати поуздане податке који могу бити од значаја за супротстављање тероризму из свих сектора безбедности. Да би се то остватило мора постојати и сарадња и координација таквог процеса.

Безбедносна аналитика се користи за идентификацију и процену потенцијалних претњи безбедности и предвиђање будућих инцидената. У контексту спречавања терористичких

напада безбедносна аналитика се фокусира на прикупљање и обраду података који могу допринети разумевању методологија терористичких група, тактика, техника и процедура које користе у свом деловању, те резултат може бити препознавање образаца понашања и савладавање изазова у превенцији терористичких напада.

Аналитички производи код тероризма, између осталог, могу нам указати и на следеће:

- начине и методе регрутације терористе,
- политичке, економске и културне факторе који могу допринети подстицању насиља и екстремизма и
- на то како се одвија развој тероризма у постконфликтним друштвима.

Да бисмо дошли до таквих резултата јасно је да се тероризму не може приступати само са војног и безбедносног аспекта. Морамо укључити психолошки приступ како бисмо разумели психолошке и идеолошке факторе који мотивишу појединца да постане терориста. Затим, да бисмо проучили утицај друштвених, културних, верских разлика у ширењу терористичких идеологија морамо користити и социолошки приступ. За истраживање финансијских терористичких мрежа и њихове улоге у извршењу конкретних напада потребан је економски приступ и томе слично. Дакле, модел безбедносне аналитике у супротстављању тероризму мора бити постављен интердисциплинарно.

Када би се наведени модел применио у пракси, на пример у Републици Србији, он би морао бити прилагођен постојећим институционалним оквирима као и законодавству, оперативним методама и доступним технологијама.

Посебан аспект примене теоријског модела безбедносне аналитике у пракси, а на примеру супротстављања тероризму, дат је у наставку текста.

2.5.3.1 Прикупљање података

„Домаће обавештајне агенције попут БИА, ВОА, ВБА, МУП-а имају дугу традицију прикупљања података из различитих извора: агентуре и обавештајци (ХУМИНТ), технички подаци (СИГИНТ) и други извори. Праћењем међународних трендова усвојени су и принципи из СОКТА документа, Полицијско-обавештајног модела и други савремени принципи који су применљиви на супротстављање тероризму. Поред оперативних веза,

присутно је и обавештајно истраживање, као и јединице задужене за обавештајну активност и криминалистичко-обавештајну аналитику“ (Ђурђевић и Радовић, 2012: 2).

Интернационална сарадња. Од посебног значаја за прикупљање података о терористичким организацијама је сарадња са међународним организацијама које се баве овим питањем попут Европола и Интерпола, али и сарадња и размена података о терористичким претњама у региону.

Анализа отворених извора података (ОСИНТ): У пракси би то значило прикупљање података са интернета, из научне литературе, медија и слично, То подразумева претрагу друштвених мрежа, форума, вести, па чак и анонимних онлајн комуникација, што постаје све важнији алат у борби против тероризма. У Србији би обавештајци, али и аналитичари из МУП-а, пратили комуникацију која може да укаже на терористичке активности, радикализацију или планирање напада.

2.5.3.2 Анализа података

„Контрола на којој се заснива аналитички процес јесте укупно знање (сазнање) о предметној проблематици. То је сазнање које сеже у сферу безбедности, конкретне безбедносне појаве која је подвргнута аналитици, као и сазнање о методама и техникама које се користе у раду аналитичара“ (Андрић и Тишма, 2022: 34).

„Истина се обично не открива у почетним подацима, већ у њиховом правилном схватању током обраде, јер конкретну чињеницу можемо разјаснити само заједно са другим чињеницама. Обрада информација, после претходног сакупљања чињеница и конкретне поставке проблема подразумева:

- систематизацију чињеница које се разврставају по степену односа према неком питању,
- проналажење кључних момената, ослањајући се на интуицију,
- постављање претпоставки којима се објашњавају основне чињенице;
- прикупљање, ако је неопходно, допунских података;
- формирање закључака и њихова провера у односу на усаглашеност с другим чињеницама“ (Ронин, 2009: 8).

У првом делу дисертације детаљније су објашњене аналитичке методе које се користе у безбедносној аналитици. Када је у питању тероризам, можемо издвојити анализу

образаца понашања, предиктивну аналитику и рачунарске симулације и мрежну анализу, Где се анализа образаца понашања користи за препознавање понављајућих образаца у понашању терористе. Могу се уочити, на пример, устаљене руте кретања, путовања терористе, чланство у радикалним организацима или одређене финансијске трансакције и активности на интернету.

„Приликом разјашњавања и откривања ове врсте дела, посебан акценат треба ставити на утврђивање мотива и намере учиниоца, као и на све чињенице и околности које су присутне на самом лицу места, што представља квалитетну базу за продуктиван даљи криминалистички рад“ (Бошковић, 1998: 217).

Предиктивна аналитика треба да нам омогући да предвидимо будуће терористичке нападе, мете и временски оквир за њихово извршење. Српске безбедносне агенције могу користити напредне технологије за анализу великих количина података, где се примењују алати за препознавање и класификацију образаца. Могу се користити и алгоритми машинског учења, који такве предикције могу дати на основу историјских података и тренутних уочених образаца.

Мрежна анализа у случају тероризма може да нам укаже на одређене интеракције међу члановима терористичких организација, финасијске и логистичке мреже и слично. У овој фази, аналитичари би могли да уоче везе између особа, организација и њихових ресурса. На пример, могли би анализирати финансијске трансакције, телефонске позиве, интернет комуникацију и путне обрасце како би се открили терористичке мреже и њихови симпатизери.

2.5.3.3 Достављање информација и реакција

С обзиром на то да је тероризам политички облик насиља који може представљати претњу по националну безбедност, обрађене информације морају се достављати највишем политичком руководству, које ће даље давати упуства. Међутим, ове информације се могу дистрибуирати и другим институцијама које се могу укључити у борбу против тероризма. Мора да постоји координација између свих актера који могу имати значаја по овом питању, односно између служби безбедности (БИА, ВОА, ВБА), полицијских органа, правосудних органа и других значајних организација, агенција и институција.

Информације се морају размењивати адекватно и уз поштовање стандарда, како би дошло до благовремене реакције.

„Треба нагласти и значај служби надлежних за контролу преласка државне границе, јер би управо они могли запазити потенцијално сумњиве особе и извршити одређене провере које ће или потврдити или елеминисати сумњу и самим тим у раној фази спречити потенцијални терористички напад“ (Гаћиновић, 2005: 200).

Када се препозна озбиљна претња или када аналитичари открију необичне активности, информације се хитно упућују на адресу одговарајуће надлежне институције која може да реши ситуацију. На пример, уколико се дође до открића плана напада или идентификације терористичке ћелије, МУП и БИА ће одмах реаговати координисано.

Безбедносна аналитика у спречавању тероризма има двојаку улогу. Прва је превентивног карактера и односи се на анализе настале пре извршења терористичког акта, а друга је реактивног карактера и односи се на анализе настале након извршења терористичког акта. Када дође до терористичког напада реакција мора да буде брза, али и адекватна, како се не би испустили значајни подаци.

„Ради једноставније и лакше координације и руковођења, старешина тј. руководилац акције даје смернице и групише задатке у неколико целина: оне које ће он лично извршавати, групу за оперативне задатке, за спровођење истраге, за вршење увиђаја и на крају групу задужену за аналитичке послове“ (Жерајев, 1986: 319).

„Пре него што се приступи противтерористичким дејствима, тј. акцији ослобађања талаца, неопходно је прикупити одређене информације: 1) личне податке о терористима, да ли су наоружани и ако јесу, којом врстом оружја, 2) колики је број терориста и који су им циљеви и намере, 3) информације о месту где се врши терористички акт; 4) у каквом су психичком и физичком стању таоци; 5) открити места за лакши и безбеднији прилаз објекту где су терористи, а нарочито небрањени простори, мртви углови и нека осетљива места; 6) који је најједноставнији и најлакши начин да се онеспособе и разоружају терористи и 7) какви су наоружање и опрема са којима располажу специјалне антитерористичке јединице“ (Милојевић, 2009: 298).

У циљу превенције тероризма безбедносне агенције могу сарађивати са образовним, верским и невладиним организацијама како би се смањила радикализација, посебно међу

младима. Такође, ефикасно праћење и анализа екстрема у друштву може се вршити у сарадњи са оваквим организацијама.

„У циљу откривања и идентификовања терористичке групе, идентификације њихових чланова, тајних канала, логистика, начина и извора финансирања, циљева и планова извођења акција, користе се разноврсне методе и средства, а генерално за све полиције света јавља се проблем инфилтрације и контроле затворених људских ентитета, као што су верско-фанатичне и национално-сепаратистичке и терористичке организације. Из тог разога, неопходан услов за квалитетно и успешно супротстављање тероризму укључује и сарадњу и координацију између различитих полицијских и неполицијских служби“ (Симоновић, 2004: 661).

2.5.3.4 Нормативни оквир

„Задатак новог модела безбедносне аналитике је да утврди стандарде у свим секторима безбедности, као и општи стандард безбедносне аналитике, који се може применити (порилагођено) у посебним формама, у зависности од сектора који је у питању“ (Андрић и Тишма, 2022: 36). Овај модел безбедносне аналитике, који се односи на спречавање тероризма, има за циљ да предупреди и предвиди будуће терористичке претње. Да би то могло да се оствари, неопходна је константна размена података између различитих сектора безбедности, како је већ појашњено.

„Велики број суверених држава данас има проблем јер терористичке организације превазилазе државне границе и учестало се суочавају са пријатељском конкуренцијом и љубоморним чувањем обавештајних „извора и метода“, што опет у значајном обиму спутава адекватну размену и проток информација са другим земљама“ (Хармон, 2002: 268).

Да би то заживело у пракси, потребно је формирати и нормативни оквир како би се тај процес стандардизовао. Потребно је донети адекватне прописе, законе и планове и правилнике како на нивоу републике тако и у појединачним секторима безбедности. Пре свега, оно што нам недостаје је закон о безбедности Републике Србије. Ипак, не смемо занемарити да у пракси већ постоје неки нормативни акти на које се можемо ослонити када је борба против тероризма у питању.

На пример, ту су закони о борби против тероризма и екстремизма. Србија је усвојила различите законе и стратегије, укључујући Закон о сузбијању тероризма и Националну стратегију за борбу против тероризма, који омогућавају препознавање терористичких активности и законске оквире за процесуирање починилаца. Такође, у сарадњи са међународним организацијама, Србија користи средства за праћење финансијских токова повезаних са тероризмом (нпр. финансирање терористичких организација), као и имплементацију закона о прању новца, који може да буде од кључне важности у спречавању финансирања тероризма.

Треба напоменути и да је важно балансирати безбедност са заштитом људских права, посебно када је реч о приватности и слободи изражавања. Прикупљање података везаних за тероризам мора бити у складу са домаћим законодавством и међународним нормама.

2.5.3.5 Складиштење података

„Током 1999. године, најзначајнију активност у борби против тероризма представљало је укључивање Европола у тај процес, под ограниченим и контролисаним условима. Првих пет главних задатака одељења Европола за сузбијање тероризма (познати као *SeriousCrime 5 – SC5*) подразумевало је: прикупљање информација и почетних сазнања за формирање досијеа битних за аналитички рад у сузбијању тероризма *(Analytical Work Files – AWFs*), стављање акцента на размену информација између држава чланица и релевантних државних органа у борби против тероризма, преузимање одговорности од националне администрације држава и њен трансфер на администрацију Директоријума Европске уније за оспособљавање и за борбу против тероризма; стварање погодних услова за формирање законског оквира оснивањем центара за борбу против тероризма и усаглашавење одговарајућих законских решења и формирање ‚црних листа' (глосаријума) терористичких група. Даље, поред ових, усаглашени су ставови поводом осталих кључних задатака Европола у том контексу, где су најзначајнији: анализа безбедносних стања и трендова, усвајање директива о одговору на тероризам на националном плану и израда листа доступних извора информација“ (Матић и Милошевић, 2006: 32).

Глобалне базе безбедносних информација чине камен темељац у борби против међународног тероризма. Интерпол је познат по таквим базама, захваљујући којима повезује полицију у 190 земаља чланица. То су једине базе података које постоје на тако широком и међународном нивоу.

„Интерполова сигурна комуникациона мрежа користи се и за замрзавање терористичких средстава, издавањем забрана путовања и спречавањем трговине оружјем. Од 6. новембра 2009. године, 46 држава чланица, укључујући и УН, имплементирало је *MIND/FIND* интернет везу која нуди државама чланицама бржи приступ Интерполовој бази података. Ово се може применити на граничним прелазима и другим местима како би се ухватио осумњичени терориста“ (Noble, 2008: 62).

Као што је већ поменуто, и савремене технологије се могу користити у прикупљању података о терористичким претњама. Тероризам је претња безбедности код које употреба ОСИНТ података може бити изузетно значајна. Поред тога, савремене технологије и методе машинкског учења, као и вештачка интелигенција могу да се примене у анализи података.

> „Стручњаци за сајбер безбедност указују на потребу за отварањем извора података због једноставног разлога што модели машинског учења могу помоћи у бољем разумевању сајбер претњи, а такође подржати обавештајни рад. Познавање науке о подацима и машинског учења може повећати капацитете стручњака за сајбер и информатичку безбедност, пружајући им могућност за увођење система за рана упозоравања, прикупљање информација о сајбер претњама, обучавање машина за препознавање већине злонамерног софтвера и напада социјалног инжењеринга или чак за развој кода“ (Тишма и Андрић, 2021: 288).

Поред тога, треба напоменути да се у савременим условима подаци које чувају и размењују безбедносне службе и други елементи могу чувати у посебним условима, То јест, могу се похрањивати у посебним базама података које су посебно креиране да олакшају и унапреде рад безбедносних аналитичара. Такве базе користе посебна софтверска решења која могу олакшати претрагу података, њихову корелацију и анализу.

2.5.3.6 Профил аналитичара и обучавање

Припадници безбедносних служби и специјалних јединица који се ангажују у борби против тероризама континуирано пролазе кроз различите врсте вежби и обука како би одржали неопходан ниво способности. Међутим, када је у питању безбедносна аналитика и рад аналитичара, не постоји довољно података о потребним квалификацијама, образовању и способностима за обављање овог посла.

> „Послови и задаци обавештајно-сигурносних служби захтевају разне врсте и нивое способности од професионалних, полупрофесионалних и алтернативних сарадника у процесу рада. Број знања и вештина који се захтевају тако је велики да се поставља питање да ли је могуће ваљано дефинисати општи профил обавештајца који би све захтеве задовољио“ (Алиспахић**,** 2011: 177).

За бављење послом безбедносног аналитичара потребно је одлично познавање свих сектора безбедности, њиховог нормативног уређења, процедура и стандарда. С друге стране, потребне су и одређене вештине и искуство у овој области. То нас доводи до чињенице да теоријски модел безбедносне аналитике треба да утврди и неопходне личне особине и квалификације за бављење овим послом.

> ,,Ако пажљиво проучимо задатаке које обављају обавештајно-сигурносне службе, видећемо да у њиховој структури у одређеним компонентама деловања преовлађују *знања,* дакле интелектуална компонента, у другим умећа (рутинска примена знања по прихваћеним моделима), у трећим вештина стечена увежбавањем примене знања; у четвртим примена физичке снаге и брзине; у петим примена нужних функционалних комбинација знања, умећа, вештина, физичке снаге и брзине“ (Алиспахић, 211: 178).

Мора се имати на уму и то да посао безбедносног аналитичара није идентичан послу који обављају обавештајци, те се и потребне квалификације разликују. Група аутора из Безбедносног истраживачког института из Аустралије (Security Research Institute Edith Cowan University, Perth, Australia) направила је табелу вештина и атрибута безбедносних аналитичара анализирајући постојећу литературу коју је значајно приказати. Треба напоменути и то да се овакав кадар не може добити комплетно формиран и оспособљен ни из једне институције, већ се такав кадар мора стварати како наводи Алиспахић кроз:

1) ,,избор и проверу избора,
2) инструисањем, саопштавањем одговарајућег сазнања,
3) увежбавање и

4) примену у пракси извршавања задатака“ (Алиспахић, 2011: 177).

Дакле, сви који раде на обавештајним задацима морају проћи додатни вид обуке и тренинга како би унапредили своје способности. Такве обуке су базиране на припреми за одређену групу обавештајних задатака и усмерене су на унапређење знања и вештина стечених у цивилном, војном и полицијском образовању.

Република Србија може да организује обуке и вежбе за своје безбедносне снаге кроз симулације терористичких напада како би се тестирала ефикасност у реалним условима. Овакве обуке се могу проширити и на аналитичаре, обавештајце и оперативце како би лакше преознали терористичке претње и адекватније реаговали на њих.

> „Програм почетног основног образовања посебно примереног потребама обавештајне службе треба да похађају извршиоци – оперативци-почетници. Међутим, он није прилагођен потребама аналитичара и шифраната, као и неким члановима логистике. За потребе аналитичара неопходно је оформити прогам који ће их научити логичким компонентама деветовалентне односно мултивалентне логике (почевши од појма и термина до закључивања), као разним облицима примене методе ‚анализе садржаја докумената’ (квалитативне и квантитативне), формирању регистара и досијеа и томе слично“ (Алиспахић, 2011: 185).

Анализирајући горенаведену табелу видећемо да се неке квалификације и жељене особине безбедносних аналитичара понављају, а поједине битно разликују у зависности од аутора. Међутим, без обзира на то ком аутору били наклоњенији, јасно је да се у ове кадрове мора улагати у смисли њиховог перманентног усавршавања. Овде треба поменути и то да ће такво усавршавање бити неминовност, с обзиром на напредак технологије, брзину размене података и развој електронских медија. Такође, ако узмемо у обзир и да је теоризам променљив феномен у смислу метода и начина деловаља, избора мете и слично ово постаје још логичније.

> „Развој роботике и биологије још увек не представља питање потребе за људима, али отвара питања потребног броја и профила професионалног састава обавештајно-сигурносних служби. Хоће ли одређене особине и сопособности оперативаца за извршење теренских задатака бити непотребне? Хоће ли бити немогуће извршити тајни претрес стана који је, као и цела зграда, у систему електронског надзора? На ова питања за сада не можемо прецизно одговорити, али је извесно да ће обавештајно-сигурносне службе морати више инсистирати на интелектуалним способностима и образовању својих професионалаца

и на одређеним специјалностима, као и на проширивању техничких знања“ (Алиспахић, 2011: 190).

2.5.4 Базе података – конкретни примери

Може се закључити да практична примена теоријског модела безбедносне аналитике у борби против тероризма у Србији захтева координацију између различитих безбедносних и правосудних институција, коришћење напредних технологија за анализу података, али и строго поштовање законских норми и људских права. Такође, неопходно је извршити процес стандардизације области безбедносне аналитике и уз то утврдити неопходне квалификације безбедносних аналитичара. *Српске агенције би се ослониле на методологије попут анализе образаца, предиктивне аналитике и мрежне анализе како би се ефикасно бориле против тероризма, уз стално унапређивање обука и процедура.*

Теоријски модел безбедносне аналитике у супротстављању тероризму је свеобухватан, динамичан и флексибилан, како би могао да се прилагоди стално променљивом терористичком окружењу. Кроз интеграцију различитих аналитичких метода, теорија и технолошких алата, као и континуирано учење из претходних искустава, овај модел омогућава безбедносним институцијама да унапреде своје капацитете за превенцију, детекцију и одговор на терористичке претње. Овај оквир може послужити као темељ за даљи развој и имплементацију специфичних методологија у борби против тероризма.

Модел безбедносне аналитике који је приказан на примеру супротстављања тероризму смо проверили и кроз истраживање са експертима из области безбедносне аналитике, криминалистике, обавештајног рада, стратегије и других релевантних области. Резултати истраживања су приказани у следећем поглављу.

У процесу прикупљања података посебно се обраћа пажња на изворе из којих се подаци прикупљају. Изворе података посебно треба преиспитати када је у питању борба против савременог тероризма, где имамо значајан уплив савремене технологије. Неопходно је користити савремене софтверске алате како би се дошло до значајних безбедносних података како би се исти и проверили. У том процесу значајне могу бити отворене и научне базе података, као и оне које креирају и користе међународне безбедносне организације попут Интерпола.

Базе података могу бити двојако значајне за безбедносну аналитику. Прво, као извор података, а други значај могу имати за складиштење података у савременом контексту. Те базе података и њихов значај треба размотрити из више углова.

2.5.4.1 Научне базе података и отворени подаци као извор података безбедносне аналитике

Експанзија интернета донела је и нове изворе података који могу бити значајни за рад полиције и служби безбедности. Данас се само преко „Гугл“ претраживача може приступити различитим друштвеним мрежама, форумима, пропагандним сајтовима и слично. Тако се у дигиталном облику могу пронаћи многи безбедносно интересантни подаци.

Ово се посебно односи на борбу против тероризма. Данас свака већа и организованија терористичка организација има свој сајт или интернет портал путем кога пласира своје екстремистичке идеје. Такође, комуникација између терориста се често одвија путем интернета, па пресретање такве комуникације често може спасти много људских живота. Међутим, у контексту ове дисертације желимо да скренемо пажњу на нешто што може да буде онлајн извор података, а што заправо има научно утемељење. То су научне базе података које су креирали иностранu универзитети и институти и значајне међународне организације.

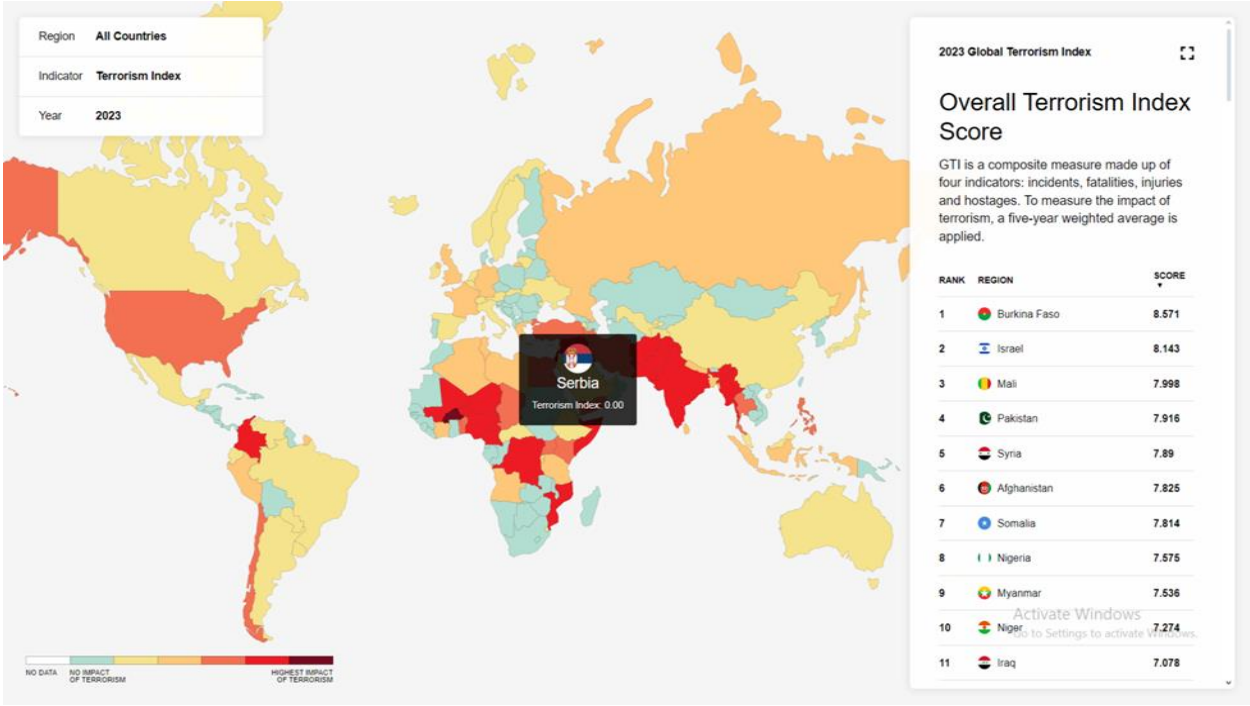
Овакве базе података прикупљају податке о прошлим догађајима везаним за тероризам и организовани криминал и сортирају их по годинама и регионима у којима су се десили. У контексту стратешке безбедносне аналитике могу бити изузетно корисни у смислу предиктивне аналитике. На основу података о прошлим догађајима у појединим регионима можемо доћи и до предикција будућих догађаја. Оно што је посебно значајно јесте да овакве базе имају начно утемељење и да садрже проверене податке.

„Често тежимо да утврдимо просторни распоред терористичких напада, њихове последице, смртност, порекло и финансирање терористичких организација, да ли су реакције на те нападе биле адекватне и, што је најважније, да предвидимо где, када и како би могао да се догоди следећи напад. Предиктивна функција оваквих анализа је разлог што се оне често изводе под претпоставком хитности, штуро и непотпуно. За овакву анализу потребан је значајан број проверених података до којих није лако доћи и зато

треба сачекати да се такви подаци прикупе. У ту сврху постоји више база података које бележе податке везане за терористичке нападе“(Андрић и Ковач**,** 2021: 111).

Глобални индекс тероризма

Институт за економију и мир из Њујорка (ИЕП) је креирао Глобални индекс тероризма (ГТИ) и учино га јавно доступним свима. ГТИ је свеобухватна студија која анализира утицај тероризма на 163 државе, односно на 99,7% светске популације. ГТИ производи композитни резултат како би се обезбедио редован ранг земаља о утицају тероризма. ГТИ оцењује сваку земљу на скали од 0 до 10, где 0 представља никакав утицај тероризма, а 10 представља највећи мерљиви утицај тероризма (https://www.visionofhumanity.org/maps/global-terrorism-index/#/).

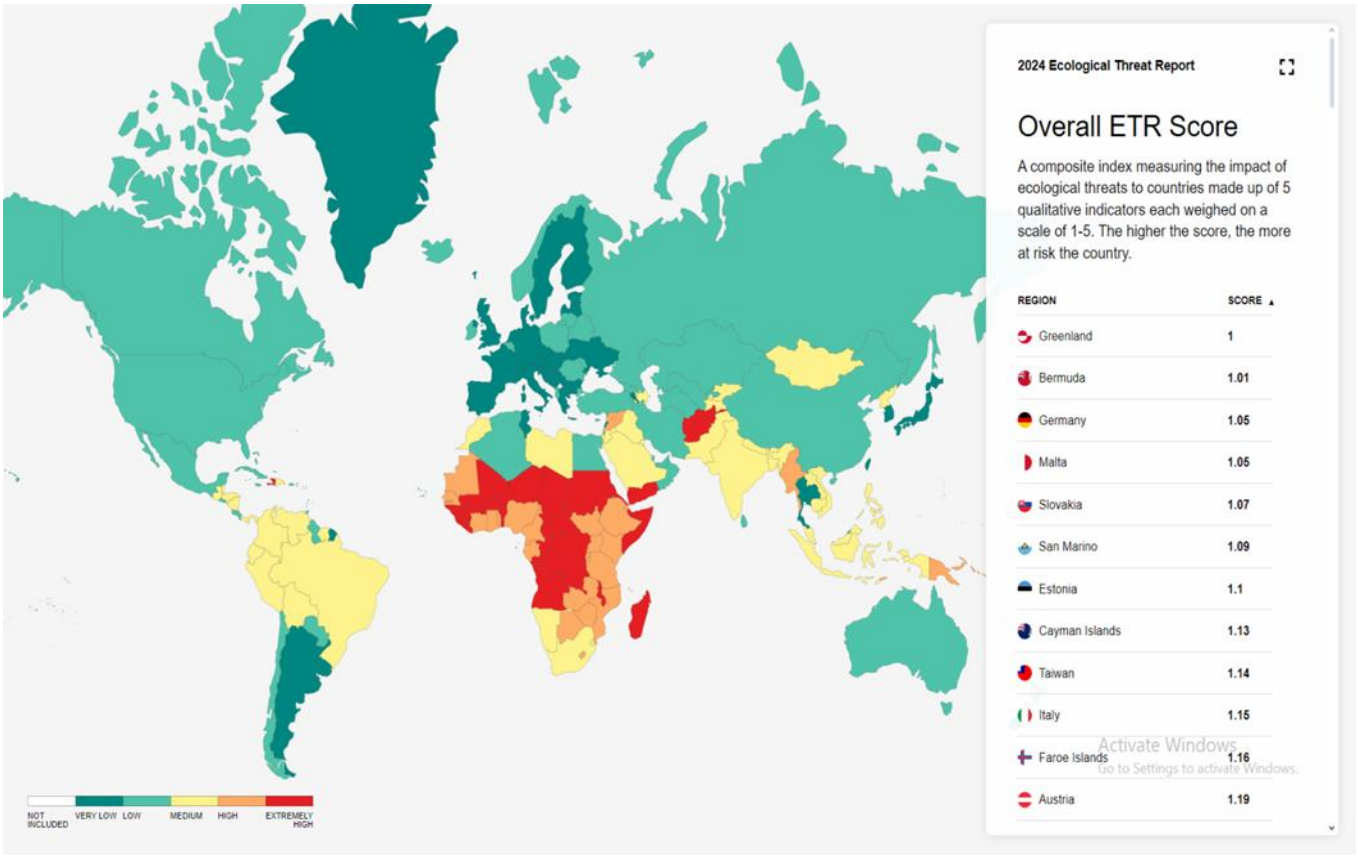


Слика 27. *Приказ глобалног индекса тероризма за 2023. годину*

Извор: *https://www.visionofhumanity.org/maps/global-terrorism-index/#/ доступан 29. 1. 2025.*

На основу доступних и научно заснованих података врши се процена утицаја претње тероризмом на 163 државе. Утицај се односи на политичку стабилност, економију и друге

значајне факторе. За живописнији приказ дате су и мапе приказане на слици изнад, а са десне стране налази се листа држава сложена по индексу од најугроженијих ка мање угроженим. На слици су приказани подаци за 2023. годину, где је Србији додељен индекс 0.00. Поред података везаних за тероризам, овде се могу наћи и процене утицаја на животну средину и подаци везани за ту област безбедности.



Слика 28. *Приказ еколошке угрожености на планети за 2024. годину*

Извор: *https://www.visionofhumanity.org/maps/global-terrorism-index/#/ доступан 29. 1. 2025.*

Истраживање користи вишеструки приступ анализирајући еколошке претње на националном, субнационалном и градском нивоу, док истовремено процењује претње по друштвену отпорност и нивое мира. Да би помогао међународној заједници у приоритизацији свог фокуса, ИЕП је идентификовао земље, административне области и градове који имају најтеже претње и најниже капацитете за савладавање. То су земље које

ће највише патити од повећаних нивоа конфликата у вези са еколошким претњама. Извештај о еколошким претњама такође гледа у будућност, са прогнозама до 2050. године (https://www.visionofhumanity.org/maps/global-terrorism-index/#). Такође, поред наведеног постоји и свеукупни индекс мира који је такође праћен извештајем и мапом.

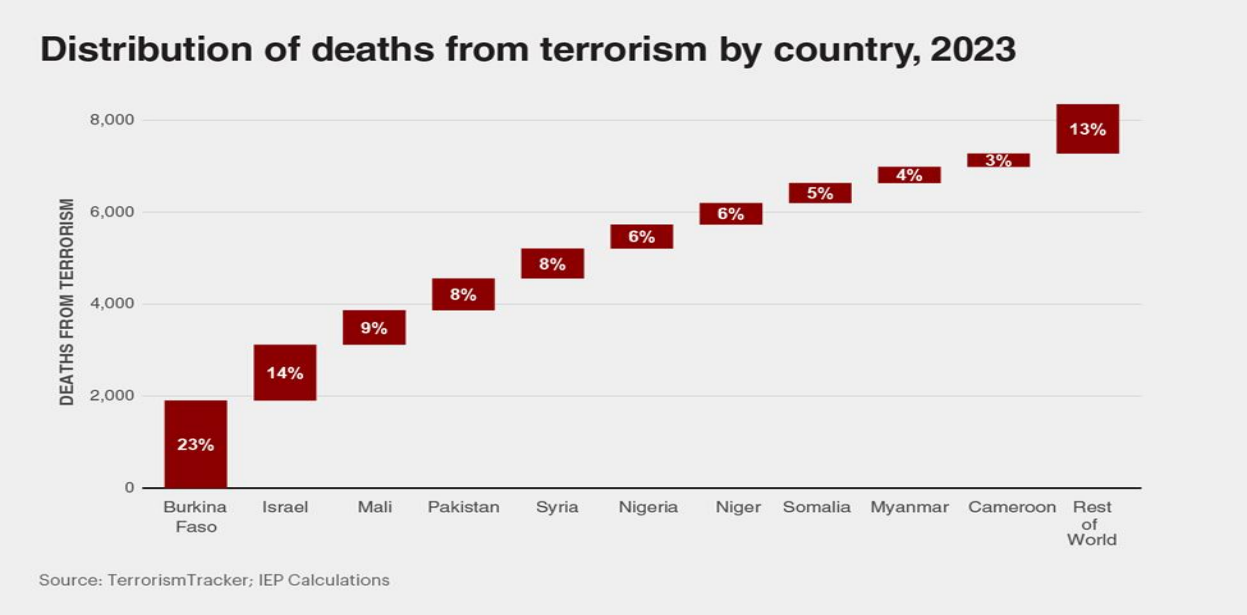
Институт за економију и мир (ИЕП) произвео је Глобални индекс мира (ГПИ) је водећи светски показатељ глобалне мирноће. Овај извештај представља најобухватнију анализу на основу података о трендовима у миру, његовој економској вредности и томе како развијати мирољубива друштва. Глобални индекс мира покрива 99,7% светске популације, а израчунава се користећи 23 квалитативна и квантитативна индикатора из високопоштованих извора и мери стање мира у три области:

- ниво друштвене безбедности и сигурности,
- опсег текућег домаћег и међународног конфликта и
- степен милитаризације (https://www.visionofhumanity.org/maps/#/).

Ову базу података могу да користе студенти, новинари и сви остали заинтересовани. Службе безебедности и аналитичари који се баве, на пример, питањем борбе против тероризма, могу добити значајне податке и користити овај сајт као алат који је доступан у пар кликова.

Након обраде података, извештаји се раде за сваку претходну годину. У периоду писања ове дисертације издати су неки кључни подаци за трендове тероризма у 2023. години, које ћемо приказати ради иулустрације. Између осталог, наводи се да:

- Смртни случајеви узроковани тероризмом повећали су се за 22%, на 8.352 особе, што је највиши ниво од 2017. године.
- Епицентар тероризма се преместио са Блиског истока у регион Централног Сахела у субсахарској Африци, који сада чини више од половине свих смртних случајева од тероризма.
- Утицај тероризма постаје све више концентрисан, са десет земаља које чине 87% свих смртних случајева узрокованих тероризмом.
- Конфликт остаје главни покретач тероризма.



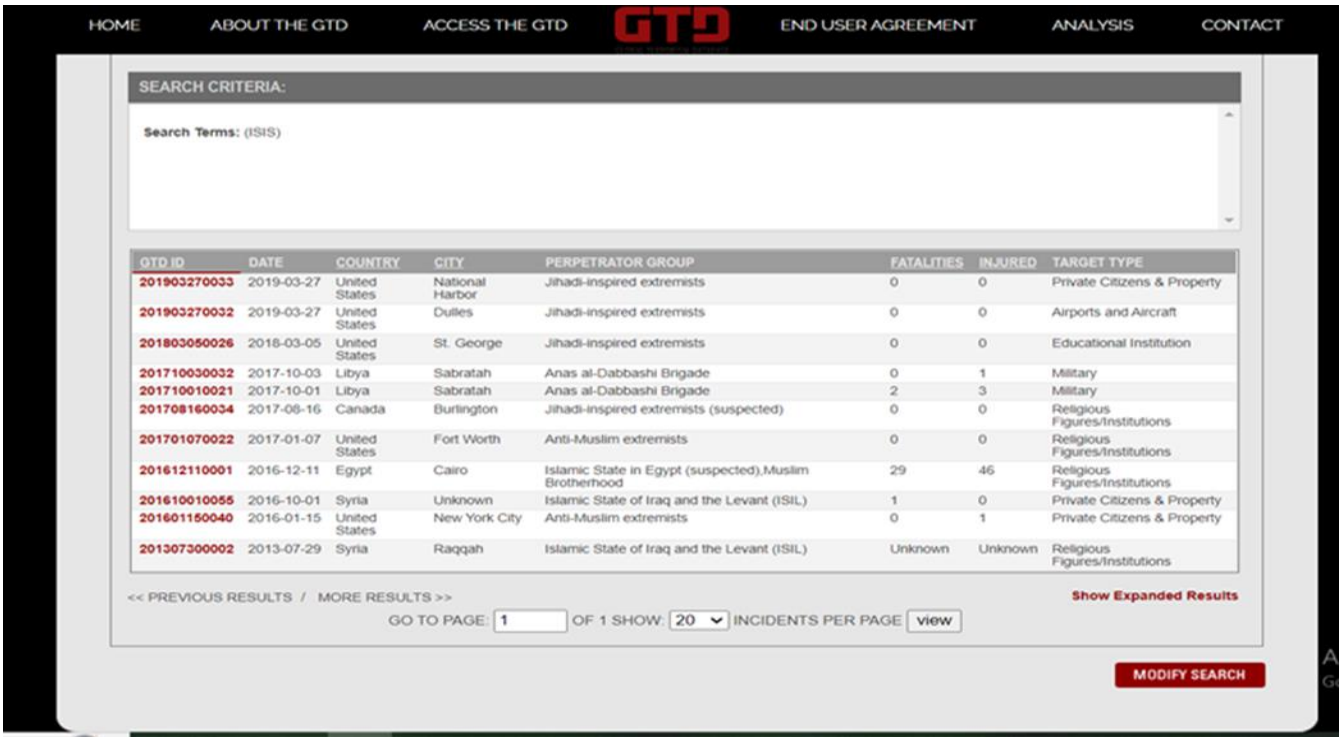
Слика 29. *Распоред смртних исхода по земљама за 2023. годину*

Извор: *https://www.visionofhumanity.org/7-key-findings-from-the-global-terrorism-index-2024/*

База глобалног тероризма (ГТД)

„Не смемо прескочити *Базу глобалног тероризма*. Академска база која припада Универзитету у Мериленду, у Колеџ Парку, специфична је по томе што, између осталог, садржи и податке о томе како и зашто се формирају терористичке групе и обухвата период од 1970. до 2018. године“ (Андрић и Ковач, 2021: 116). Ова база се такође односи на податке везане за терористичке нападе и у тој области представља једну од најкомплетнијих, с обзиром на то да садржи податке везане за датуме, локације, врсте напада и број жртава терористичких напада широм света. Користећи ову базу као ресурс за анализу образаца тероризма могу се направити процене утицаја терористичких догађаја на различите регије (https://www.visionofhumanity.org/maps/#/).

Ова база омогућава да се у задатим временским и географским оквирима претраже подаци везани за теоризам, при чему критеријуми претраге могу бити различити. Тако се терористички акти могу претраживати по врсти оружја које је коришћено у нападима, методама или броју жртава. На пример, могу се претражити самоубилачки напади који су се догодили у Европи у периоду од 2000. до 2018. године.



Слика 30. *Пример претраге базе података о тероризму*

Извор: *https://www.start.umd.edu/gtd/*

Базе података националног центра за борбу против тероризма (НЦТЦ)

Након терористичких напада 11. септембра 2001. године, председник Џорџ В. Буш, издавањем Извршне наредбе 13354 и Конгрес Сједињених Америчких Држава (САД), доношењем Закона о реформама обавештајних служби и превенцији тероризма (IRTPA) из 2004. године, реформисали су обавештајни систем нације, са посебним фокусом на обавештајне податке везане за тероризам. Ови основни документи дефинишу главне улоге, мисије и одговорности НЦТЦ-а (https://www.dni.gov/index.php/nctc-who-we-are).

Национални центар за борбу против тероризма у САД је основан са намером да се обавештајни подаци о тероризму централизују, анализирају и буду дистрибуирани међу релевантним владиним агенцијама. То укључује и идентификацију потенцијалних претњи, праћење терористичких активности, као и развој стратегија за превенцију терористичких напада. У те сврхе користи се више база података:

Terrorist Identities Datamart Environment (TIDE) – Ово је централна база података која се односи на податке везане за идентитет лица за која се сумња да су повезана са тероризмом (имена, презимена, биографски подаци).

- NCTC Online – То је интранет портал који омогућава приступ различитим обавештајним подацима и извештајима о тероризму. Овај портал је доступан особљу NCTC-а и партнерским агенцијама, омогућавајући им да брзо приступе најновијим информацијама и анализама. Worldwide Incidents Tracking System (WITS) – Ова база података бележи информације о свим значајним терористичким инцидентима широм света. WITS омогућава аналитичарима да прате трендове у терористичким активностима, идентификују географске тачке са високим ризиком и проучавају методе које користе терористи (https://www.dni.gov/index.php/nctc-who-we-are).

Поред примера база које смо навели треба поменути и друге јавно доступне базе које се питањем тероризма баве индиректно:

- JCTOP је једна од најпознатијих база података у академским круговима, нарочито у области друштвених и хуманистичких наука. Специфично, JCTOP садржи богату колекцију радова везаних за политичке науке, социологију и студије безбедности, укључујући и студије о тероризму (https://www.jstor.org/).
- Proquest Central је мултидисциплинарна база података која обухвата широк спектар области, укључујући и студије тероризма (https://about.proquest.com/en/products-services/ProQuest_Central/).
- SAGE Journals је још једна кључна база података која нуди приступ високорангираним академским часописима у областима друштвених наука и безбедности (https://journals.sagepub.com/).
- Homeland Security Digital Library је специјализована база података која пружа приступ документима и извештајима који се баве националном безбедношћу, укључујући и тероризам. Ова база је посебно корисна за истраживаче који се баве практичним аспектима борбе против тероризма и политикама везаним за националну безбедност (https://www.hsdl.org/c/).

Безбедносна питања попут тероризма захтевају да се посматрају из шире перспективе. Тако не можемо разматрати терористичке претње у Србији уколико не посматрамо шта се дешава у региону и свету. Дакле, да бисмо могли да се супротставимо тероризму, морамо анализирати трендове којима тежи и како се они могу рефлектовати на нашу државу. Наведене базе података могу бити изузетно корисне јер аналитичару могу да скрате време претраге и да укажу можда на неке нове перспективе. Стога треба размотрити, по угледу на Базе података националног центра за борбу против тероризма у САД, креирање сличних база података у Србији. Такве базе се могу креирати за различите врсте претњи безбедности, које су од стратешког значаја, а свакако захтевају умрежавање свих релевантних институција и креирање координационог тела како би се размена информација и употреба оваквих база података одвијала несметано. Наравно, поред

наведених примера база података као извора информисања, треба напоменути и базе које различите службе имају у склопу свог посла, али и оне међународне.

2.5.4.2 Базе података у оквиру служби безбедности

Како је већ наведено, у оквиру различитих служби безбедности информације се чувају као ресурс за будуће анализе. Како би информације и подаци до којих су дошли оперативци и аналитичари биле доступне и за касније аналитичке процесе, оне се похрањују у базама података. Уношење података у базу се може сматрати и једним од корака у процесу безбедносне аналитике.

Раније су подаци архивирани у аналогном облику и чувани су у другачијим формама него данас. Развој технологије је допринео томе да се подаци и информације чувају у дигиталним базама података. Софтвери који се данас користе омогућавају службама да се подацима лакше приступа и знатно је олакшана и сама обрада података.

Аналитички сектори имају сопствене базе и архиве података које љубоморно чувају и ретко деле са другима. Међутим, када су у питању сложене претње безбедности, на чијем спречавању и сузбијању је неопходно укључивање више институција, онда се мора вршити размена података и неке базе или њихови делови учинити доступним и другима, што је често проблем у пракси. С друге стране, добри примери размене података су Интерполове базе које су доступне полицијама многих земаља.

> „Интерпол је и специјализована организација која сарађује у борби против криминалитета, са најозбиљнијим институционалним оквиром и дугом традицијом у остваривању мултилатералне сарадње између полицијских органа из целог света. А криминалитет, предмет сарадње у оквиру МОКП, постао је глобални проблем број један. Разне међународне организације (нпр. ОУН, НАТО, ОЕБС и др.) су, у својим програмима након 11. септембра, као један од најважнијих циљева уврстиле и борбу против транснационалних и нетрадиционалних изазова – ‚претњи' , међународног тероризма и организованог криминалитета (трговина дрогом, пролиферација нуклеарног, хемијског и биолошког оружја и трговина људима). Ти глобални изазови – претње безбедности, делују на међународну заједницу као јаке интегративне силе, захтевајући јаче повезивање и сарадњу, јер чињеница је да ниједна држава, ма колико моћна била, не може самостално да се ‚ухвати укоштац' са тим проблемом. Кристално је јасно да борбу против ‚глобалног криминалитета',може добити једино ‚глобална сарадња'“ (Николић, 2007: 20).

Иако је после напада на САД из 2001. године примарни фокус Интерпола био на борби портив тероризма у савременом контексту, то ипак није више тако, те су се и Интерполове базе проширили и на друге области. „Улога тероризма је релативно избледела у међународној полицијској организацији. Управо упркос широко признатом глобалном карактеру проблема тероризма, улога Интерпола у питањима борбе против тероризма тренутно је бледа у поређењу са стратегијама борбе против тероризма које су осмислиле појединачне полицијске агенције унутар нација“ (Deflem, 2024: 3).

Тако данас Интерпол има 19 база података у којима се складиште различите врсте података: подаци о криминалцима и почињеном криминалу, подаци о путним документима, затим подаци о сексуалном злостављању деце, украденим уметничким делима и тако даље.

> „Националне полиције могу прегледати наше базе података у реалном времену као део њихових истрага. То може бити учињено преко њиховог НЦБ-а (Национални центар за Интерпол) или директно на фронту, на пример, од стране специјализованих јединица за борбу против криминала и граничних званичника.
> Базама података се приступа преко I-24/7, нашег сигурног глобалног система за комуникацију полиције. Ово је техничка мрежа која повезује органе за спровођење закона у свим земљама чланицама и омогућава овлашћеним корисницима да деле осетљиве и хитне полицијске информације са својим колегама широм света.“ Ово је наведено на сајту Интерпола (https://www.interpol.int/en/How-we-work/Databases).

Несумњиво је да и наше службе безбедности, војска и полиција имају сопствене базе података, али с обзиром на тајност података о њима се у литератури не говори пуно. Свакако, Република Србија на свом путу ка ЕУ и као чланица међународних организација тежи да испрати и технолошке и друге стандарде у очувању података.

У прилог томе навешћемо и једно истраживање. Рацић и Достић, у свом испитивању које су спровели у оквиру организационих јединица надлежних за обављање криминалистичко-обавештајног рада, дошли су, између осталог, и до следећих резултата:

> „Одговори руководилаца у организационим јединицама у седишту Дирекције полиције и подручним полицијским управама на питање: *Оцените квалитет база података у којима се евидентирају оперативне везе.*Анализом одговора запослених на наведено питање, од укупног броја запослених у посматраном узорку у ‚Студији 2019’, 60,5% запослених је оценило базе података са ‚углавном корисне/ и ‚у потпуности корисне’, а 27,5% као неквалитетне са оценама ‚углавном неквалитетне’ и ‚у потпуности неквалитетне’, а 12% изјаснило да ‘нема мишљење’. У посматраном узорку након протока времена у ‚Студији

2022', 6,06% је дало позитивну оцену, а 93,94% је оценило базе података као неквалитетне. У посматраним узорцима постоји статистички значајна разлика између учесталости позитивних и негативних оцена ($\chi 2$ emp = 41,647, df = 1, $p < 0,01$). Може се закључити да је потребно спроводити даље активности на унапређењу квалитета база података у којима се евидентирају оперативне везе у криминалистичко-обавештајном раду у полицији Републике Србије"(Рацић и Достић, 2024: 109).

Дакле, у контексту теоријског модела безбедносне аналитике базе података се могу посматрати кроз два иновативна приступа. Један је да ОСИНТ податке и јавно доступне базе треба уврстити у изворе безбедносне аналитике, док је други да се на основу изложеног у овој дисертацији може закључити да је неопходно формирање и једне централизоване базе података када су у питању претње безбедности на стратешком нивоу. Ова база би требало да буде форматирана тако да омогућава и размену података између различитих релевантних елемената система безбедности покривајући све секторе безбедности.

ТРЕЋИ ДЕО: РЕЗУЛТАТИ ИСТРАЖИВАЊА

Свако научно истраживање има свој теоријски и емпиријски део. У том смислу, у оквиру теоријског истраживања, примарно приказаног у прва два дела дисертације, изведени су основни закључци на основу увида у научну литературу, бројне практикуме и службена документа националног и међународног карактера. Теоријски закључци до којих се дошло на основу анализе доступне литературе и других релевантних извора наводе се у даљем тексту.

Осим теоријског, спроведено је и емпиријско истраживање. С обзиром на природу теме ове дисертације (предмет истраживања), итраживање је спроведено међу експертима из области безбедности, безбедносне аналитике, а нарочито са појединцима који су аналитичке послове обављали у пракси. Емпиријско истраживање је имало два дела 1) *Усмерени интервју*, са 46 испитаника (Упитник за усмерени интервју који су испитаници попуњавали налази се у **Прилогу 1**) и 2) *Усмени интервју -– разговор* са петочланом експертском групом (Компетенције експертске групе приказане су у **Прилогу 2**).

Напослетку, креирани теоријски модел безбедносне аналитике проверен је на примеру супротстављања тероризму (**Прилог 3**).

1. РЕЗУЛТАТИ ТЕОРИЈСКОГ ДЕЛА ИСТРАЖИВАЊА – ЗАКЉУЧЦИ О ТЕОРИЈСКОЈ И ПРАКТИЧНОЈ ИЗГРАЂЕНОСТИ БЕЗБЕДНОСНЕ АНАЛИТИКЕ

Анализом постојећег стања теоријске дефинисаности и функционисања безбедносне аналитике у пракси долази се до сазнања која су, као премисе, искоришћена у креирању њеног теоријског модела. Значајне премисе за креирање теоријског модела безбедносне аналитике, а као резултат спроведене анализе, могу се груписати у теоријске и практичне.

1.1 Теоријски аспект закључака из анализе стања безбедносне аналитике

Као кључни закључци истраживања теоријског карактера могу се сматрати:

- Појам (термин) *аналитика* је скромно разрађен у теорији, те се често и превише везује за појам (термин) *анализа*, а неретко се ти појмови (термини) поимају и као синоними.

- Додатну теоријску замршеност у односу појмова *аналитика* и *анализа* доноси и поимање *анализе* као научне методе, док се *аналитика* третира као поступак (процес) који користи и научне и ненаучне методе (поступке). Отуда, аналитика се и поима више као практична делатност аналитичара, која треба да буде и научно заснована (да користи и научне методе).
- У складу с наведеним, прихватљива дефиниција аналитике гласи: *Аналитика је делатност стицања (и употребе) релативно истинитог, у одређене сврхе употребљивог сазнања систематски и континуирано, применом проверених, плодотворних, првенствено научних метода.*
- Појам (синтагма) *безбедносна аналитика* (Security Analytics) појављује се само у малом броју теоријских радова и наставној литератури, при чему преовладава њено оквирно одређење као „специјална врсте аналитике“ у оквиру сектора безбедности, којом се баве државни органи, војска, полиција и службе безбедности, а мање се срећу експлицитне дефиниције тог појма (синтагме).
- Значајан проблем у дефинисању безбедносне аналитике јесте превод енглеске речи *Intelligence*, који има три основна гледишта: 1) Intelligence дословно преведено као *обавештајно*, 2) Intelligence као *(са)знање* и 3) сублимат претодна два превода, односно поимање intelligence као *обавештајна информација,* која има комплекснији значај од „сирових“ информација које користи у доласку до обавештајне информације (сазнања).
- Користећи на наведени начин превод речи intelligence, безбедносна аналитика остаје на нивоу форме обавештавање, а мање се осврће на суштину, односно на знање о системском поимању безбедности: субјект угрожавања – субјект безбедности – референтни објект безбедности.
- Такође, фокусирајући се на форму обавештавање, теорија безбедносне аналитике је саму аналитику, која се најчешће именује као анализа, као фазу (корак), сместила у шири процес, који је и именован као *обавештајни циклус*.
- Безбедност, као појам, поготово у државоцентричним међународним односима, предуго се задржала на рату (војни сектор безбедности) као кључној претњи безбедности, већим делом занемарујући остале секторе, као што су: политички, економски, социјетални и еколошки, које је утврдила научна теорија у тзв. проширењу

појма безбедност. Научна теорија о секторима безбедности широко је прихваћена у свету.

- Војно-стручна теорија је била извор успостављања теорије аналитике у полицији, која је, по инерцији, задржала назив „обавештајна“, са додавањем префикса „криминалистичка“ (криминалистичко-обавештајна) за саму аналитику (анализу), а и у склопу ширег процеса задржан је назив обавештајни циклус (криминалистичко-обавештајни циклус).
- С временом, теорија аналитике у полицији заокружена је у оквиру ширег теоријског модела рада и организовања полиције, именованог као Intelligence-ed Policing – ILP, који се најчешће преводи као обавештајно вођен полицијски рад или полицијски рад заснован на обавештајним сазнањима.
- У Републици Србији Законом је уређено увођење Полицијског обавештајног модела – ПОМ, заснованог на ILP.
- На основу теоријског дела истраживања, утврђена је дефиниција безбедносне аналитике: *Безбедносна аналитика је посебна врста аналитике, која се испољава као интелектуална, организована, систематска, циљна и сврсисходна делатност усмерена ка стицању релативно истинитих и употребљивих сазнања о субјекту угрожавања, неопходним за рад субјекта безбедности у заштити референтног објекта безбедности.*

1.2 Практични аспект закључака из анализе стања безбедносне аналитике

Као кључни закључци који извиру из анализе праксе безбедносне аналитике могу се сматрати:

- У Републици Србији није експлицитно утврђена и уређена функција безбедности. Наиме, Устав Републике Србије користи израз „одбрана и безбедност“. У каснијем, Законом о одбрани је одбрана експлцитно дефинисана као функција државе. Међутим, безбедност није препозната експлицитно као функција државе. Тако, тек 2019. године, не у закону, већ у Стратегији националне безбедности, први пут се дефинише појам „национална безбедност“.
- Безбедносна аналитика која системски захвата националну или колективну безбедност не функционише у пракси, односно најчешће се појављује у два

примарна облика (врсте) 1) војна (спољна) безбедност, именује се као *обавештајна аналитика* и 2) унутрашње-спољна безбедност, пре свега у борби против криминала, када се именује као *криминалистичка* (криминаласитчко-обавештајна) *аналитика,* али са чешћом употребом речи *анализа* од аналитика.

- Обавештајна аналитика (условно војна) остала је у домену једног сегмента безбедности (аналитике) – информације о противнику (непријатељ), при чему противник подразумева и државу и њену војску.
- Криминалистичка анализа (аналитика) акцептира се у информацијама о облицима и носиоцима криминала.
- И обавештајна и криминалистичка (криминалистичко-обавештајна) аналитика (анализа) део су ширег процеса, који с именује као обавештајни циклус или криминалистичко-обавештајни послови, који у пракси, суштински, имају слично утврђене фазе (кораке).
- Криминалистичко-обавештајни послови (крим-обавештајни циклус) у новије време интегрисани су у комплетан рад и организовање полиције на националном и међународном нивоу, именовани као Intelligence-led policing – ILP, који се најчешће преводи као обавештајно вођен полицијски рад или полицијски рад заснован на обавештајним сазнањима. Интегрисани нивои на националном нивоу именују се као национални обавештајни модел (National Intelligence Model) као, на пример, у Великој Британији, САД и другим државама. Типичан пример интернационалног криминалистичко-обавештајног модела (ECIM – European Criminalistic Intelligence Model)) користи се у Европској унији.
- У Републици Србији је Intelligence-led policing – ILP преведен и уведен у праксу као Полицијско-обавештани модел – ПОМ.
- Након драстичних облика угрожавања безбедности у САД (терористички напад Ал-Каиде, 2001) и ЕУ (вирус корона и напад Русије на Украјину), приступа се развоју и примени обједињеног модела безбедносне аналитике, који обухвата податке оружаних снага, полиције, служби безбедности, али и других војних и цивилних органа и агенција, а осим војног, захвата и остале секторе безбедности.

- Обједињавање безбедносне аналитике на стратегијском нивоу посебно је карактеристично и у државама нашег окружења. Пример Координације у систему националне безбедности Хрватске непосредна ј потврда наведеног.
- Безбедносном аналитиком се римарно баве особе и тимови именовани као аналитичари, са изузетно разуђеним односом према карактеристикама које те особе треба да поседују.
- У свом раду аналитичари примењују сличну прцедуру, те користе велики скуп научних и ненаучних метода и поступака, примерених подручју у којем се аналитика обавља. Све више се успоставља захтев да аналитичари у свом раду користе напредне научне методе и технике.
- Општи је закључак да се аналитичари у значајној мери ослањају на искуство (интуиција) и знање (критичко мишљење).
- У раду аналитичара користи се ванредно велики број података и информација. У том смислу, незамењиве су базе информација у домену конкретне врсте аналитике, као и обједињене безбедносне аналитике.
- Све више се истиче захтев који се примењује у пракси савремених земаља, да се и процес и процедуре рада аналитичара стандардизују.

2. РЕЗУЛТАТИ ЕМПИРИЈСКОГ ИСТРАЖИВАЊА

Домен безбедности често јесте под велом тајности. Ово се, пре свега, односи на изворе података и конкретне закључке на основу њих. Стога, тешко је доћи до потребних информација за научна истраживања. Међутим, у овом истраживању ради се о теоријском моделу безбедносне аналитике, за који нису потребни никакви тајни подаци, већ је неопходно прикупити опште информације којима располажу лица која се безбедносном аналитиком баве.

С обзиром на природу предмета истраживања, а ради утврђивања тренутног стања у области безбедносне аналитике у пракси, али и провере предложеног теоријског модела исте, истраживање је спроведено међу експертима из ове области. Како је безбедносна аналитика недовољно истражена област, тако није било једноставно пронаћи лица која су се директно бавила овим пословима. па је истраживање проширено и на лица која су се

индиректно бавила безбедносном аналитиком, кроз свој радни *ангажман или научно-истраживачки рад*.

Према Милићу Милићевићу, основа експертског оцењивања је у томе да се у поступку добијања неопходне нове информације користе људи компетентни у датој области, експерти који проводе интуитивно-логичку анализу одређеног проблема и износе своје мишљење о решаваном проблему. Мишљење експерата прикупља се у ситуацијама када су: подаци оскудни или их је тешко добити, када је добијање података неким другим методама превише скупо, када подаци нису једнозначно одређени и могу се тумачити на различите начине и када постоји потреба да се изврши почетни приказ проблема. Мишљење експерата може се имплементирати у добијање процене нових, раритетних, сложених или слабо разумљивих проблема, а посебно у процесу доношења војних одлука (Милићевић, 2014).

Истраживање које је спроведено кроз *Упитник усмереног интервјуа* обухватило је 46 лица из области безбедности и безбедносне аналитике, већим делом доктора наука. Поред тога, а након обављеног усмереног интервјуа, одабрана је група од пет експерата предметне области која је у *усменом разговору*, *интервјуу*, дала своју оцену теоријског модела безбедносне аналитике.

2.1 Испитивање применом упитника за усмерени интервју

Структура испитаника

У Табели 21 приказана је структура узорка по полу, узрасту, образовању и искуству на пословима везаним за безбедносну аналитику[27].

Табела 21. *Структура испитаника који су учествовали у истраживању*

[27] Истраживање је обављено методом испитивања, применом технике усмереног интервјуа. Испитаницима је путем интернета достављен упитник за усмерени интервју, којом приликом им је саопштено да је интервју анониман и да служи само за потребе израде докторске дисертације. Стога, у дисертацији се не наводе имена испитаника, али су позната ментору, који је одобрио њихов списак.

Категорија	Поткатегорија	Проценат
Пол	Мушки	96,43%
	Женски	3,57%
Старосна доб	До 40 година	7,14%
	Од 40 до 55 година	39,29%
	Преко 55 година	53,57%
Професионални статус	Активни припадници служби безбедности	21,43%
	Пензионисани припадници службе безбедности	46,43%
	Академска заједница	14%
	Корпоративна безбедност и менаџмент	14%
	Пословне/владине канцеларије	4,14%
Искуство у безбедносној аналитици	До пет година	7,14%
	Од пет до10 година	39,29%
	Преко 10 година	53,57%
Образовање	Високо образовање/мастер	14,81%
	Докторске студије	85,19%
Институција у којој су се бавили безбедносном аналитиком	Војне институције (ВОА, ВБА, Генералштаб, Команде Војске)	36,84%
	Полицијске/државне институције (МУП, БИА, РДБ Р. Српске)	31,58%
	Образовне/истраживачке институције (институт, факултет)	15,79%
	Остало (приватни сектор, канцеларија савета, кроз наставу)	15,79%
Период бављења аналитиком	Између 1992. и 1999.	12,50%
	Између 1999. и 2009.	25%
	Након 2009.	29,17%
	Комбиновано (више периода)	33,33%

Безбедносна аналитика је примарно „мушко занимање“, што се може и видети из овог истраживања (претходна табела), где су жене минимално заступљене. Апсолутну већину од 96,43% чине мушкарци. Највећи број испитаника припада категорији старосне доби преко 55 година, 53,57%, али је значајан број и у категорији 40-55 година старости, 39,29%. Стога не чуди и да пензионисани припадници службе безбедности чине највећи део узорка, 46,43%, док су активни припадници мање заступљени са 21,43%, што значи да истраживање више одражава ставове и искуства оних који су завршили активну службу. Остали учесници долазе из академске заједнице 14%, корпоративне безбедности и менаџмента 14% и пословних/владиних канцеларија 4,14%.

Ово показује да узорак углавном чине искуснији и старији професионалци, што може указивати на дубоко знање и дугогодишње искуство, али и на слабију заступљеност

млађих генерација аналитичара. Такође, структура показује да узорак има мултисекторску димензију, али да доминирају војно-безбедносна искуства.

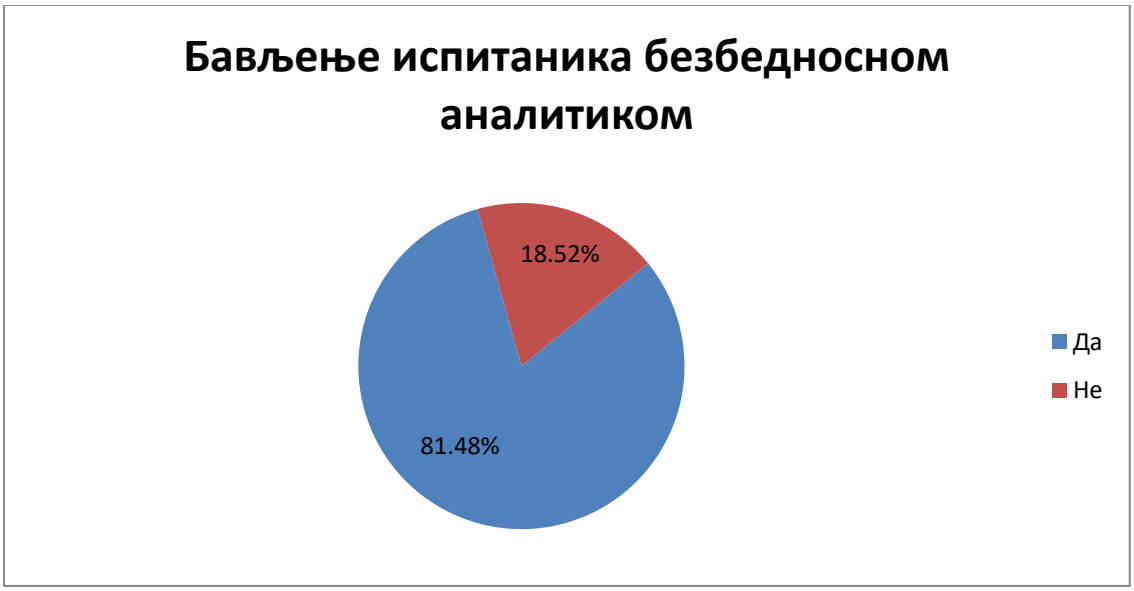
Највећи број испитаника има преко 10 година искуства (53,57,%), што показује да је узорак веома поуздан, 39,29% има 5-10 година искуства, што представља групу са средњим искуством. До пет година има 7,14 %, тако да је део млађих аналитичара и даље укључен. Занимљиво је, а врло значајно за ово истраживање, да поред деценијског искуства у безбедносној аналитици, већина испитаника има и докторске дипломе, 85,19%.

Резултати показују да су испитаници који су се бавили безбедносном аналитиком углавном долазили из војних и државних институција, што потврђује и податак да је највећи број испитаника (36,84%) радио у војним структурама као што су ВОА, ВБА, Генералштаб и команде Војске. Значајан део узорка (31,58%) чинили су стручњаци из полицијских и безбедносних служби (МУП, БИА, РДБ), док је мањи број ангажован у образовним и истраживачким институцијама или у приватном сектору. Оваква структура указује да су одговоре давали испитаници са практичним искуством у кључним институцијама националног безбедносног система, али и да је присутан мањи број теоријски оријентисаних учесника.

Када је реч о временском оквиру њиховог ангажовања, примећује се да су најзаступљенији они који су се безбедносном аналитиком бавили у периоду након 2009. године (29,17%) или континуирано током више периода (33,33%), што упућује на то да се ради о релативно савременом и актуелном искуству. Укупно преко 60% испитаника има искуство стечено у последње две деценије, што сугерише да је узорак у складу са савременим развојем аналитичких пракси у области безбедности.

Сумирано, може се закључити да су испитаници високо компетентни, већином из државних и војних институција, са ангажовањем у скоријем временском периоду, што повећава поузданост и релевантност њихових ставова у истраживању. У даљем, следе питања из усмереног интервјуа и одговори испитаника.

На питање: *Да ли сте се у професионалној служби бавили безбедносном аналитиком,* одговори испитаника приказани су на Графикону 1.



Графикон 1. *Бављење испитаника безбедносном аналитиком*

Дакле, 81,48% испитаника се бавило безбедносном аналитиком директно кроз професионални рад, док је 18, 52% то чинило на друге начине (научно-истраживачки рад, на пример).

Следеће питање је било: *Да ли сте у склопу свог образовања имали прилике да изучавате тематику везану за безбедносну аналитику (кроз предмете, наставу, практичну наставу и слично)*? Одговор је приказан на Графикону 2.

Графикон 2. *Изучавање безбедносне аналитике испитаника*

На ово питање 71,43% испитаника је одговорило са „да“, 21,43% је одговорило са „да, индиректно“ и 7,14% са „не“. Овај резултат показује да већина испитаника има значајно искуство и формално или практично образовање у области безбедносне аналитике.

Чињеница да се 81,48% њих бави безбедносном аналитиком директно кроз професионални рад указује на то да узорак чине углавном стручњаци са конкретним радним искуством у овој области, што повећава релевантност њихових одговора.

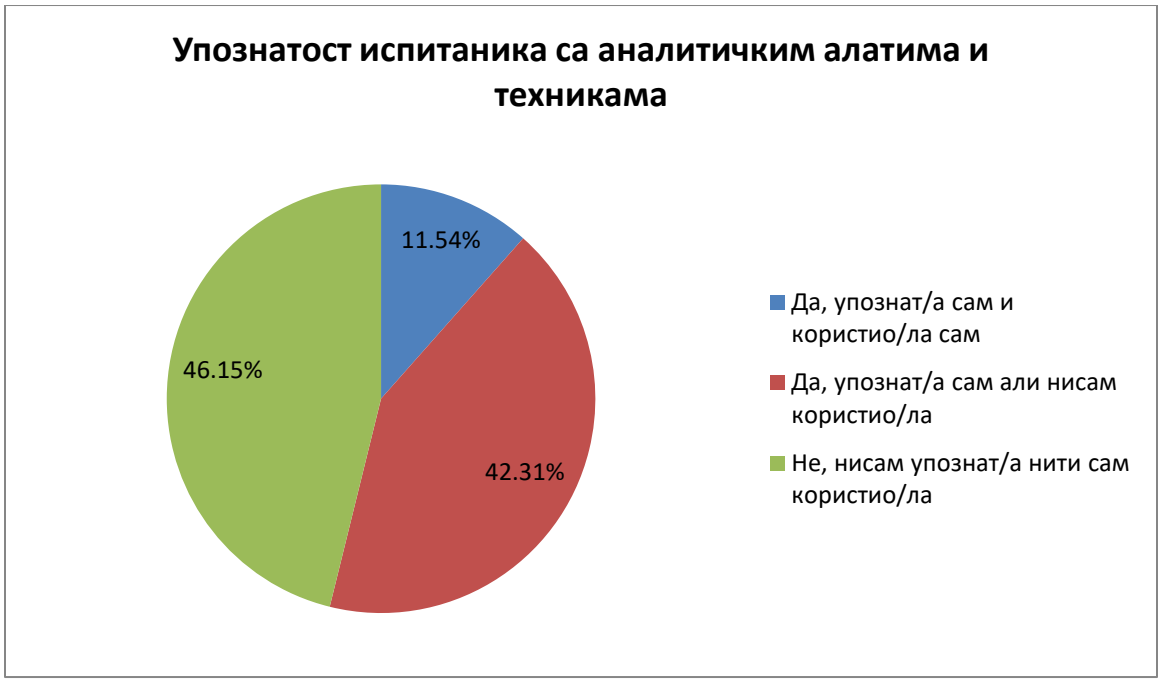
С друге стране, 71,43% је имало прилике да изучава безбедносну аналитику током образовања, а додатних 21,43% индиректно, што говори о солидној теоријској основи и академској упућености у теме безбедности. Само 7,14% испитаника без формалног образовног контакта са овом облашћу указује на то да је реч о појединачним изузецима.

У целини, резултати показују да узорак обухвата висококомпетентне појединце и са практичним и са образовним искуством у безбедносној аналитици, што представља добру основу за валидност и поузданост добијених ставова у истраживању.

Затим, на питање: *Да ли сте кроз образовање или приликом заснивања радног односа имали прилике да прођете неку врсту обуке за обављање послова из домена безбедносне*

аналитике, сви испитаници су одговрили са „да“, дакле 100% њих. Ово индикује да је безбедносни систем формално обезбедио едукацију у овом сектору.

На питање: *Да ли сте пре ступања на своје дужности (за оне који су радили у обавештајном сектору) били упознати са аналитичким алатима и техникама које би Вам олакшале рад попут брејнсторминга, креирања индикатора или анализе супротстављених хипотеза*, одговори испитаника се могу видети на Графикону 3.



Графикон 3. *Упознатост испитаника са аналитичким алатима и техникама*

1) Не, нисам упознат/а са наведеним техникама нити сам исте користио/ла у свом раду 46,15%,
2) Да, упознат/а сам са наведеним техникама, али их нисам користио/ла у свом раду 42,31% и
3) в) Да, упознат/а сам са наведеним техникама и користио/ла сам их у свом раду 11,54%.

Добијени резултати указују на изражен дисконтинуитет између формалног образовања, професионалног искуства и реалне примене савремених аналитичких техника у области безбедносне аналитике. Наиме, иако је 81,48% испитаника навело да се бавило аналитиком кроз професионални рад, 71,43% је изучавало аналитику у склопу формалног

образовања, а свих 100% је прошло одређени вид обуке приликом ступања на аналитичке послове, само 11,54% њих је било упознато и користило конкретне аналитичке алате и технике као што су брејнсторминг, креирање индикатора или анализа супротстављених хипотеза.

Ови налази упућују на закључак да постоји структурни недостатак у програмима образовања и обуке – нагласак је претежно стављен на теоријска знања и опште методолошке оквире, док је практична примена савремених техника остала у другом плану. Као последица, значајан број аналитичара није развио неопходне вештине за систематско коришћење алата који би могли унапредити квалитет аналитичког процеса и донетих закључака.

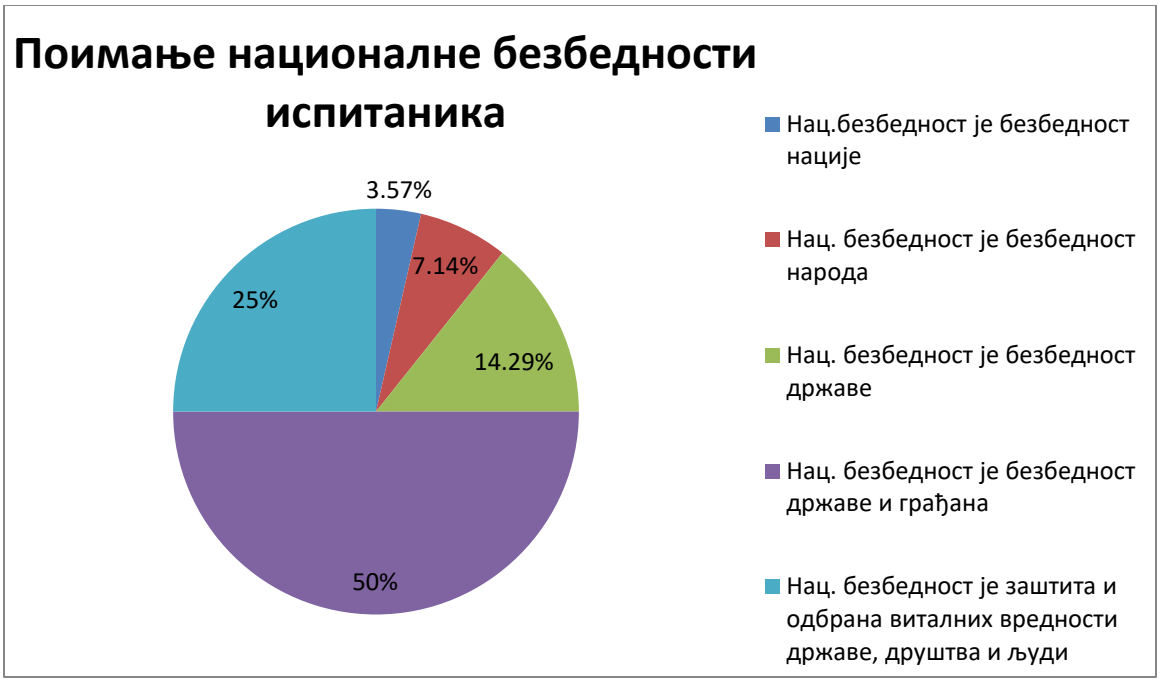
Стога, импликације за праксу су јасне: потребно је унапредити постојеће наставне програме и модуле обуке тако да већи акценат буде на практичним вежбама, студијама случаја и раду са конкретним аналитичким техникама. На тај начин би се обезбедило да обука не остане на нивоу формалне процедуре, већ да заиста резултира применљивим знањима и вештинама.

2.1.1 Усмерени интервју

Усмерени интервју чине три дела: 1) питања из опште, претежно националне безбедности, 2) питања везана за безбедносну аналитику и 3) питања везана за теоријски модел безбедносне аналитике.

1) Питања од опште (националне) безбедности

С обзиром на фокус истраживања – националну безбедност, логично је било да прво утврдимо шта испитаници под тим појмом подразумевају. *У теорији постоји став да је појам национална безбедност остао недефинисан. Од понуђених одговора подвуците онај који одговара Вашем ставу или допишите свој став ако се не слажете са понуђеним*, испитаници су одговорили на следећи начин:



Графикон 4. *Поимање националне безбедности испитаника*

1) Национална безбедност је безбедност нације 3,57 %,
2) Национална безбедност је безбедност народа 7,14%,
3) Национална безбедност је безбедност државе 14,29%,
4) Национална безбедност је безбедност државе и грађана 50% и
5) Национална безбедност је заштита и одбрана виталних вредности државе, друштва и људи 25%.

Највећи део испитаника (75%) своје схватање националне безбедности везује за интеграцију државе и појединца, односно за заштиту виталних вредности друштва у целини. То показује да се традиционални ужи појмови (држава или нација) све више напуштају, а да се у пракси усвајају концепти ближи савременим доктринама безбедности, у којима је у фокусу не само држава као носилац суверенитета, већ и грађани као носиоци права и вредности које држава штити.

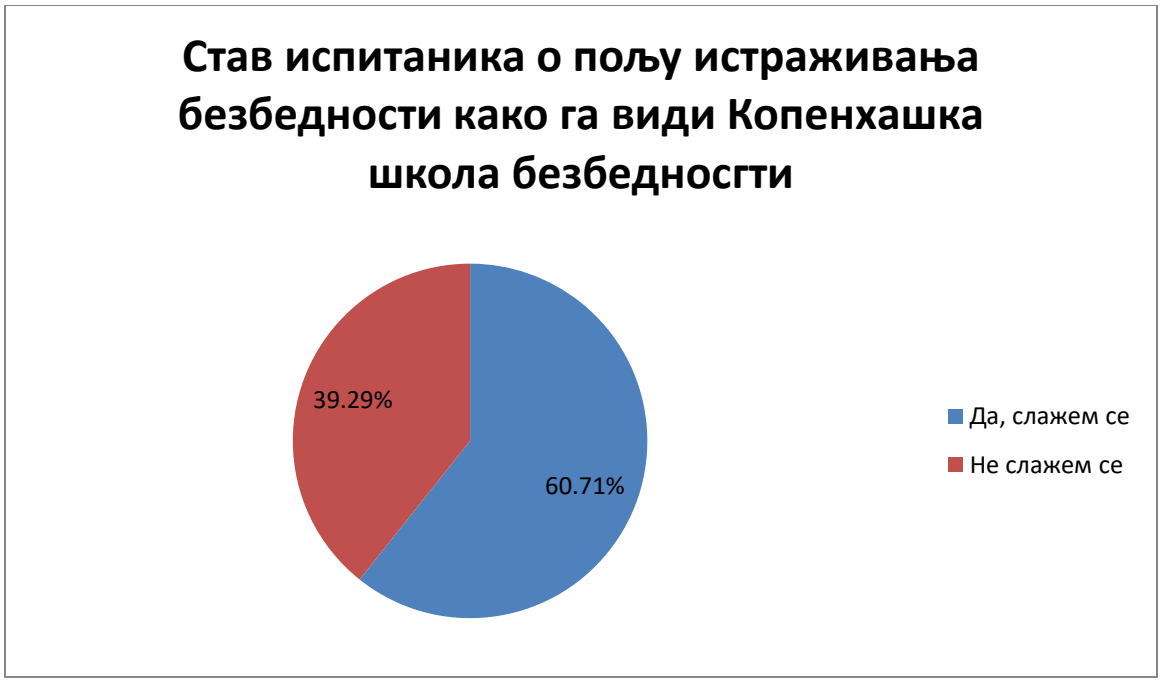
С обзиром на то да у тероији не постоји консензус по питању референтног објекта националне безбедности, логично је било да утврдимо шта по том питању мисле испитаници. На питање: *Шта је по Вама референтни објект националне безбедности*, одговори испитаника (експерата) су приказани на Графикону 5.

Графикон 5. *Став испитаника о референтном објекту националне безбедности*

1) Територија државе (границе) 3, 57%,
2) Националне вредности, интереси и циљеви 75% и
3) Остало 21,43%.

Већина експерата (75%) сматра да су националне вредности, интереси и циљеви референтни објект националне безбедности. Овакав став је у складу са савременим теоријским приступима који безбедност не своде искључиво на територију или војни аспект, већ је посматрају шире, као заштиту виталних вредности и интереса државе и друштва.

У теоријском моделу безбедносне аналитике његов први сегмент јесте знање о безбедности, које је, с научног аспекта посматрано, преузето од Копенхашке школе безбедности. Стога, следеће питање у интервјуу односило се на Копенхашку школу безбедности, која је осим војног, утврдила и друге секторе безбедности (политички, економски, војни, социјетални и еколошки сектор). Питање за експерте било је: *Слажете ли се да се тиме исцрпљује поље безбедности или имате другачије гледиште, односно додатак наведеним секторима*?

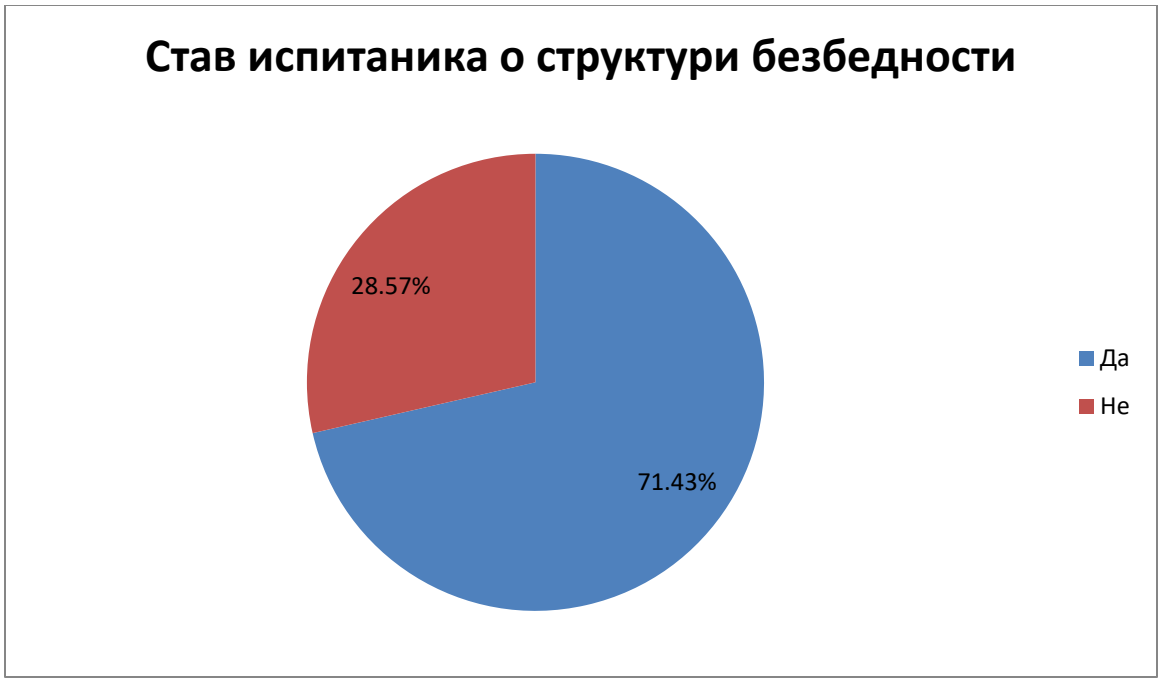


Графикон 6. *Став испитаника о пољу истраживања безбедности како га види Копенхашка школа безбедности*

На ово питање 60,71% испитаника је одговорио да се слаже са ставовима Копенхашке школе безбедности у погледу сектора безбедности, а 39, 29% не мисли тако.

Већина експерата прихвата проширену концепцију безбедности која иде изван класичног војног оквира, што указује на релативну зрелост приступа безбедности у пракси. Међутим, чињеница да 39,29% није у потпуности сагласно, указује да постоје различите перспективе, нпр. неки експерти сматрају да би се безбедност могла анализирати и кроз друге секторе, као што су кибернетички, културни или технолошки сектор. Ово показује да иако је Копенхашка школа дала широк оквир, дискусија о „додатним“ секторима је и даље актуелна.

Следеће питање је било: *У теорији постоји класификација битних чиниоца (компоненти) националне безбедности на унутрашњу, спољашњу и интегралну безбедност. Да ли се слажете да наведени чиниоци представљају структуру система безбедности*?



Графикон 7. *Став испитаника о структури безбедности*

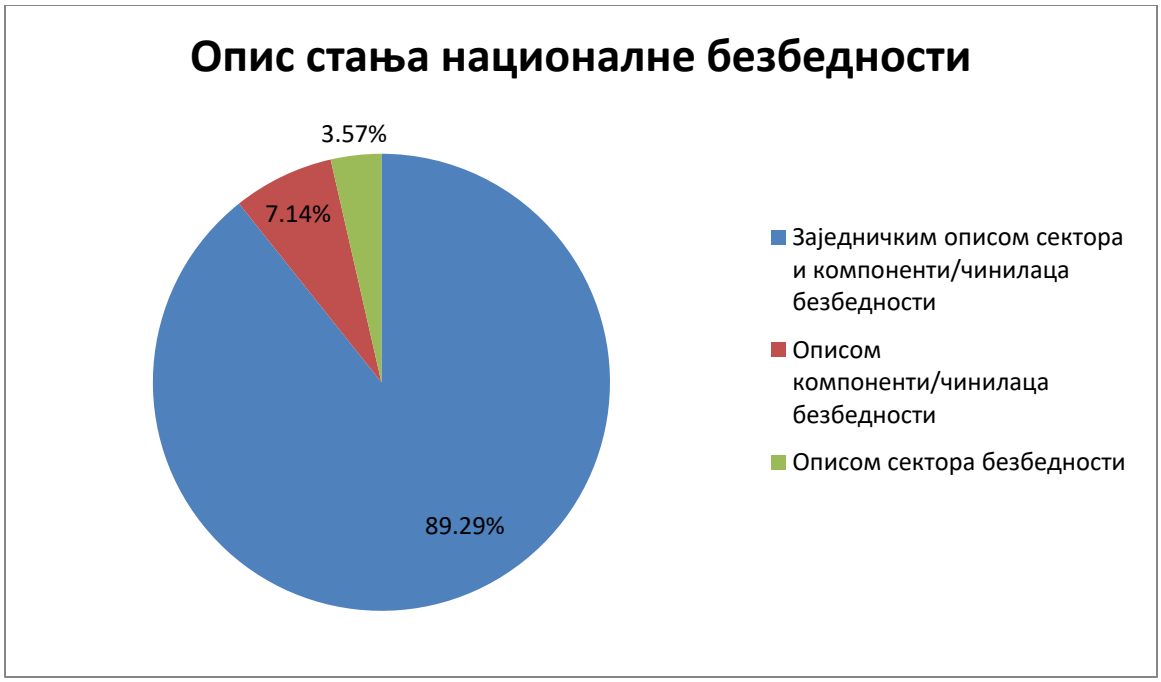
На ово питање 71,43% је одговорило са „да“, док је 28,57% њих имало другачије виђење.

Већина експерата види класичну тријаду као корисну и применљиву за систематизацију чинилаца безбедности. Овај резултат показује јаку консензусну подршку традиционалној подели на унутрашњу, спољашњу и интегралну безбедност. При томе, и анализа националне безбедности преко компоненти унутрашња, спољна и интегрална, у крајњем, обухвата секторе безбедности како их је утврдила Копенхашка школа безбедности, свакако са могућом доградњом.

Наредно питање је повезало претходна два: *Опис стања националне безбедности као целине, а узимајући у обзир ставове из претходних питања, могуће је дати*:

1) Описом сектора безбедности,
2) Описом компоненти/чинилаца безбедности аналитичким приступом и
3) Заједничким описом сектора и компоненти/чинилаца безбедности аналитичко-синтетичким приступом.

Одговори су приказани на Графикону 8.



Графикон 8. *Опис стања националне безбедности*

Одговори на ово питање су такви да 89,29% испитаника сматра да се заједничким описом компоненти/чинилаца безбедности аналитичко-синтетичким приступом може дати опис стања националне безбедности као целине, док њих 7,14% сматра да се то може учинити описом компоненти/чинилаца безбедности аналитичким приступом, а 3,57 само описом сектора безбедности.

Подршка аналитичко-синтетичком приступу са интеграцијом и сектора и чинилаца указује да испитаници препознају комплексност савремене националне безбедности, где изоловано посматрање није довољно. Безбедност се све више разуме као систем повезаних елемената, од државних институција, преко економских, социјалних, еколошких до информационих и других димензија. Отуда је интегрално сагледавање неопходно за реалан и потпун опис њеног стања.

С обзиром на то да се теоријски модел безбедносне аналитике проверава на супротстављању тероризму, следећи сет питања односи се на тероризам као претњу. Прво такво питање је: *Да ли се слажете да тероризам представља опасност за све државе света без изузетка?* Одговори су приказани на Графикону 9.

Графикон 9. *Став о тероризму*

Одговори испитаника су такви да се 89,29% њих слаже са овом тврдњом, 7,14% није сигурно, а 3,57% се не слаже.

На питање: *Да ли се слажете са тврдњом да тероризам увек функционише у домену политике и спада у сложене облике политичког насиља*, испитаници су одговорили на следећи начин: 78,57% се слаже, 17,86% није сигурно и 3,57% се не слаже. Ови одговори су приказани на Графикону 10.

Графикон 10. *Тероризам као политичка категорија*

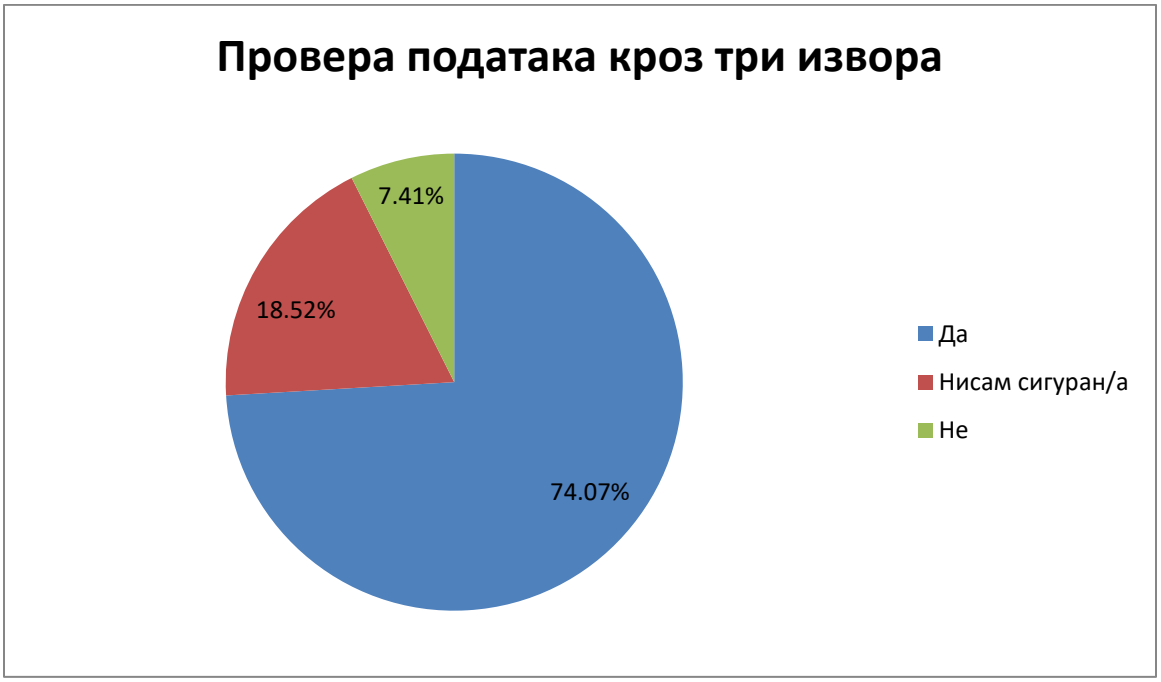
Наредно питање је: *Често тежимо да утврдимо просторни распоред терористичких напада, њихове последице, смртност, порекло и финансирање терористичких организација и сличне податке. Стога, да ли сматрате да је обавештајни рад значајан за супротстављање савременом тероризму као претњи безбедности?* Сви испитаници, њих 100% је изабрало одговор са „да, изузетно значајан“.

Ови резултати указују на висок степен свести испитаника о претњи коју тероризам представља на глобалном нивоу, будући да 89,29% учесника сматра да тероризам угрожава све државе без изузетка. Такође, већина испитаника, 78,57%, препознаје политички карактер терористичких активности и сложеност облика политичког насиља, што указује на разумевање тероризма као феномена који је дубоко укорењен у политичком контексту. Потпуна сагласност испитаника, 100%, у погледу значаја обавештајног рада за супротстављање савременом тероризму, додатно наглашава перцепцију критичне улоге информација и анализе у превенцији и управљању безбедносним претњама. Укупно, ови налази потврђују да испитаници тероризам виде као сложен и глобално релевантан безбедносни изазов, чије разумевање и контрола захтевају интегрисан приступ који обухвата политичке, аналитичке и обавештајне аспекте.

2) Питања из домена безбедносне аналитике

Питања из домена безбедносне аналитике тежишно су била усмерена на познавање те области, као и ставове испитаника о Полицијско-обвештајном моделу у Републици Србији.

Прво питање из домена безбедносне аналитике у спроведеном истраживању било је: *Да би прикупљени подаци били веродостојни, морају се проверити кроз најмање три различита извора. Да ли је наведена тврдња истинита?* Одговори су приказани на Графикону 11.

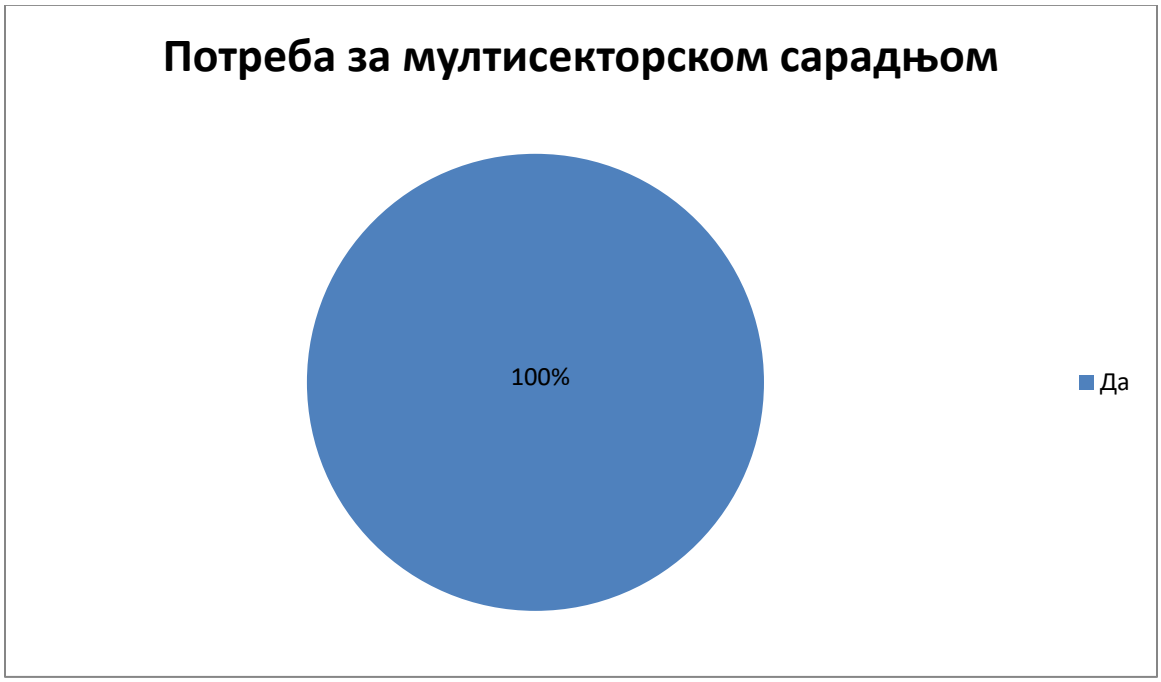


Графикон 11. *Провера података кроз три извора*

Одговор „да“ је дало 74,07% испитаника, 18,52% „није сигурно“, а 7,41% се не слаже са наведеном тврдњом. Резултати првог питања из домена безбедносне аналитике показују да већина испитаника, њих 74,07%, препознаје значај верификације података кроз најмање три различита извора као предуслов њихове веродостојности, што представља један од кључних принципа савременог аналитичког рада. Ипак, присуство неодлучних, 18,52% и оних који се не слажу са овом тврдњом, 7,41%, указује на постојање извесног недовољног

разумевања аналитичких стандарда и различитих приступа у процени поузданости информација.

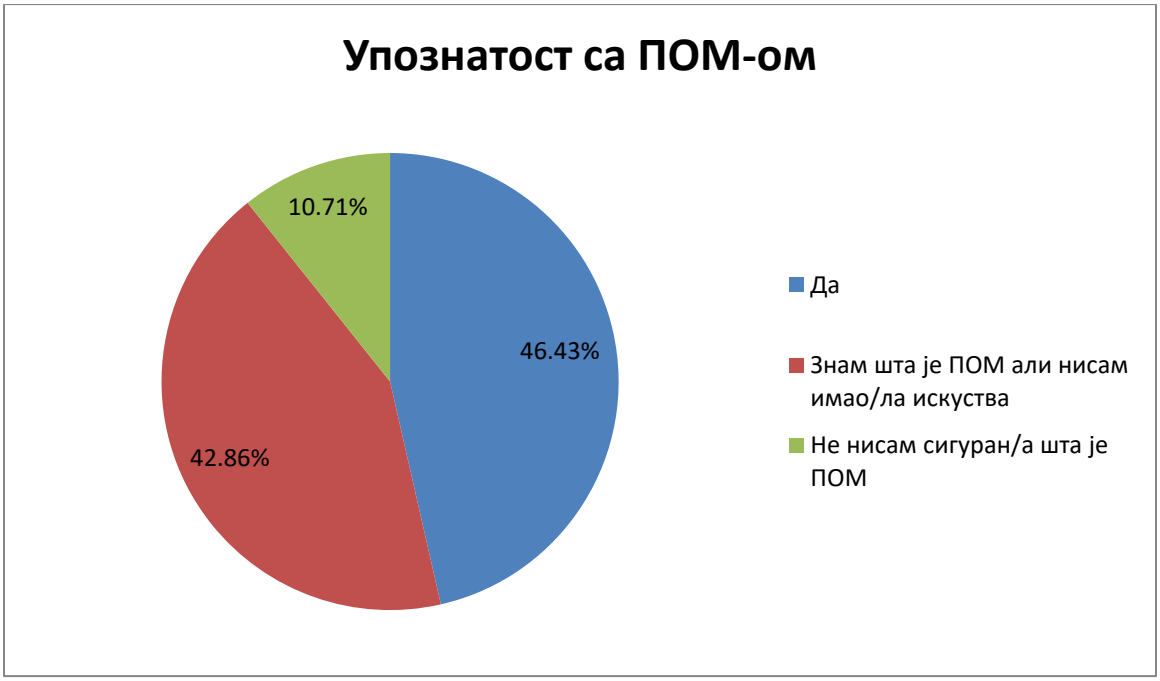
Следеће питање је било: *Како би се дошло до потпуних обавештајних података, на пример, о питањима везаним за тероризам или стању безбедности једне државе, потребна је мултисекторска сарадња (полиција, војска, службе безбедности, цивилни сектор и слично)?* На питање да ли је наведена тврдња истинита, 100% испитаника је одговрило са „да“.



Графикон 12. *Потреба за мултисекторском сарадњом*

Овај налаз указује да постоји јасна свест о томе да савремене безбедносне претње, као што су тероризам и сложене кризне ситуације, превазилазе капацитете појединачних институција. Због тога је неопходно укључивање различитих сектора – полиције, војске, безбедносних служби, али и цивилних структура, како би се добила свеобухватна и поуздана слика безбедносног стања. Потпуна сагласност испитаника истиче мултисекторску сарадњу као кључни предуслов за ефикасно супротстављање савременим изазовима и ризицима по националну и међународну безбедност.

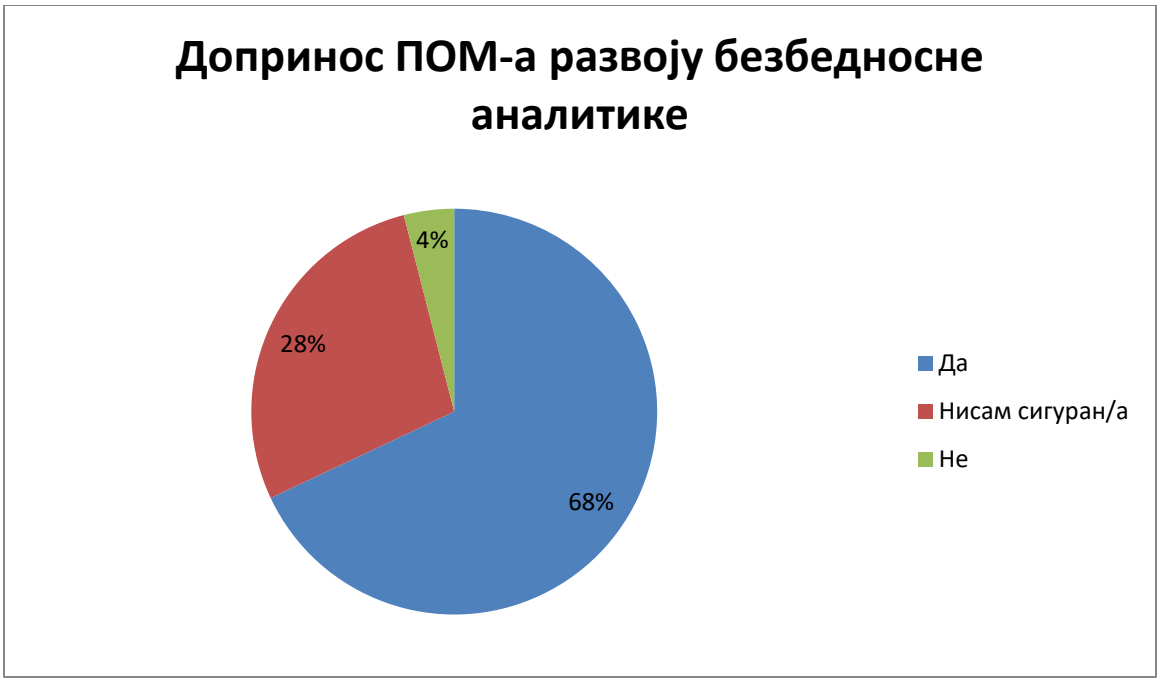
Кроз овај део истраживања смо проверили како испитаници гледају на полицијско-обавештајни модел кроз питање: *Да ли сте кроз свој рад упознати са полицијско-обавештајним моделом (ПОМ)?* Одговрои су приказани на Графикону 13.



Графикон 13. *Упознатост са ПОМ-ом*

На ово питање 46,43% испитаника је одговорило са „да“, а 42,86% са знам шта је ПОМ, али нисам имао/а практична искуства, док је 1071% одговорило да није сигурано шта је ПОМ.

Они који су одговорили са „да“ на ово питање, одговарали су и на следеће: *Уколико је ваш одговор на предходно питање „да“, да ли мислите да ПОМ може бити један од чинилаца који доприноси развоју безбедносне аналитике*? Одговор је приказан на Графикону 14.



Графикон 14. *Допринос ПОМ-а развоју безбедносне аналитике*

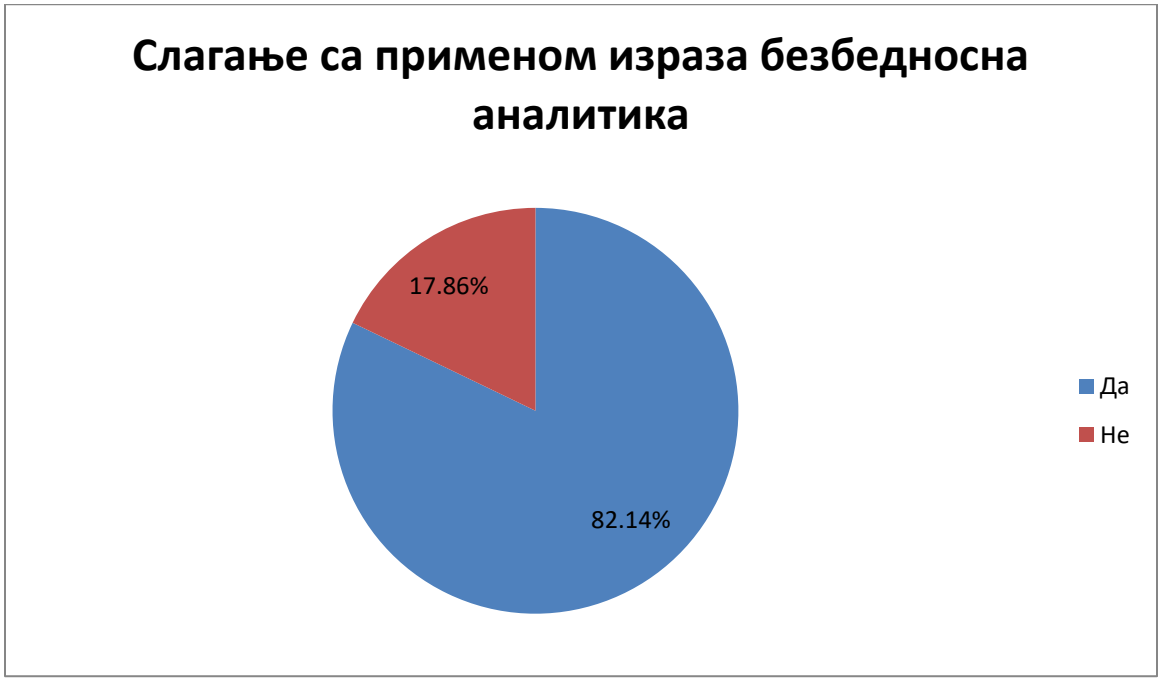
На ово питање 68% од оних који су упознати са ПОМ-ом сматра да је он чинилац који може да допринесе развоју безбедносне аналитике, 28% њих није сигурно, док је 4% одговорило са „не“.

Резултати истраживања указују да је познавање полицијско-обавештајног модела (ПОМ) међу испитаницима релативно високо. Конкретно, 46,43% испитаника изјавило је да има практично искуство са ПОМ-ом, док 42,86% познаје теоријске основе модела, али није имало практичну примену. Мања група, њих 10,71%, није било сигурно у своје знање о ПОМ-у. Ови подаци указују да је већина испитаника на неки начин упозната са моделом, што потврђује релевантност узорка за даље испитивање перцепције значаја ПОМ-а у безбедносној аналитичкој пракси.

Међу испитаницима који имају практично искуство са ПОМ-ом већина, 68%, сматра да модел може значајно допринети развоју безбедносне аналитике. С друге стране, 28% испитаника није сигурно у његову ефикасност, док мањина од 4% категорички не види његов допринос. Ово указује да ПОМ генерално има позитиван утицај на безбедносну анализу, али и да постоје извесне нејасноће или недоумице у погледу његове примене.

На питање: *Безбедносна аналитика је уједно и мултисекторска вештина и мултидисциплинарна област јер обухвата више различитих сектора безбедности и има мултидисциплинарну примену у истраживању области безбедности. Да ли је наведена тврдња истинита*, сви испитаници, 100% су одговорили са „да“.

Следеће питање је било: *Да ли сте сагласни са ставом да се израз* ***безбедносна аналитика*** *примењује у пракси под називима Обавештајна аналитика, Криминалистичка анализа, Криминалистичко-обавештајна аналитика и другим?* Одговор је приказан на Графикону 15.



Графикон 15. *Слагање са применом израза безбедносна аналитика*

Од укупног броја испитаника, њих 82,14% је одговорило са „да“, а 17,86% са „не“.

Резултати истраживања показују висок степен сагласности испитаника у погледу мултисекторске и мултидисциплинарне природе безбедносне аналитике. Сви испитаници су се сложили са тврдњом да безбедносна аналитика обухвата више различитих сектора безбедности и има мултидисциплинарну примену у истраживању области безбедности. Што се тиче терминологије, већина испитаника, њих 82,14%, сматра да се израз „безбедносна аналитика“ у пракси примењује и под називима као што су обавештајна

аналитика, криминалистичка анализа или криминалистичко-обавештајна аналитика, док 17,86% испитаника није сагласно са овом тврдњом.

Ови резултати указују на универзално прихватање мултисекторског и мултидисциплинарног карактера безбедносне аналитике, као и на постојање варијација у терминологији у стручним окружењима, што може имати импликације за стандардизацију појмова и праксе у овој области.

У наредном питању истраживани су ставови експерата о обавештајном циклусу. Стога је у питању дата табела у којој су ставови из теорије који указују на фазе обавештајног циклуса. Испитаници су замољени да се определе за један став: *Молимо Вас да се определите за неки од предлога (заокружите број) или да допишете шта Ви сматрате као фазе обавештајног циклуса*. Да би избегли пристрасност, у Табели нису дата имена аутора који су дефинисали наведене фазе (Види: Табела 4).

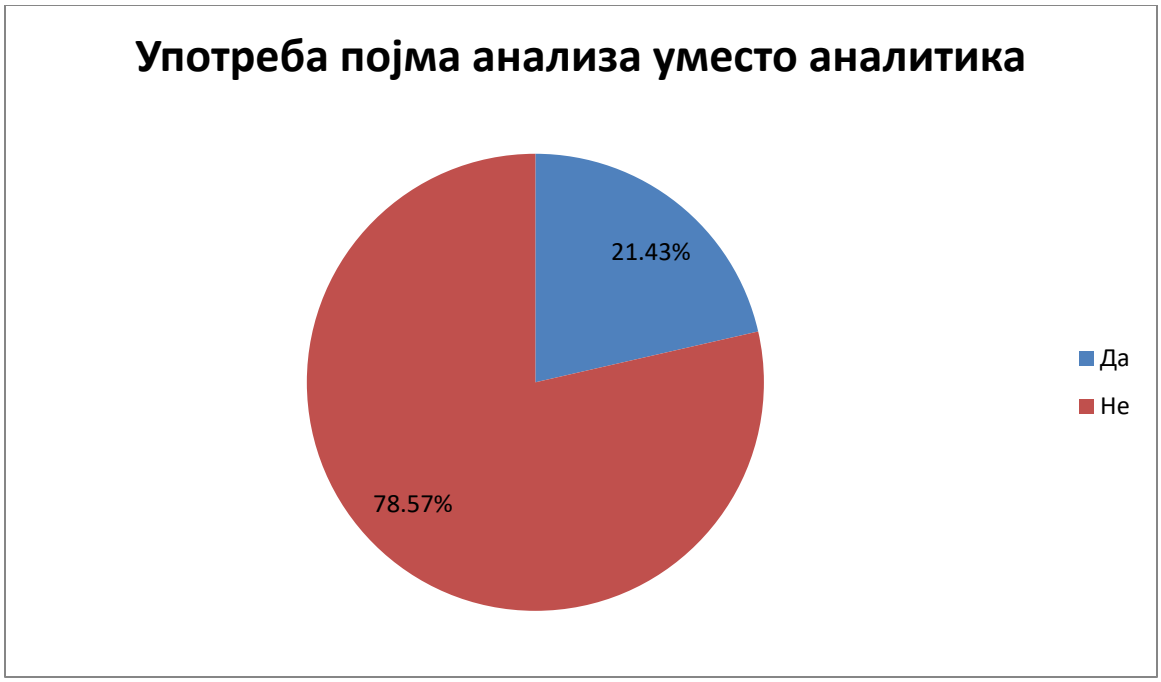
Резултати одговора на ово питање приказани су на Графикону 16.

Графикон 16. *Став испитаника о фазама обавештајног циклуса*

Најчешћи одговор је био број 6, за који се определило 53,7% испитаника, одговор под 1 је добио 10,7%, као и одговор под 5. Исти проценат има и број 7, где је 10,7% испитаника имало неку своју дефиницију фаза обавештајног циклуса, а те дефиниције су у суштини биле комбинације понуђених одговора. Затим, за одговор под бројем 4 одлучило се 7,2% испитаника, под 2 и 3 одговорило је по 3,5%.

Више од половине испитаника, 53,7% је изабрало одговор 6, што указује на то да већина сматра да обавештајни циклус треба да обухвати све фазе, од иницијативе до повратне спреге, тј. да је најдетаљнији модел најприкладнији. Одговори 2 и 3 (једноставнији модели) су добили најмању подршку, по 3,5%, што показује да већина испитаника сматра да једноставан циклус није довољан. Одговори 1, 4 и 5 су добили умерену подршку од 6,9 до 10,7%, што показује да постоји мала група која више цени теоријске или управљачке аспекте. Део испитаника, њих 10,7% је само дефинисало фазе, али у суштини су комбиновали постојеће моделе. То указује на креативан, али стандардизован приступ. Испитаници генерално прихватају комплетан и циклусни приступ обавештајном циклусу (од идентификације проблема до анализа, продукције и повратне спреге). Мање сложени модели и строго теоријски модели нису толико бирани, што може да указује на практичну оријентацију испитаника.

Следеће питање односило се на повезивање аналитике и обавештајног циклуса: *Аналитика, као део Обавештајног циклуса, негде се (нпр. у полицији) именује као анализа. Да ли сматрате да је употреба појма анализа уместо аналитика коректно?* Одговори су приказани на Графикону 17.



Графикон 17. *Употреба појма анализа уместо аналитика*

На ово питање 78,57% испитаника је одговорило са „да“, а 21,43% са „не“.

Добијени подаци показују на тенденцију ка практичном усвајању термина анализа уместо аналитика, што упућује на доминацију језичке и институционалне праксе над стриктним теоријским разликовањем појмова. Међутим, релативно висок проценат оних који инсистирају на разграничењу показује да у стручној заједници постоји свест о значају прецизне терминологије и потреба да се аналитика као шири појам не своди искључиво на процес анализе.

У оцени веродостојности информације и поузданости извора користе се модели „4 x 4“ (Србија, ЕУ), „5 x 5“ (Велика Британија) и „6 x 6“ (САД), што је приказано у претходном делу дисертације. Питање је гласило: *Који је по Вама модел најкомплекснији и најприхватљивији за нашу теорију и праксу, заокружите одговор*. Одговори су приказани на Графикону 18.

Графикон 18. *Прихватљивост модела оцене веродостојности информација*

За модел „4 x 4“ се определило 46,43% испитаника, за „6 x 6“ 32,14%, а за „5 x 5“ њих21,43%.

Резултати истраживања показали су да је највећи број испитаника, 46,43%, изабрало модел „4 x 4“. Овај налаз указује на то да је 1) ово модел који се примењује у нашој пракси, те су се испитаници на њега навикли и 2) овај модел препознат као најјаснији и најфункционалнији оквир, заправо као модел који обезбеђује довољну прегледност и применљивост без непотребног усложњавања.

С друге стране, значајан проценат испитаника, њи (32,14%,определило се за модел „6 x 6“, што сведочи о постојању групе која сматра да је свеобухватнији и детаљнији приступ погоднији за анализу сложенијих процеса. Овај модел, због своје разрађености, упућује на потребу за дубљим аналитичким увиђајем и прецизнијим операционализацијама. Модел „5 x 5“ добио је најмању подршку од 21,43%. Овакав резултат може да сугерише да испитаници не виде довољну предност у „средњем решењу“ које није ни једноставно као „4 x 4“, нити довољно комплексно као „6 x 6“.

Наредно питање било је: *У теорији постоје различити ставови какве особине треба да има безбедносни (обавештајни) аналитичар. На основу свог искуства изнесите став о*

томе које су пожељне особине које треба да одликују обавештајног (безбедносног) аналитичара? С обзиром на то да су испитаници одговарали на ово питање произвољно (без понуђених одговора), набројали су мноштво особина сходно личном нахођењу и искуству. Сваки испитаник имао је простора да наброји колико год жели особина. Међутим, одређене особине су се нашле код више испитаника или свих.

Испитаници виде идеалног безбедносног аналитичара као особу са више кључних професионалних и личних особина. Најчешће помињане особине приказане су у Табели 22.

Табела 22. *Ставови испитаника о пожељним особинама безбедносних аналитичара*

ОСОБИНА	ПРОЦЕНАТ ИСПИТАНИКА	КОМЕНТАРИ СТАВОВА ИСПИТАНИКА
Образован	**52%**	Већи број испитаника је навео образовање као кључну особину, што указује на то да аналитичар треба да поседује чврсту теоријску основу и широку општу културу. Образовање је сматрано фундаменталним, јер омогућава разумевање сложених информација и контекста у коме се доносе одлуке.
Интелигентан	**50%**	Испитаници сматрају да аналитичар мора бити интелигентан, са способношћу логичког и критичког размишљања, брзог учења и обраде сложених података. Интелигенција је основа за решавање сложених проблема и правилну интерпретацију информација.
Информисан	**50%**	Овај проценат показује да испитаници веома цене познавање актуелних догађаја, контекста унутрашње и спољне безбедности и релевантних података. Аналитичар који је информисан боље разуме ситуацију и може донети прецизније закључке.
Комуникативан	**47%**	Испитаници наглашавају значај комуникације у раду аналитичара. Способност да пренесе информације јасно, да сарађује са тимом и да ефективно комуницира са колегама и надређенима сматра се једном од суштинских вештина.
Радознао	**43%**	Радозналост показује унутрашњу мотивацију аналитичара да истражује, прикупља податке и доводи у питање постојеће закључке. Ова особина је критична за развој креативних решења и откривање нових информација које могу бити од кључног значаја.
Аналитичан	**40%**	Испитаници сматрају да је способност анализе информација, идентификовање образаца и логичко закључивање суштински део посла аналитичара. Аналитичност омогућава структурирање и интерпретацију података на начин који доноси практичне и применљиве закључке.
Објективан	**36%**	Објективност је способност да се закључци доносе без личних пристрасности, емоција или спољних утицаја. Испитаници истичу да је ова особина важна за поузданост анализа и квалитет безбедносних процена.
Професионалан	**29%**	Испитаници наглашавају значај професионализма, који обухвата етику, дисциплину, поштовање процедура и стандарда у раду. Професионалан приступ омогућава поуздано и одговорно обављање задатака.
Критичко мишљење	**28%**	Ово је способност провере информација, процене њихове веродостојности и препознавања потенцијалних ризика. Испитаници сматрају да је критичко размишљање основно за избегавање грешака у анализи.
Способност (искуство) у оперативном	**20%**	Практично искуство у теренском раду или оперативним активностима омогућава боље разумевање података и стварног контекста у коме се информације користе.

раду		Испитаници истичу да теоријско знање мора бити допуњено практичним искуством.
Поуздан	**19%**	Испитаници указују да поузданост и доказана способност одговорног обављања задатака повећавају квалитет рада аналитичара.
Поштен	**15%**	Моралне и етичке вредности, као што је поштење, доприносе интегритету и професионалном угледу аналитичара.
Патриота	**10%**	Део испитаника истиче патриотизам и лојалност држави као вредност за аналитички рад.
Интуитиван	**6%**	Интуиција може помоћи у доношењу брзих закључака када подаци нису потпуни.
Прецизан, самопоуздан, индивидуалац и одговоран	**4%**	Ове особине су мање заступљене, али су се ипак појавиле више пута, уз образложење да доприносе професионалности и способности самосталног и одговорног рада.

Дакле, испитаници виде идеалног безбедносног аналитичара као образовану, интелигентну и информисану особу која је комуникативна, радознала и аналитична. Ове особине су кључне за ефикасан рад и доношење поузданих закључака. Моралне и личне карактеристике, као што су поштење, поузданост и самопоуздање, доприносе квалитету рада и професионалном интегритету, али нису пресудне за основну компетенцију аналитичара.

Наредно питање је такође било отвореног типа и омогућавало испитаницима да изнесу свој став у слободној форми. Питање је гласило: *Базе података имају велику улогу у раду безбедносних (обавештајних) аналитичара. Каква су Ваша искуства у раду са базама података?*

С обзиром на то да је питање конципирано тако да сваки испитаник може да изнесе свој став у отвореној форми, а да се не набрајају особине као у претходном питању, ово питање се не може интерпретирати кроз проценте. Међутим, може се извести закључак на основу датих одговора: испитаници наводе да су им искуства у погледу коришћња база података различита у смислу колико су дуго радили са базама и са којом врстом база података. Оно што је заједничко за све испитанике јесте да наводе да су им искуства позитивна и да аналитичке базе података олакшавају аналитичке и обавештајне послове.

На пример, високопозиционирани генерал и професор истиче: *Лична искуства као аналитичара у раду са различитим базама података су веома позитивна. Наиме, алати за приступ базама података умногоме олакшавају и временски скраћују проналажење, прикупљање, организовање, обраду, као и анализу великог броја података. Поред тога,*

базе података омогућавају бржу дисеминацију до различитих корисника у циљу правовременог обавештавања и потом доношења одговарајућих одлука надлежних органа у држави, с обзиром на многобројне претње и ризике у друштву и шире. Наиме, базе подака се прве претражују на захтев корисника, посебно када није могуће добити податке на други начин. Поједини испитаници, с друге стране, сматрају да би требало радити на даљем унапређивању аналитичких база података.

Следеће питање било је: *Да ли сте упознати са подацима доступним из јавних извора, односно ОСИНТ (open source intelligence) подацима?* Одговор је приказан на Графикону 19.

Графикон 19. *Упознатост испитаника са ОСИНТ подацима*

На ово питање 85,71% испитаника је одговорио са „да“, а 14,29% са „не“. Ови резултати указују на висок ниво свести и познавања јавних извора информација међу испитаницима, што је очекивано за професионалце у области безбедности и обавештајних анализа. Велика заступљеност упознатости са ОСИНТ подацима такође показује да аналитичари препознају значај коришћења јавних извора као поузданог допунског извора информација који може помоћи у обради и провери података пре доношења закључака.

Питање које смо следеће поставили је: *Да ли сте у свом раду користили јавно доступне научне базе попут Глобалног индекса тероризма, Института за економију и мир из Њујорка или неку сличну базу?* Одговори су приказани на Графикону 20.

Графикон 20. *Коришћење научних база*

На ово питање одговори су били такви да је 46,43% испитаника одговорило са „да“, 28,57% са упознат/а сам са овом (или сличном) базом података, али је у свом раду нисам користио/ла и 25% са „не“.

Ови резултати указују на релативно висок ниво свести о јавним научним базама, али и на постојање баријера у њиховој примени. Скоро половина испитаника активно користи ове базе у аналитичком раду, док један део препознаје њихову вредност, али их није имплементирала. Ово може указивати на потребу за додатним образовањем или практичном обуком за рад са јавним базама података.

Даље, постављено је питање: *Да ли сматрате да је безбедносна аналитика значајна за супротстављање савременим претњама безбедности попут тероризма*?

На ово питање понуђени одговори били су: да, нисам сигуран/а и не. Овде је 100% испитаника одабрало одговор „да“.

Овај резултат истиче да професионалци у области безбедности једногласно сматрају да је аналитички рад кључан за идентификацију, праћење и спречавање претњи као што су тероризам, хибридне претње и други ризици. Јасно је да безбедносна аналитика представља основни инструмент у доношењу одлука, процени ризика и развоју стратегија за ефикасно супротстављање претњама. Укратко, резултати показују да постоји потпуна свест о значају безбедносне аналитике међу испитаницима, што потврђује њену кључну улогу у савременим безбедносним системима.

У истраживању је било врло значајно утврдити какав је став познавалаца разних области аналитике по питању креирања јединственог модела безбедносне аналитике. Стога, следеће питање било је: *Сматрате ли да је могуће да се успостави јединствена безбедносна аналитика на нивоу националне (безбедност државе) безбедности?* Понуђени одговори били су „да“ и „не“, али су испитаници замољени да образложе своје одговоре, с обзиром на значај овог питања за истраживање. Резултати су приказани на Графикону 21.

Графикон 21. *Могућност успостављања јединствене безбедносне аналитике*

Ову идеју подржало је 82,12% испитаника, док је са „не“ одговорило 17,86%. Овако висок проценат позитивних одговора указује да већина испитаника препознаје потребу и потенцијал за успостављање јединственог аналитичког система на нивоу државне безбедности. Испитаници који су одговорили потврдно, углавном истичу да би јединствена безбедносна аналитика допринела бољој координацији између институција, ефикаснијем протоку информација и целовитијем сагледавању безбедносних претњи. Таква интегрисана анализа омогућила би брже и прецизније одлуке, као и развој превентивних стратегија.

С друге стране, 17,86% испитаника који су били против указали су на изазове који би могли пратити успостављање јединственог система, као што су институционалне надлежности, могући сукоби интереса, ограничен приступ подацима или ризик од прекомерне централизације.

Следеће питање се наслања на претходно и гласи: *Какав је Ваш став о потреби да се формира јединствени центар у оквиру служби безбедности, који би обједињавао досадашње моделе аналитика (обавештајна, криминалстичка…), то јест био кров за те аналитике. Заокружите и образложите одговор* Резултати су приказани на Графикону 22.

Графикон 22. *Став о формирању јединственог центра у оквиру служби безбедности*

На ово питање одговори су идентични као на предходно. Већинаиспитаника, њих 82,14% је за то да би формирање јединственог центра у оквиру служби безбедности било добро решење, док 17,86% њих не подржава ту идеју.

Ово показује доследност у одговорима и да они који сматрају да је неопходно успоставити безбедносну аналитику на националном нивоу уједно сматрају и да би њено успостављање требало да прати и формирање јединственог центра у оквиру служби безбедности, који би обједињавао досадашње моделе аналитика (обавештајна, криминалстичка…), односно био кров за те аналитике. Тако признати редовни професор у свом одговору наводи: *Савремени безбедносни изазови, ризици и претње захтевају адекватне и брзе одговоре одговарајућих институција државе на њихову појаву и отклањање, што захтева висок степен координације свих специјализованих служби, укључујући јединствену безбедносну аналитику. То захтева брз проток информација, безбедносних процена и анализа према корисницима и њихову повратну спрегу, а то се може остварити само у јединственом систему безбедносне аналитике.*

3) Стандарди

Чињеница је да су стандарди и стандардизација процеса незамењиви у свим сферама људске делатности. Стога, у овој групи питања истраживани су ставови експерата о стандардима и стандардизацији у домену безбедносне аналитике. Прво питање се односи на стандардизацију аналитичког процеса и гласи: *У разним врстама аналитике, поготово у страним државама користе се одређени стандарди. Молим Вас да укратко наведете какав је Ваш став о коришћењу стандарда у разним врстама аналитике у нашој земљи*.

Одговори на ово питање су били отвореног типа, а резултате смо груписали у три категорије. У првој се истиче потреба за увођењем и развојем стандарда и ту се налазе одговори попут: *Свакако би се морали успоставити валидни стандарди и исти поштовати, Сматрам да би стандардизација у Р. Србији била веома корисна, јер не постоје нормативна документа која дају правила и упутства за коришћење стандарда у*

разним врстама аналитике, Потребни су због једнообразног поступања, Неопходно и преко потребно.У другој сматрају да већ постоје стандарди, али да нису довољно развијени и примењени и у ову категорију спадају одговори попут: *Примена одређених стандарда је комплексна, али се у нашој земљи недовољно користе у односу на развијене државе, У Србији се недовољно користе стандарди у разним врстама аналитике, као што је то у развијеним земљама*. У трећој категорији се налазе неутрални коментари попут *„Немам став“* или *„Било би пожељно да наука понуди могућности и решења у сфери националне безбедности“.*

Када се на описани начин групишу коментари, добијени су следећи резултати: 47,8% одговора испитаника спада у прву категорију, где се истиче потреба за увођењем и развојем стандарда, 39,1% одговора спада у категорију где испитаници сматрају да већ постоје стандарди, али да нису довољно развијени и примењени и 13,1% одговора испитаника су неутрални или уопштени одговори. Резултати су приказани на Графикону 23.

Графикон 23. *Ставови о коришћењу стандарда у различитим врстама аналитике у Србији*

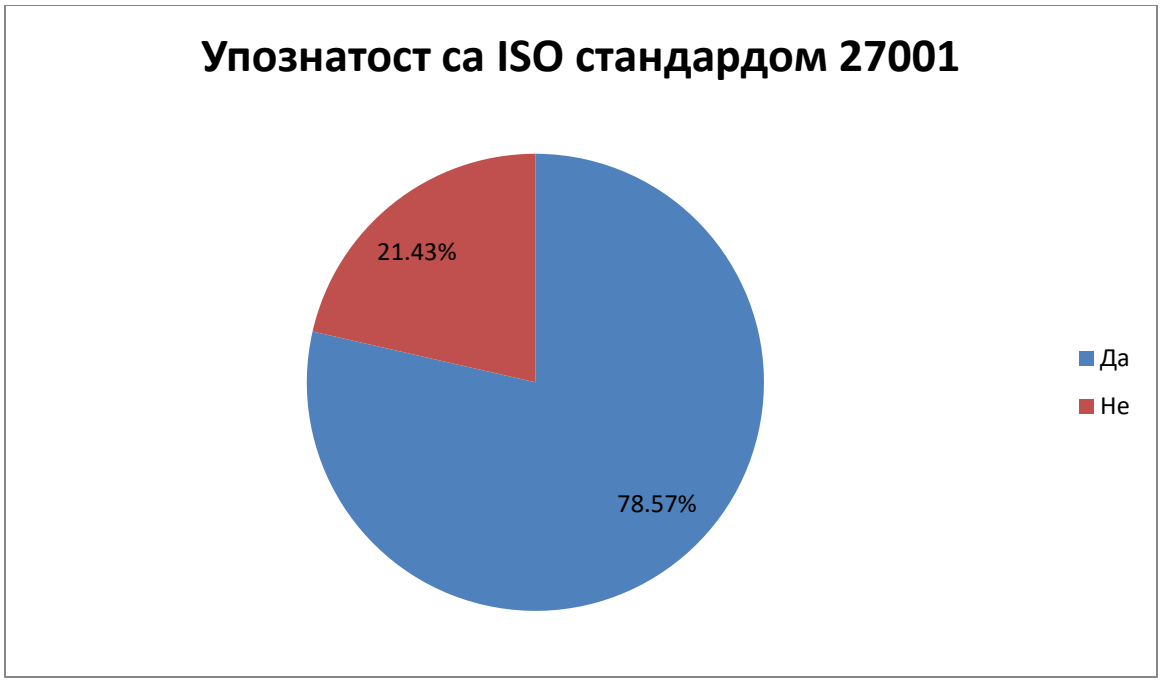
Резултати показују да већина испитаника има изразито позитиван став према потреби успостављања и унапређења стандарда у различитим врстама аналитике у Републици Србији. Највећи број одговора, њих 47,8%, истиче да је стандардизација неопходна ради обезбеђивања јединственог приступа, ефикасности и професионализације аналитичког рада. Испитаници наглашавају значај увођења валидних и униформних стандарда, као и потребу да се они институционално развијају и доследно примењују у свим секторима који се баве аналитиком.

Другу по величини групу, 39.1%, чине одговори који указују на постојање одређених стандарда, али и на проблем њихове недовољне примене и потребу за прилагођавањем савременим изазовима. Испитаници из ове категорије истичу да стандардизација у Србији често зависи од материјалних и техничких услова, да је процес сложен и неуједначен, те да стандарди морају бити динамични и усаглашени са међународним искуствима и безбедносним токовима. Овај став одражава свест о неопходности развоја флексибилног система који ће омогућити примену стандарда без губитка аналитичке креативности и адаптивности.

Мањи број испитаника, њих 13%, нема изграђен став или даје опште напомене, попут потребе за већим укључивањем научне заједнице у развој стандарда у области националне безбедности. Ови одговори могу указивати на делимичан недостатак информисаности или практичног искуства у вези са стандардизацијом аналитичких процеса.

У целини, резултати упућују на закључак да у професионалној заједници постоји јасна свест о значају стандардизације као предуслова за развој савремене аналитике, али и потреба за системским приступом који би обезбедио њихову ефикасну примену и континуирано прилагођавање динамичном безбедносном окружењу.

Наредно питање односи се на конкретан стандард, који је значајан за област безбедносне аналитике и гласи: *Да ли сте упознати са ISO стандардом 27001 – Систем управљања безебедношћу информација? Заокружите одговор.* Резултат је приказан на Графикону 24.



Графикон 24. *Упознатост са ISO стандардом 27001*

На ово питање 78,57% испитаника одговорило је са „да“, а 21,43% са „не“. Већина испитаника, њих 78,57%, изјавила је да је упозната са ISO стандардом 27001, што указује на висок ниво свести о значају система управљања безбедношћу информација у оквиру безбедносне аналитике. Ипак, мањи проценат испитаника, 21,43%, који није упознат са овим стандардом, показује да постоји потреба за додатном едукацијом и усавршавањем стручњака у овој области.

Последње питање из ове категорије је било: *Да ли сте упознати са ГДПР уредбом Европске уније (Општа уредба о заштити података о личности) којој и Србија као кандидат за чланство подлеже? Заокружите одговор*. Резултат је приказан на Графикону 25.

Графикон 25. *Упознатост са ГДПР уредбом ЕУ*

На наведено питање 71,43% испитаника је одговорило са „да“, док је 28,57% испитаника одговорило са „не“. Више од две трећине испитаника, 71,43% је упознато са ГДПР уредбом, што указује на висок ниво свести о заштити личних података међу испитаницима. Ипак, скоро трећина, њих 28,57%, још увек није упозната, што може указивати на потребу за додатним информисањем, посебно у контексту усаглашавања са европским стандардима.

Пре преласка на завршни део истраживања сумирани су досадашњи резултати. Резултати спроведеног истраживања указују на значајну потребу за унапређењем приступа безбедносне аналитике на националном нивоу. Анализа добијених података показује следеће кључне тенденције:

- **Подршка формирању стратешке безбедносне аналитике.** Испитаници су показали висок ниво подршке формирању безбедносне аналитике на националном нивоу и креирању посебног аналитичког центра који би интегрисао различите изворе података и стручности.

- **ПОМ као основа аналитике.** Велики број испитаника сматра да Полицијско-обавештајни модел (ПОМ) може представљати значајну основу за развој ефикасне безбедносне аналитике као јединственог модела.
- **Неопходност у борби против савремених претњи безбедности попут тероризма.** Истраживање показује да је аналитика неопходна за превенцију и реаговање на терористичке претње, као и за правовремено доношење одлука у критичним ситуацијама.
- **Мултидисциплинарни приступ.** Испитаници наглашавају да безбедносна аналитика мора бити мултидисциплинарна, интегришући националну безбедност, организационе процесе, технолошке алате и методе анализе података, како би била свеобухватна и оперативно ефикасна.
- **Потреба за новим моделом.** На основу добијених података, постоји јасна потреба за креирањем новог модела безбедносне аналитике који би интегрисао постојеће стандарде у различитим секторима безбедности, примену мултидисциплинарних приступа и процедура и знања, доприносећи ефикаснијој превенцији претњи безбедности.
-

4) Питања из домена теоријског модела безбедносне аналитике

Фокус и циљ ове групе питања били су да се испита став експерата о теоријском моделу безбедносне аналитике који се предлаже. Стога, експерти су замољени да дају свој коментар на у тексту приказани теоријски модел безбедносне аналитике (Види: Слика 15).

Већина испитаника се слаже са предложеним теоријским моделом безбедносне аналитике, оцењујући га као: „коректан“, „свеобухватан“, „добро осмишљен“, „у складу са актуелним безбедносним изазовима“. Истиче се и да модел почива на теоријским основама Копенхашке школе безбедности, што се сматра научно релевантним и усклађеним са савременим приступима у теорији и пракси.

Део испитаника истиче да постоји потреба за даљом разрадом и операционализацијом, сматра да модел има добро теоријско утемељење, али да је неопходна детаљнија разрада сектора, процедура и стандарда, операционализација концепта ради практичне примене и интеграција аналитичких производа за потребе

доносиоца одлука на стратешком нивоу. Ово указује да се модел види као добра полазна основа са могућношћу даље разраде.

Неколико коментара садржи конкретне предлоге за допуну модела, као што су: *увођење информатичко-кибернетичког сектора, додавање социјеталног аспекта који подразумева заштиту културних, традиционалних и историјских вредности, укључивање методологије друштвених наука у стратешку аналитику, нарочито у области праћења индикатора и друштвених појава.*

Критичка запажања односе се на то да иако је могуће објединити знања и доктрине у теоријском смислу, у пракси је то тешко изводљиво због различитог делокруга рада појединих безбедносних сектора. Ово указује на потенцијалне изазове у примени модела у реалним условима функционисања безбедносног система.

Табела 23. *Груписање резултата коментара предложеног модела*

Група	Опис	Проценат
Општа сагласност и позитивна оцена модела	Испитаници у потпуности подржавају модел без примедаба.	48%
Потреба за даљом разрадом	Испитаници који начелно подржавају модел, али захтевају даљу разраду	22,7%
Предлози за проширење модела	Конкретни предлози за додавање сектора, методологије и слично.	12,7%
Критичка запажања	Указивање на ограничења или тешкоће у практичној имплементацији.	15,6%
Неутрални одговори	Одговори попут „немам коментар“.	1%

Већина, 70,7% експерата, модел оцењује позитивно, било потпуном сагласношћу или начелно уз даљу разраду. Мањи број, 15,6%, има критичке или резервисане ставове, што показује добру прихваћеност уз свест о практичним изазовима и 12% испитаника има своје конструктивне предлоге за измене на предложеном моделу.

Закључно, резултати истраживања потврђују да нови, интегрисани модел безбедносне аналитике може значајно унапредити националну безбедност и ефикасност у реаговању на савремене претње.

2.2 Оцена теоријског модела безбедносне аналитике посебно одабране групе експерата

Испитаници који су обухваћени усмереним интервјуом, како је приказано у претходном тексту, имају завидно практично и, посебно, научно-теоријско знање о безбедносној аналитици. Међутим, и међу врсним познаваоцима предметне области постоје особе које се сматрају експертима.

У том смислу, након обављеног усменог интервјуа, а ради потврђивања опште оцене и конкретизације појединих питања предложеног теоријског модела безбедносне аналитике, одабрана је група од пет експерата. Основни критеријуми за избор групе експерата били су: 1) да поседују теоријско знање и практично искуство из безбедности, посебно у безбедносној аналитици на експертском нивоу, 2) да припадају разним структурама сектора безбедности (а) службе безбедности, (б) војна структура, (в) полиција. У групи експерата су се налазили: 1) проф. др Андреја Савић (службе безбедности), 2) проф. др Бранко Крга (Војска), 3) проф. др Нђо Даниловић (експерт у науци о безбедносној аналитици); 4) доц. др Илија Рацић (полиција); 5) проф. др Божидар Форца (повезаност праксе и теорије безбедности и безбедносне аналитике) и 6) Бранислав Аночић (пензионисани пуковник и експерт из праксе).

Са сваким припадником групе експерата обављен је интервју, усмени разговор. При томе, члановима експертске групе нису саопштени резултати спроведеног усмереног интервјуа. Експерти су дали сагласност за јавно публиковање својих ставова. Ставови сваког припадника групе експерата дају се целовито у даљем тексту.

1) *Проф. др Андреја Савић* у целини подржава креирање предложеног теоријског модела безбедносне аналитике, а конкретни ставови су:

- Домаћа теорија безбедности се доста касно почела развијати. У том смислу, у почетку и примарно су коришћени резулатати научно-теоријских истраживања и радова Копенхашке школе безбедности, посебно професора Бери Бузана.
- У складу с претходним, секторски приступ безбедности Копенхашке школе безбедности може се сматрати научно-теоријским, али и практично прихватљивим. Наравно, развој теорије и праксе у свакој области, па и у области националне безбедности, доноси новине, које је потребно научно превредновати.
- Безбедносна аналитика није целовито заступљена у пракси на националном нивоу, као појам се помиње у теорији. Највећа заслуга за то јесте чињеница да се та аналитика деценијама, па и вековима, одвија релативно сепаратно, пре свега у

војсци, затим у службама безбедности, па у полицији, а касније и у цивилном сектору.

- Предложени теоријски модел сматрам могућим, у свим његовим наведеним деловима: сектори безбедности, процедуре рада аналитичара, стандарди и доктрина. С обзиром на то да су процедуре рада аналитичара и стандарди саставни део досадашњих врста аналитике (обавештајна и криминалистичка), у теоријском смислу посебну пажњу привлачи коректно образложено опредељење ка секторима безбедности и доктрини, као целовитом приступу безбедносној аналитици на националном нивоу.
- У свету, а и у нашој земљи се све више стандардизују процеси и производи, па и аналитика. Примена стандарда треба да буде незаобилазан део модела безбедносне аналитике.

2) *Проф. др Бранко Крга* у целини подржава креирање предложеног теоријског модела безбедносне аналитике, а конкретни ставови су:

- Чињеница је да се ратови, углавном, воде за простор. Отуда, дуго је у теорији и пракси, с правом, кључна, па и једина претња био рат (војна претња). Тако, појам безбедности поистовећиван је с одбраном.
- Савремене теорије безбедности појављују се после Другог светског рата. Паралелно с тим, у пракси, прво у САД (1947), појављује се и документ *Стратегија националне безбедности*, који се крајем прошлог века распростире у већину држава света. Тако, у теорији и пракси долази до проширења и продубљења појма безбедност. Копенхашка школа безбедности је појам проширила у секторе: политички, економски, војни, друштвени и еколошки. Велшка школа је појам безбедности продубила с аспекта државе навише, ка међународној безбедности и наниже, ка људској безбедности.
- Обавештајна делатност рудиментарно настаје у војсци, примарно окренута ка потенцијалном непријатељу (противнику) споља, али не само непријатељу. У каснијем, та делатност добиће назив обавештајна аналитика, која се одвија у оквиру једног процеса именованог као обавештајни циклус. Ти појмови (обавештајна аналитика и обавештајни циклус), у каснијем, пресликаће се и на друге субјекте безбедности, посебно у рад служби безбедности и полиције, а добиће само атрибут сектора у ком се одвијају, при чему је израз обавештајни циклус задржан у свим делатностима. Тако, дошло је до диверзификације аналитике у разним секторима безбедности, али не као обједињене, већ сепаратне. Касније, аспект аналитике прелиће се и у цивилни сектор безбедности. Формално и суштински, различити сектори безбедности нису имали висок степен међусобне сарадње.
- Чињеница је да је данас безбедност недељива, свеобухватна и изложена бројним изазовима, ризицима и претњама. Такође, чињеница је да се у разним секторима безбедности аналитика константно усавршава и достиже запажен ниво

организованости и функционалности. Међутим, само најразвијеније државе света настоје да обједине различите секторе безбеднсти, односно аналитике.

- Предложени теоријски модел безбедносне аналитике ценим као коректан и могућ. С обзиром на то да су процедуре рада познате у разним врстама аналитике, као и развој стандарда у њима, то се кључно питање односи на базу знања о безбедности. Подржавам предложени приступ о бази знања о безбедности, који је заснован на теорији Копенхашке школе безбедности из два основна разлога, 1) реч је о теоријском моделу безбедносне аналитике и 2) резултати Копнехашке школе безбедности су признати у теорији и пракси и, наравно, константно се доградњују.
- Питање развоја организационе јединице за безбедносну аналитику, свакако, јесте умесно. Међутим, за конкретизацију његове организације, начина функционисања, а поготово места у систему националне безбедности, потребна је шира и дубља анализа експерата теорије и праксе. Познат је пример једне суседне државе која је формирала организациону целину под називом Координација у оквиру свог система националне безбедности.
- Стандарди треба да буду обавезан део модела безбедносне аналитике.

3) *Проф. др Нељо Даниловић* у целини подржава предложени модел безбедносне аналитике, а конкретни ставови су му:

- Национална безбедност је безбедност државе и грађана који у њој живе. Безбедност је инкорпорирана у све сфере друштва (политичку, војну, економску, социјалну, културну, технолошку, комуникационо-информатичку и све друге сфере друштвеног живота).
- Приказани сектори безбедности, како их је утврдила Копенхашка школа безбедности су коректно одабрани као знање о безбедности. Става сам да би тим секторима требало додати и *информациони сектор*, како је, иначе, предлагала један од истраживача наведене школе Лене Хансен (Lene Hansen).
- Потребно је успоставити јединствен модел безбедносне аналитике и то без одлагања. Толико је то нужност да не захтева никакво образложење. Данас се цео свет повезује, а ми у Србији доводимо у питање интегрисање база података и њихово коришћење од стране једне јединствене безбедносне аналитике која би требало да буде везана директно за Савет за националну безбедност државе, што не значи да треба укинути Аналитичке службе у појединим сегментима система безбедности.
- Аналитика је служба (делатност), а анализа је метод који користе аналитичари у аналитичким службама. Ова два појма имају различито значење и не могу бити синоними.
- Од ових особина веома су значајне психофизичке особине аналитичара, које подразумевају високу психичку стабилност која треба да буде проверена не само психолошким тестовима, већ и у пракси непосредног деловања безбедносног аналитичара.

Психофизичке особине безбедносног аналитичара, пре свега, подразумевају:

1) висок интелектуални ниво безбедносног аналитичара,

2) добро памћење,
3) да располаже добром концентрацијом, да зна да посматра и да запажа, јер способност доброг запажања и усмерене пажње значи да разликује битно од небитног и да зна шта је предмет његовог посматрања.

Отуда, аналитичари у систему безбедности треба да испуне следеће психофизичке захтеве:

- висок степен образовања из области политике, економије, права, информатике, историје, културе, спорта, војске, полиције, беспрекорно познавање језика и итд.,
- поседовање способности логичког и аналитичког мишљења, интелектуална флексибилност и радозналост, постављање претпоставки и трагање за решењима,
- избегавање једностраности у мишљењу и са тог аспекта израде стереотипних и неупотребљивих анализа и информација;
- поседовање емоционалне стабилности, чврстог морала, стабилног система вредности, вештине комуникације, искуства, позитивне мотивације и способности да успостави три једноставна механизма за успех:
- сређене породичне прилике, решен социјални статус (поседује кућу, стан), где је социјално интегрисан и адаптиран (успешан брак), јер се то одражава на његову активност,
- способност избегавања омнипотентност (поседовање знања о свему) и нарцисоидност, наметање свога мишљења свима, затим уображеност и надменост, калкулантство, брзоплетост, фрустрираност, опсесивну конфузивност, параноју, претеране амбиције, жељу за истицањем и наглашену нелојалност.За безбедносног аналитичара базе података су извор сазнања и закључивања о безбедносним појавама, процесима и догађајима. Оне морају бити доступне и похрањене у најсавременије софтвере са неограниченим могућностима селекције и класификације података ради бржег претраживања. За безбедносног аналитичара важне су интерне интегрисане базе, које воде поједини елементи система безбедности, јавне базе података ОСИНТ (open source intelligence) базе података, научне базе података и посебне, прилагођене софтверске могућности коришћења база вештачке интелигенције, чије резултате треба укрштати са подацима из других база података.
- Успостављени стандарди и етички кодекси у аналитичкој служби мора да постоје и мора да се поштују уз строго законско санкционисање оних појединаца и служби који их крше. Злоупотреба ових аналитичких података доводи до нестабилности, погрешних одлука, а најчешће и сукоба, па и ратова, што се мора спречити. У Србији е стандарде треба транспарентно да утврде експерти, а затим да их усвоје надлежн законодавни и извршних органа власти.
- Предложени *теоријски модел безбедносне аналитике* мора да се у првом реду заснива на општим научним основама аналитике као научне дисциплине, затима на научним основама теорије посебних дисциплина које изучавају посебне аналитике, специфичне само за те научне дисциплине. Аналитичке службе у цивилном, војном, полицијском, социјалном, културном, обавештајно-безбедносном, информатичко-сајбер кибернетском сектору морају полазити од општих научних основа аналитике као уз развијање посебних теориских сазнања за поједине државне делатности где се по дифолту образују аналитичке службе,

без којих нема адекватних података за ваљано доношење одлука и за превентивно безбедносно деловање, нарочито у спречавању свих облика корупције, криминала, тероризма, верске, политичке и сваке друге нетрпељивости, посебно сукоба.

4) *Доц. др Илија Рацић* у целини подржава креирање предложеног теоријског модела безбедносне аналитике, а конкретни ставови су му:

- Изузетно ценим научни покушај да се успостави јединствен модел безбедносне аналитике. Ово, пре свега, из разлога што је безбедност недељива. Такође, методолошки коректним ценим да се овај модел именује као теоријски.
- Принципијелно посматрано, предложени теоријски модел безбедносне аналитике постоји у пракси, али само појединих врста аналитика као, на пример, криминалиситчке (криминалистичко-обавештајне). Основна разлика предложеног теоријског модела безбедносне аналитике и постојећих у пракси њених врста јесте прва група знања. У предложеном теоријском моделу то су знања о безбедности, док се код појединих врста (криминалистичка аналаитика) ради о стратегији, односно бази информација конкретне (криминалистичке) области. Типичан пример за речено јесте ANACAPA модел, који се примењује у пракси криминалистичке аналитике. У складу с наведеним, у пракси постоје значајно развијене базе података конкретне аналитике и утврђене процедуре рада аналитичара, са мање развијеним, али ипак присутним стандардима.
- Дакле, конкретније би требало да се изјасним о првом делу знања, знања о безбедности. С обзиром на то да се ради о безбедности у општем смислу, као и теоријском моделу безбедносне аналитике, сматрам да врло коректно за пример узети ставове Копенхашке школе безбедности из Данске. Наиме, ако би се за овај део узео приступ из домаће теорије, где се говори о компонентама безбедности (унутрашња, спољна и интегрална), опет би се, у крајњем, вратили на секторски приступ безбедности у оквиру наведених компоненти.
- С обзиром на то да долазим из теорије и праксе рада полиције, односно криминалистичке аналитике којом сам се бавио и практично и посебно теоријски (моја докторска дисертација је из те области, као и монографија коју сам касније написао), могу да истакнем следеће: 1) криминалистичка аналитика је имала своје фазе развоја, до значајно уређене области која је у нас утврђена и разрађена у оквиру Полицијско-обавештајног модела. Тај модел, познат под називом Intelligence-led policing, изузетно је развијен у бројним државама света и у Европској унији. Наша земља непосредно учествује у моделу ЕУ, посебно у пројекту SOCTA, 2) Полицијско-обавештајни модел може да послужи као основа (приступ) за развој теоријског модела безбедносне аналитике.
- Базе података у Републици Србији са аспекта националне безбедности су децентрализоване, што чини слабост у начину прикупљања, обраде и анализе података. Сваки сектор безбедности има више база података које, такође унутар једног сектора, нису у потпуности централизоване. На пример, терористички напад у САД у 2001. години се управо и десио услед недостатка централизоване базе података, где је свака служба располагала одређеним обавештајним сазнањима, али која нису били видљива на једном месту (на пример, израђен јединствен обавештајни производ). Наведени догађај је условио декомпозицију постојеће

организационе структуре реструктурирањем и успостављањем централизоване организационе јединице (Фузионог центра) са циљем прикупљања информација у централизовану (обједињену) базу података, којом би се на ефикаснији и ефективнији начин усмеравале криминалистичке истраге и предузимале проактивне мере.

- Покушај да се успостави централизовани систем Р. Србије је успостављање Националног криминалистичкообавештајног система, који представља централизовану платформу за размену података између релевантних државних органа у циљу спречавања и сузбијања свих облика тешког и организованог криминала (погледати детаљније монографију *Полицијско-обавештајни модел у Републици Србији*, Рацић И., 2023). Ово је са аспекта безбедносне аналитике јако битно.
- Рад аналитике у полицији Србије се заснива на примени подзаконских аката (у виду Инструкције и Правилника), чиме се прописују процедура рада, улоге и задаци аналитичара. Такође, аналитичар је неопходно и да примењује Закон о евиденцијама и обради података у области унутрашњих послова. Овим Законом уређује се обрада података о личности у области унутрашњих послова, сврха обраде, права и заштита права лица чији се подаци обрађују, врсте и садржина евиденција, рокови у којима се подаци обрађују, размена података, чување, заштита и контрола заштите података, као и друга питања од значаја за обраду података у области унутрашњих послова.
- Теоријски модел безбедносне аналитике је процес који анализира доступне податке како би проактивно спречио претње. Користи комбинацију прикупљања података, агрегације података и вештачке интелигенције за откривање, идентификацију и одбрану од безбедносних претњи. У свом раду је неопходно да има развијене стандарде и процедуре поступања, укључујући и доктрине/знања аналитичара (мислим да је битно дефинисати како би се звали ти аналитичари, „стратешки аналитичари“ или „безбедносни аналитичари“?. Ко би вршио обуку за такве аналитичаре? Они би по моделу пратили одређене секторе безбедности, што значи да би имали широка овлашћења. Такође је неопходно развити централизовану базу података (НКОС или слично, о чему сам писао). То је јако битно због обраде и анализе затворених база података (под условом да све службе безбедности у оквиру МУП-а, БИА, МО прихвате да податке уносе у ту базу и на тај начин да се могућност аналитичару да може да врши претрагу).
- Модел обухвата секторе: 1) војни сектор обухвата офанзивне и дефанзивне капацитете држава, као и њихове међусобне односе, 2) политички сектор разматра организациону стабилност државе и њеног система власти, 3) економски сектор разматра приступ ресурсима, финансијама и тржиштима; 4. социјетални сектор разматра одрживост језика, културе, религије и осталих елемената националног идентитета и 5) сектор животне средине разматра питања услова средине неопходних за опстанак. Као област проактивног начина рада подела на секторе би била исправна. Међутим, као кључни стратешки документ у раду безбедносне аналитике била би израда стратегије националне безбедности, која би идентификовала кључне приоритете и израдила акциони план за њено спровођење. Такође, служила би као аналитичка јединица Канцеларији савета за националну безбедност и заштиту тајности података ради израде и других аналитичких

производа, а на основу захтева Канцеларије када се идентификују безбедносни ризици по безбедност Републике Србије.

- Стандарди и стандардизација морају да буду обухваћени у моделу безбедносне аналитике.
- Потпуно сам сагласан са предлогом формирања једног тела, које може да се именује као координационално тело безбедносне аналитике. У складу са до сада наведеним, става сам да би то тело требало да буде у оквиру Бироа за координацију рада служби безбедности (Канцеларија).

5) *Проф. др Божидар Форца* у целини подржава креирање предложеног теоријског модела безбедносне аналитике, а конкретни ставови су:

- Теорија безбедности у нас је у рудиментарном развоју, те се претежно користе теоријски приступи западних, а у новије време и тзв. источних (совјетски, руски) извора.
- У практичном, посебно правном смислу, безбедност у нас није утврђена нити уређена као функција државе. Прецизније, Устав Републике Србије (2006) користи израз „одбрана и безбедност“. Та чињеница у каснијем, ближем уређењу одредаба Устава различито се рефлектовала на уређење одбране и безбедности. Тако, одбрана је Законом (Закон о одбрани) експлицитно утврђена као функција државе, која се класификује на војну и цивилну одбрану. С друге стране, безбедност није експлицитно утврђена као функција државе. Тако, тек 2019. године, не у закону (Србија нема закон о националној безбедности), већ у документу Стратегија националне безбедности, по први пут у нашим званичним актима дефинисана је национална безбедност. При томе, референтни објект националне безбедности акцептира се у заштити националних вредности и интереса од свих облика угрожавања. Посебно потенцирам став „од свих облика угрожавања“. Тако, у стратегији је идентификовано 20 изазова, ризика и претњи, који сежу у све секторе безбедности, принципијелно како их је теоријски утврдила Копенхашка школа безбедности.
- Како није експлицитно утврђена као функција државе, тако се безбедност у нас ни теоријски ни практично не разлаже на своје подфункције. У том смислу, у нас преовладава став да је безбедност оно чиме се баве Војска, полиција и службе безбедности.
- Ако се узме у обзир што сам навео о теоријском и практичном (правном) приступу безбедности у нас, чињеница је да се безбедносна аналитика, као појам, појављује само у теорији. У пракси, она је првенствено постојала и даље постоји у Војсци (команде и војне безбедносне службе) као обавештајна аналитика. Касније, та аналитика се појављује и у полицији и службама безбедности, примарно као криминалистичка, односно криминалистичко-обавештајна аналитика. Наравно, и обавештајна и криминалистичка (криминалистичко-обавештајна) аналитика односе се на безбедност, али не као целовиту функцију, већ њене посебне делове. Стога,

поставља се питање да ли је тиме исцрпљена аналитика потребних информација о безбедности?

- Одоговор на наведено питање је јасан – „не“. Безбедност је изузетно сложен појам, јер нису само рат и криминал оно што нас угрожава. Бројни аспекти безбедности нормативно, организационо и функционално нису обухваћени једним општим приступом какав треба да буде безбедносна аналитика. Овде, пре свега, мислим на социјеталну безбедност, обојене револуције (хибридне претње), миграције, тероризам, природне несреће и катастрофе, пандемије и епидемије, енергетску безбедност и друге аспекте.
- У најразвијенијим државама света уназад неколико деценија, и у теорији и у пракси, безбедност се поима целовито, преко свих својих врста. У том смислу, безбедносна аналитика се обједињује на стртешком нивоу у националне (интернационалне) моделе. У томе предњаче САД, што непобитно показује пример Обавештајне заједнице САД, посебно након теористичких напада Ал Каиде на објекте у Њујорку и Вашингтону, 11. септембра 2001. године.
- У дисертацији предложени теоријски модел безбедносне аналитике сматрам методолошки и сазнајно коректно успостављеним. Суштина јесте знање у кључним доменима: 1) безбедност, 2) процедура рада аналитичара и 3) стандарди.
- Приступ знањима из безбедности теоријски, с обзиром на то да се ради о теоријском моделу аналитике, коректно је ослоњен на научно-теоријски приступ Копенхашке школе, као рудимента. Процедуре рада аналитичара су највише истражени, познати и најприхватљивији део модела из праксе. Посебно су значајни стандари у овој области, јер су они незамењиви у свим процесима, па и у моделу безбедносне аналитике. Тако, прихватајући овај теоријски модел, става сам да, након његове верификације, исти треба да се дограђује у теорији и пракси и да резултује једним општим стратешким моделом безбедносне аналитике у нас, који би симболично могао да се назове СрбАн.
- Предложени теоријски модел безбедносне аналитике примарно се односи на стратешки ниво управљања системом националне безбедности у Републици Србији. У том смислу, предлог да се формира посебна организациона јединица безбедносне аналитике, начелно, јесте прихватљив. Уважавајући надлежности у управљању системом националне безбедности, става сам да је ту организациону јединицу могуће уградити у Савет за националну безбедност.
- На крају, очевидно је да се и теорија и пракса безбедносне аналитике у нас морају подићи на виши ниво одређености, уређености, организације и функционисања. За то су нам потребни научно-стручна истраживања и теоријски радови, усвајање закона о националној безбедности (закона о систему националне безбедности) и бројних других подзаконских аката. Стога, теоријски модел безбедносне аналитике, предложен у овој дисертацији сматрам врло значајним делићем напора који стоје пред системом националне безбедности Републике Србије.

6) *Бранислав Аночић* у целини подржава креирање предложеног теоријског модела безбедносне аналитике, а конкретни ставови су:

- Националну безбедност схватам као безбедност нације, где је референтни објект безбедности националне вредности, интереси и циљеви.
- У предлогу теоријског модела безбедносне аналитике, код првог аспекта – знање о безбедности, рекао бих да наведеним секторима (Копенхашка школа безбедности) треба додати и историју, традиције и културу. Међутим, с обзиром на то да се ради о теоријском моделу, предложени сектори безбедности се могу сматрати коректним за модел. По питању остала два дела модела (знања), процедуре рада аналитичара и стандарди, она су позната и неизоставна у пракси, наравно, са различитим степеном развијености у појединим државама.
- Изузетно добро ми је познато да постоје у пракси различите врсте аналитике. Међутим, све оне воде порекло од обавештајне аналитике. Стога, као дугогодишњи (више деценија) обавештајац ја сам за промену вокабулара у смислу да се више користи обавештајна терминологија, по угледу на амерички појам „intelligence“, који има најмање троструко значење. Код нас се своди на појам „безбедност“, а иза и у центру тог појма јесте безбедност државног апарата и личности на власти, док се далеко мање мисли на заштиту и одбрану државе или националних интереса, што се може постићи само офанзивним обавештајним радом. Дакле, мој предлог је да се све то назове „ОБАВЕШТАЈНА АНАЛИТИКА“, а њени елементи би били разни сегменти безбедности. Суштина је да се обавештајном аналитиком долази до кључних информација које се онда користе у заштити појединих националних интереса и остварују циљеви националне безбедности.
- Поред претходно наведеног, а с обзиром на развој теорије и праксе безбедности у нас, а посебно у свету (развијене земље), сматрам изузетно коректним предлог да се све врсте аналитике у држави обједине у један модел безбедносне аналитике. У том смислу, подржавам и формирање једне организационе јединице безбедносне аналитике, у којој би се прикупљале, чувале и размењивале само информације од капиталног (стратегијског) значаја.
-

2.2.1 Дискусија ставова групе експерата

Иако је усмени разговор (интервју) са групом експерата примарно био усмерен на утврђивање њихових ставова о предложеном теоријском моделу безбедносне аналитике, ипак, у њиховим појединачним одговорима обухваћена су и питања из теоријског дела истраживања. У том смислу, од значаја за ово истраживање могу се генерализовати следећи ставови експертске групе:

- Домаћа теорија безбедности није довољно развијена, а у свом развоју примарно се ослањала на западне изворе.

- Безбедносна аналитика не постоји у пракси као целовита, већ се појављује само у теорији, као општи појам за све врсте аналитике. У пракси се испољава у разним подсистемима система националне безбедности, као што су војска, полиција и службе безбедности.
- Сви чланови експертске групе су сагласни да у представљеном теоријском моделу безбедносне аналитике процедуре рада аналитичара и стандарди чине његов део.
- По питању првог дела модела безбедносне аналитике *знање о безбедности,* ставови експертске групе су углавном позитивни и слични, са опрезним додацима који се односе на могућу доградњу секторског приступа Копенхашке школе безбедности.
- Сви припадници експертске групе су става да је могуће, па и пожељно, објединити разне врсте безбедносне аналитике у јединствен модел на стратегијском нивоу, под називом безбедносна аналитика. При томе, пажњу заслужује став Бранислава Аночића (бивши начелник Обавештајне управе Генералштаба и изасланик одбране у Мађарској и САД), који тврди да се обједињена аналитика не именује као безбедносна, већ као обавештајна. Међутим, опет би дошли у спор око форме (обавештајна) и суштине (безбедносна) аналитика.
- Сви чланови експертске групе подржавају формирање јединственог тела за безбедносну аналитику на стратегијском нивоу управљања системом националне безбедности, са различитим виђењима његовог места у систему безбедности. Преовладава став да је место тог организационог тела при Савету за националну безбедност, прецизније у Бироу за координацију рада служби безбедности.
-

2.3 Дискусија резултата емпиријског истраживања – доказивање хипотеза

У претходном тексту, који се односи на емпиријско истраживање, дата је и дискусија одговора испитаника на поједина питања, као и дискусија ставова експертске групе. У оваквим истраживањима прилично је да се, у смислу потврђивања или оповргавања хипотеза, изведе и посебна дискусија резултата емпиријског истраживања. При томе, доказују се посебне хипотезе, а њиховим доказивањем се и генерална хипотеза потврђује.

2.3.1 Доказивање прве посебне хипотезе

Прва посебна хипотеза гласи: *Знања/доктрина о секторима безбедности су део теоријског модела безбедносне аналитике.*

За доказивање прве посебне хипотезе посебно су значајни следећи резултати истраживања:

- Недвосмислено и из више извора је доказано да је безбедносна аналитика знање, процес и организација.
- Знање о безбедности методолошки и сазнајно коректно је везано за секторе безбедности. Секторе безбедности, односно проширење појма безбедности, утврдила је Копенхашка школа безбедности из састава Института за истраживање мира – КОПРИ, из Копенхагена (Данска). Ти сектори прихваћени су у научној теорији безбедности.
- Чињеница је да се у стратешким документима држава света (стратегија националне безбедности) идентификују изазови, ризици и претње. Увидом у најновија издања стратегија националне безбедности бројних држава света, идентификација изазова, ризика и претњи препознаје се по секторима безбедности, како их је утврдила Копенхашка школа безбедности.
- Сектори безбедности обухватају и 1) државоцентрични и друштвеноцентрични приступ безбедности и 2) унутрашњу и спољну, односно интегралну безбедност.
- У истраживању спроведеном усмереним интервјуом већина испитаника, 67,1% је става да су наведени сектори безбедности (Копенхашка школа безбедности) коректно утврђени као знање о безбедности, а тиме и као део теоријског модела безбедносне аналитике.
- Треба истаћи да је део испитаника става да се потпуна информација о стању националне безбедности, поред наведених сектора безбедности, може добити њиховом комбинацијом са компонентама националне безбедности: спољна + унутрашња = интегрална безбедност.
- Сви чланови посебно формиране експертске групе начелно прихватају став да знање о безбедности јесте коректно пресликано од секторског приступа Копенхашке школе безбедности, уз нагласак да се та теорија константно доградњује новим сазнањима.

У складу с наведеним, прва посебна хипотеза се сматра *највећим делом потврђеном.*

2.3.2 Доказивање друге посебне хипотезе

Друга посебна хипотеза истраживања гласи: *Процедуре рада аналитичара су део теоријског модела безбедносне аналитике.*

За доказивање друге посебне хипотезе евидентни су следећи резултати истраживања:

- Из теоријског и описа разних врста аналитике (обавештајна, криминалистичка и друге) у пракси, евидентно је да су процедуре рада аналитичара саставни део свих врста аналитике.

- Сви испитаници усмереног интервјуа, дакле њих 100%, става су да процедуре рада аналитичара јесу неизосатаван део теоријског модела безбедносне аналитике пројектованог у истраживању.
- Сви чланови посебно формиране експертске групе, дакле њих 100%, потврђују став да су процедуре рада аналитичара обавезан део безбедносне аналитике, па и пројектованог теоријског модела.

Дакле, друга хипотеза истраживања је *у потпуности потврђена.*

2.3.3 Доказивање треће посебне хипотезе

Трећа посебна хипотеза гласи: *Стандарди су део теоријског модела безбедносне аналитике.*

За доказивање треће посебне хипотезе евидентни су следећи резултати истраживања:

- Истраживањем је недвосмислено потврђено да постоје бројни међународни (ISO) и домаћи (SRB) стандарди који се односе и на безбедност, у општем смислу, али и у појединим секторима.
- Из теоријског описа разних врста аналитике (обавештајна, криминалистичка и друге) евидентно је да се све више уводе стандарди како у општем смислу који се односи на конкретну врсту аналитике тако и посебно у смислу стандардизације рада аналитичара.
- У емпиријском делу истраживања, примарно код усмереног интервјуа, питање стандарда у моделу безбедносне аналитике рашчлањено ја на два потпитања 1) став о примени стандарда и 2) познавање само неких од постојећих стадарда, као „блиц провера".
- Став о примени стандарад у моделу безбедносне аналитике углавном је позитиван. Испитаници су по овом потпитању давали описне одговоре, који су генерализовани као: 1) истиче се потреба за увођењем и развојем стандарда 47,8%, 2) сматрају да већ постоје стандарди, али да нису довољно развијени и примењени, 39,1% и 3) неутрални коментари 13%. Дакле, може се закључити да је огромна већина, око 87% испитаника, за примену стандарда у моделу безбедносне аналитике.
- У другом потпитању, као „блиц провера" постављено је питање о познавању два стандарда 1) ISO 27001 и 2) ГДПР Уредба ЕУ. Већина испитаника, њих 78,57%, изјавила је да је упозната са ISO стандардом 27001. Такође, већина испитаника, 71,43% је одговорило да је упозната са ГДПР Уредбом ЕУ. Дакле, може се закључити да већина испитаника познаје два наведена стандарда.
- Сви припадници посебно формиране експертске групе (100%) сагласни су применом стандарда у аналитици, односно става су да су стандарди неизоставан део теоријског модела безбедносне аналитике.

У складу с претходно наведеним, трећа посебна хипотеза је *потврђена у потпуности*.

2.4 Провера теоријског модела безбедносне аналитике на примеру супротстављања тероризму

У овом делу истраживачког приступа изградњи теоријског модела безбедносне аналитике приказаћемо базу података за тај модел, коју би развијао и користио Координациони аналитички центар. У складу са општим приступом у истраживању, чија је суштина теоријски модел безбедносне аналитике, тако ће и база података за тај модел бити приказана само у својим основним елелментима пројектовања.

2.4.1 База података за теоријски модела безбедносне аналитике кроз пример супротстављања тероризму

Претпоставке за креирање ове базе су: израда обавештајно-аналитичких производа морада буде централизована и претпоставка да се врши интеграција вишеагенцијских безбедносних података (полиција, одбрана, спољни послови итд.) у јединствену аналитичку инфраструктуру, уз управљање подацима које чува поверљивост. За пример ћемо узети да се база бави обрадом података из домена тероризма (у пракси се то може односити на све претње безбедности државе на стратешком нивоу).

Овај систем је заснован на моделу државне интеграције података. Међутим, циљ није да се постојећи државни органи одрекну контроле над сопственим подацима у корист координационог центра, већ да сваки државни орган система безбедности (нпр. Министарство унутрашњих послова, Министарство одбране, Министарство спољних послова, обавештајне агенције) задржи контролу над својим оперативним подацима, али допринесе стандардизованим, декласификованим или анонимизованим изводима података на централном релационом складишту података.

Ово заједничко складиште података служи као аналитички слој, омогућавајући вишедимензионалну анализу, док истовремено осигурава да осетљиви подаци остану под законским власништвом сваког органа. Тако се, на пример, за потребе планирања неке

антитерористичке акције или прављења стратегија борбе против тероризма могу користити подаци из свих значајних органа и агенција убрзано и аутоматизовано. Дакле, база би омогућила аналитичару да претражује економске, еколошке, војне, полицијске или друге податке значајне за конкретан случај на коме ради уз прескакање слања захтева за размену података и сличних процедура које постоје у пракси. Аналитичар би користио податке који су му потребни у том тренутку, али не би мењао њихову локацију нити би их померао из њихове матичне базе. Такође, тиме би скратио и време анализе. Ово је посебно значајно код тероризма, где се често захтева хитно поступање и балговремена реакција.

Дизајн складишта података се може изградити кроз нормализовану структуру SQL базе података. SQL је језик за базе података који користе сви релациони системи база података (RDBMS). За разлику од других програмских језика, SQL је једини језик за базе података који се рачуна. Његова основа је релациона алгебра, те је то језик заснован на строгом математичком моделу (Петковић, 2025).

Сваки извор података попуњава повезане табеле путем ETL (Extract,transform,load) или ELT (Extract, oad, transform) процеса. Пример структуре шеме са димензијама је следећи:

- Dim_Agency (Agency_ID, Name, Data_Sensitivity_Level)
- Dim_Time (Date, Year, Month, Quarter)
- Dim_Location (Location_ID, Country, Region, City, Geo_Coordinates)
- Fact_Incidents (Incident_ID, Agency_ID, Date_ID, Location_ID, Type, Severity, Casualties, Source_Confidence)
- Fact_Operations (Operation_ID, Agency_ID, Type, Outcome, Risk_Level)
- Fact_Intelligence_Reports (Report_ID, Keywords, Topic, Threat_Score).

База података може бити имплементирана у безбедном локалном или сувереном „клауд“ (cloud) окружењу. „Миграција локалних дата центара се брзо сели у ‚клауд’, остављајући за собом традиционалне моделе рачунарских мрежа, који су више засновани на дизајну основних система. Такве мреже су дефинисане хардверске и софтверске спецификације, којима се управља или би се могло управљати само под једним именом домена или предузећем. У поређењу са имплементацијом рачунарства у ‚клауду’, оне су подложне концепту интернета и софтверски дефинисаним методологијама. Овај модел пружа основу за даљинско управљање, омогућавајући праћење саобраћаја и инжењеринг“ (Stephenson, 2025).

Дакле, коришћењем „клауда“ аналитичар користи податке такорећи на даљину, али их не копира и не премешта из њихових изворних база. Ово потребно окружење може бити интерни владин дата центар који користи неку од платформи, као што су MSSQLS, SQL Server Enterprise / PostgreSQL са безбедношћу на нивоу редова (Row Level Security). „Владе, предузећа и грађани могу развити нове апликације и услуге како би радили са повезаним отвореним владиним подацима (LOGD), анализирали их и разумели“ (Katis et al., 2014).

Коришћење „клауда“ за складиштење безбедносних података већ функционише у пракси. На пример, у западним земљама се као платформе користе Microsoft Azure Government Cloud, AWS GovCloud и NATO Secure Cloud, који користе слојеве података (нпр. Azure Synapse Link, PostgreSQL FDW или Oracle Data Integrator) који се могу повезати са више агенцијских база података без потпуне репликације, чувајући власништво и минимизирајући изложеност података.

Поверљивост и контрола приступа

Безбедност на нивоу реда и колоне у SQL-у осигурава да корисници виде само податке за које су овлашћени. RLS нивои класификације података (нпр. јавни, интерни, поверљиви, ограничени, тајни) одређују политике шифровања и дељења. Шифровање се може обавити коришћењем AES-256 и TLS 1.3 протокола. Такође, овај систем мора имати константну евиденцију ревизије и праћење контроли приступа ради осигурања одговорности. Систем може користити и добро праке заштите података из међународних стандрада, као што је група ISO 27000.

Анонимизација и агрегација података

Пре него што се подаци учитају у аналитичко складиште, лични идентификациони подаци и класификовани идентификатори се хеширају, то јест маскирају, што омогућава да само они чланови који управљају системом могу имати увид у осетљиве податке корисника.

Геопросторне координате могу се агрегирати у административне регионе ради очувања оперативне безбедности, уз коришћење виртуелне приванте мреже (VPN). Осетљиви текстуални документи (обавештајне белешке, дипломатске депеше) се обрађују

путем цевовода (pipeline) за обраду природног језика (NLP), који издвајају теме и индикаторе претњи без откривања сировог текста (Raw data).

Након интеграције, подаци се могу интерно анализирати коришћењем:

- Python / R за статистичко и предиктивно моделирање (нпр. груписање, откривање аномалија, бодовање ризика).
- Power BI / Tableau / Qlik за интерактивне контролне табле и свест о ситуацији или интерни програми за визуелизацију који ће радити на локланим машинама.
- GIS системима (ArcGIS, QGIS) за просторну анализу инцидената и мрежа претњи.

Релациони модел омогућава ефикасно спајање преко димензија: време, географија, државни орган и тип претње, подржавајући и тактичко (на нивоу инцидената) и стратешко (на нивоу трендова) доношење одлука.

Пример: Power BI безбедносна контролна табла (Dashboard).

Коришћење истог принципа дизајна као у примеру америчке безбедносне аналитике:

Инстанца Power BI сервиса може се распоредити унутар интерне мреже владе, директно повезана са SQL складиштем података, где визуелни прикази укључују:

- трендове тероризма и криминала током времена,
- анализу криминала, инцидената и других безбедносних претњи у свету и региону,
- топлотне мапе претњи по региону (heat maps);
- метрике сарадње између агенција и
- ефикасност распоређивања ресурса.

Python скрипте могу се интегрисати унутар Power BI за откривање аномалија или предвиђање трендова коришћењем машинског учења (нпр. ARIMA, Prophet или изолационе шуме).

Ток рада обраде података

Корак 1 – ETL:

Подаци унети из изворних система (у систему САД су то полицијски RMS, војни SIGACT-ови, дневници догађаја MFA) путем безбедних API-ја или групних екстракција. Ово представља основне сирове податке које треба обрадити.

Корак 2 – Припрема и нормализација података:

Извршава се у контролисаном ETL окружењу коришћењем SSIS, Python (pandas) или Apache NiFi и других алата.

Корак 3 – Учитавање у SQL складиште:

Обрађени и валидирани записи се чувају у релационим табелама.

Корак 4 – Слој приступа подацима:

Аналитички алати (Power BI, Jupyter свеске, GIS платформе) упитују путем креденцијала заснованих на корсиницима.

Корак 5 – Континуирана повратна информација:

Аналитички увиди се достављају агенцијама, побољшавајући свест о ситуацији и међуодељењску координацију.

Успостављање интегрисане, релационе платформе података за аналитику безбедности и одбране омогућава владама да трансформишу фрагментиране информације у кохезивну обавештајну слику. Комбиновањем структурираног релационог складиштења, управљања безбедним приступом и модерних аналитичких алата, агенције могу побољшати и стратешко предвиђање и оперативни одзив уз очување поверљивости и суверенитета података.

Такав систем, изграђен на инфраструктури заснованој на SQL-у и проширен Python-ом и Power BI-јем, ствара основу за безбедносну политику засновану на доказима и међуагенцијску сарадњу без угрожавања поверљивих информација.

Овај пример нам приказује да је технички и технолошки могуће успоставити јединствену базу података која се може успоставити на нивоу државе и која може користити безбедносне податке из различитих структура без угрожавања власништва над подацима, а у сврху супротстављања тероризму као претњи безбедности на стратешком нивоу. **Такође, наведено је у складу са директивом Европске уније о јавном сектору за поновну употребу података јавног сектора**[28], чији је циљ да подстакне и подржи јавне управе да усвоје политике отворених података и да омогуће ефикасну интеграцију апликација путем отварања и виртуелизације више владиних извора података, без потребе за редизајнирањем информационих система и/или складиштењем података у централизованим „силосима података“. Истовремено, иницијатива подржава очување аутономије и власништва над оригиналним подацима, што значи да се успоставља повезивање између података са власницима како би и даље имали потпуну контролу над

[28] European Parliament & Council of the European Union (2019). Directive (EU) 2019/1024 on open data and the re-use of public sector information (recast). *Official Journal of the European Union, L 172*, 56–83.

својим оригиналним подацима и апликацијом (који се такође могу сачувати у свом оригиналном облику) (Bizer, 2009).

Приказ описане базе дат је у Прилогу 3.

2.4.2 Доказивање четврте посебне хипотезе истраживања

Четврта посебна хипотеза гласи: *Теоријски модел безбедносне аналитике могуће је проверити на примеру супротстављања тероризму.*

На основу представљеног модела интегрисаног аналитичког система за потребе државне безбедности, показује се да је хипотеза у потпуности доказива. У моделу су дефинисани и оперативно описани сви неопходни технички, организациони и безбедносни услови који омогућавају да се теоријски концепт безбедносне аналитике примени на конкретан домен, односно на анализу и супротстављање терористичким претњама.

У доказивању четврте посебне хипотезе евидентни су следећи резултати истраживања:

1) Прво, модел се заснива на постојећим технологијама релационих база података (SQL), стандардизованој нормализованој структури табела и дефинисаним ETL/ELT процесима за преузимање, трансформацију и уношење података. **Ово показује да концептуални модел није апстрактан, већ технички изводљив у реалном безбедносном окружењу.** Додатно, предложена архитектура обухвата димензије као што су време, локација, институција и тип претње, што омогућава да се терористички инциденти и оперативне активности анализирају на тактичком и стратешком нивоу.

2) Друго, модел јасно демонстрира да се подаци из различитих безбедносних структура полиције, одбране, спољних послова, обавештајних служби и других **могу интегрисати у заједнички аналитички слој без централизације сирових података и без нарушавања власништва над информацијама.** Задржавање контроле над оригиналним подацима од стране сваког органа система безбедности омогућено је применом декласификованих, анонимизованих или агрегираних извода. На овај начин избегава се стварање централног „силоса података“, а истовремено се омогућава да аналитичари приступе релевантним подацима без одлагања и процедуралних препрека.

3) -Треће, употреба „клауд“ технологија, као што су Azure Government Cloud, AWS GovCloud и NATO Secure Cloud, **додатно потврђује изводљивост модела у савременим безбедносним архитектурама**. Ове платформе омогућавају повезивање више извора података путем слојева виртуелизације и федеративних приступа (нпр. Azure Synapse Link, PostgreSQL FDW или Oracle Data Integrator), што значи да се подаци могу користити на даљину, без њиховог премештања из матичних база. Оваква архитектура је посебно погодна за антитерористичке операције, где су брзина приступа и очување поверљивости подједнако важни.

4) Четврто, модел укључује механизме заштите података који су неопходни у раду са поверљивим и класификованим информацијама. Безбедност на нивоу реда и колоне, шифровање (AES-256 и TLS 1.3), контроле приступа и обавезна ревизија приступа гарантују **да аналитичари добијају само оне информације за које имају овлашћење**. Истовремено, применом анонимизације, агрегације геопросторних података и НЛП техника за екстракцију индикатора претњи, омогућено је да се осетљиви текстуални и оперативни подаци обрађују без ризика од откривања сирових података.

5) Пето, модел прихвата коришћење модерних аналитичких алата, као што су Python / R Power BI, GIS системи и интерни системи визуелизације, **чиме се омогућава развој напредних аналитичких производа предиктивних модела, heat мапанализа, откривања аномалија, процена ризика и ситуационих панела**. Овакве алатке су већ стандард у савременим антитерористичким центрима, што додатно доказује да је модел употребљив у пракси.

6) Шесто, предложено решење усклађено је са европским нормативним оквиром, укључујући и Директиву (ЕУ) 2019/1024 о отвореним подацима и поновној употреби података јавног сектора. Ова директива наглашава управо оне принципе на којима почива и предложени модел: виртуелизацију података, задржавање институционалног власништва над изворним подацима и централозацију по потреби. То показује да модел није само технички могућ, већ и правно и организационо одржив. С обзиром на то да је Србија као национални интерес утврдила чланство у ЕУ и у току су приступни преговори, са чијим правним актима

жели и мора да се усклади, јасно је да правни оквир за предложени модел већ има своје основе.

7) Седмо, сличан модел размене података постоји у САД у оквиру Америчке обавештајне заједнице (Intelligence Community – IC) која представља скуп агенција и организација у САД које се баве обавештајним радом, прикупљају, обрађују и размењују обавештајне податке, што смо раније већ описали.

Предложени модел омогућава боље, брже и прецизније одлуке у борби против тероризма јер интегрише податке из више безбедносних структура у јединствени аналитички слој, убрзава приступ информацијама елиминацијом бирократских процедура размене података, уводи аутоматизоване ELT процесе и омогућава примену напредних аналитичких техника, као што су: статистичко моделирање, визуелизација и предиктивна аналитика. Ово смањује време потребно за процену претњи, повећава обим података доступних аналитичарима и значајно унапређује тачност процена и ситуациону свест.

Сумирано, сви представљени елементи (техничка архитектура, процес интеграције података, стандарди безбедности, употреба савремених аналитичких алата и усклађеност са правним оквирима) показују да је предложени теоријски модел могуће успешно применити на анализу терористичких претњи. Због тога се закључује да је четврта посебна хипотеза *потврђена*, јер модел омогућава реалну, практичну и ефикасну примену у домену супротстављања тероризму на стратешком нивоу.

Потврђивањем и четврте посебне хипотезе, доказана је и генерална хипотеза. Највећи број испитаника усмереним интервјуом, 70%, као и сви чланови посебне експертске групе, позитивно су се изјаснили о потреби и могућности креирања теоријског модела безбедносне аналитике.

ЗАКЉУЧАК

Безбедност је предуслов опстанка и развоја човечанства. Тако је записано у научној теорији, али и службеним документима бројних држава света. У пракси, нарочито од постанка савремених држава на простору Европе 16. и 17. века, безбедност се дуго поистовећивала с одбраном државе, односно примарно се односила на војну претњу. Међутим, развој научне теорије безбедности довео је до проширења и продубљења појма безбедност.

За проширење појма безбедност заслужна је Копенхашка школа безбедности (Данска), која је у секторском приступу безбедности, осим војног, утврдила политички, економски, социјетални и еколошки сектор. Уз мање примедбе да наведени сектори нису коначни, тај приступ безбедности прихваћен је у научној теорији, али и при идентификацији изазова, ризика и претњи безбедности у безбедносним стратегијама држава. С друге стране, Велшка школа безбедности је заслужна за продубљење појма безбедности. С нивоа државе (национална безбедност), појам безбедности се продубљује 1) наниже, ка појединцу (људска безбедности) и 2) навише, ка међународној заједници - међународна и глобална безбедност.

Иако је рат остао најдрастичнији облик (претња) безбедности, у теорији и пракси идентификовани су бројни изазови, ризици и претње. Теорија изазове, ризике и претње безбедности, углавном, везује за секторе безбедности, како их је утврдила Копенхашка школа безбедности. У пракси, државе идентификују изазове, ризике и претње безбедности у складу са сопственим аспирацијама и позицијом у међународним односима. Истраживањем је доказано да се у безбедносним стратегијама великог броја држава идентификовани изазови, ризици и претње безбедности, у највећем, поклапају с теоријским одређењима Копенхашке школе безбедности.

С обзиром на то да су државе опстале као кључни субјект међународних односа, то је истраживање предмета и усмерено на националну (безбедност државе и грађана) безбедност. Тако, национална базбедност, осим државе (територијални интегритет и сувереност), обухвата и њене грађане, с једне стране, и неодвојива је од међународне безбедности, с друге стране. У складу с наведеним, питање угрожавања националне безбедности постало је једно од кључних питања државне политике и стратегије. Стога, било је потребно истражити како угрожавању безбедности приступају стране државе и

организације, како би се подаци истраживања поредили са приступом у домаћој теорији и пракси.

Чињеница је да се безбедност, и у страним државама и у Србији, сматра недељивом, у смислу њеног угрожавања, с једне и, одговорности за стање безбедности, с друге стране. Међутим, и поред те чињенице, рудиментарно, спознаја о угрожавању безбедности државе спроводила се сепаратно, по секторима безбеднсти. При томе, примарно су прикупљане обавештајне информације у војсци (оружаним снагама), полицији и службама безбедности, као традиционалним елементима система безбедности. У том смислу, прва је развијена обавештајна делатност у војсци (оружаним снагама), касније именована као обавештајна аналитика. Касније, развија се и аналитика у полицији и службама безбедности, претежно везана за криминал, а именује се као криминалистичка (криминалистичко-обавештајна) аналитика. С друге стране, све снажнији облици угрожавања безбедности у сфери економије, енергетике, природних несрећа и катастрофа, као и пандемија заразних болести, утицали су на развој разних облика аналитике у тим подручјима. Међутим, све аналитике су реализоване сепаратно, одвојено једна од друге.

У последњих неколико година, пре свега у САД и Европској унији, као и државама нашег окружења, након драстичних искустава о угрожености безбедности, безбедносној аналитици се приступа концентрисано. То подразумева синхронизацију разних постојећих аналитика (војна, полицијска, службе безбедности, цивилне структуре) у једну, намењену за стратешки ниво одлучивања. Типичан пример јесте аналитика у Обавештајној заједници САД, Директива ЕУ и Координација у систему националне безбедности Хрватске.

Република Србија је самостална и независна држава од 2006. године. У врло кратком периоду, Србија је донела Устав и друге прописе потребне за уређење свих сфера државе и друштва. У том смислу, Устав Републике Србије је утврдио надлежност Републике да „уређује и обезбеђује одбрану и безбедност Републике Србије и њених грађана“. Дакле, употребљена је синтагма „одбрана и безбедност“, као рецидив прошлог времена. Та чињеница имала је за последицу врло изражене разлике у начину уређења „одбране“ и „безбедности“ Србије. Тако, одбрана Србије, након Устава, уређена је законима, стратегијама и другим подзаконским актима, а експлицитно је утврђена као функција државе. С друге стране, у сфери безбедности, након Устава, Србија нема закон о

безбедности, те је највиши акт Стратегија националне безбедности. Такође, први пут је национална безбедност у Србији у једном званичном документу државе дефинисана тек 2019. године. При томе, безбедност Србије није експлицитно утврђена као функција државе, као што је то случај с одбраном. Дакле, безбедност је остала делом недефинисана и недовољно уређена област.

Иако је Србија, у Стратегији националне безбедности, идентификовала изазове, ризике и претње безбедности слично као и друге државе Европе и света, ипак, обавештавање о појавама угрожавања безбедности одвија се сепаратно. Принципијелно посматрано, примарно се развијају обавештајна и криминалистичка аналитика. Наравно, анализи се подвргавају и други облици угрожавања, али не као утврђени обавештајни организациони облици, већ у склопу разних државних тела (савети, кризни штабови…).

Србија је успоставила систем националне безбедности, који има управљачки и извршни део. Управљачки део чине: Народна скупштина, председник Републике, Влада и Савет за националну безбедност. Законима и другим актима прописане су надлежности наведених управљачких органа. Међутим, ниједним прописом у Србији није утврђено ко информише стратешки ниво управљања системом безбедности Србије о угрожавању безбедности као целовитој појави. Чињеница је да постоје органи обавештајне и криминалистичке аналитике, а да се анализе других претњи спроводе од појаве до појаве.

Теорија и пракса безбедности у страним државама, поготово по питању угрожавања безбедности, иницирале су истраживање за потребе ове докторске дисертације. Полазна идеја и основни циљ истраживања било је креирање теоријског модела безбедносне аналитике, који се проверава на примеру супротстављања тероризму. Јединствени теоријски модел подразумева обједињавање постојећих модела аналитике и оних које треба развити у систему националне безбедности. Модел је окарактерисан као теоријски, јер је то први пут у нашој теорији и пракси да се приступа проблему на овакав начи, те да се његовим прихватањем могу створити претпоставке за доградњу и примену у пракси. Модел је провераван на супротстављању териризму пошто је тероризам и даље једна од највећих претњи безбедности и држава и међународног мира и стабилности. У складу с наведеним, методолошки и сазнајно оправдано, истраживање је имало теоријску и емпиријску форму.

Свако научно истраживање даје свој допринос двема кључним фунцијама науке 1) да потврди праксу, односно њене ставове превреднује и уврсти у начни фонд и 2) да да нови научни допринос за теорију и праксу.

На основу извршене теоријске анализе, разматрања нормативног оквира, упоредне праксе и резултата спроведеног емпиријског истраживања, може се потврдити свеобухватан научни закључак о значају, неопходности и могућностима развоја безбедносне аналитике у Републици Србији.

Пре свега, утврђено је да аналитика, као интелектуална, организована и сврсисходна делатност, у савременом друштву добија пажњу примарног инструмента за разумевање актуелних процеса, што посебно долази до изражаја у области безбедности. Савремени безбедносни изазови, ризици и претње од националних, преко регионалних до глобалних, захтевају интегрисан аналитички приступ који обједињује различите изворе података, методолошке приступе и институционалне надлежности. Безбедносна аналитика, дефинисана као посебна врста аналитике која је усмерена на стицање истинитих и употребљивих сазнања о безбедносним појавама, показује се као неопходан ресурс за функционисање система безбедности у целини.

Анализа нормативног оквира и постојећих организационих решења у Србији указује на структуралне недостатке, као што су: нејасно нормативно дефинисање функције безбедности, фрагментација аналитичких процеса у оквиру различитих сектора, раздвојеност обавештајне и криминалистичке аналитике и изостанак јединственог стандардизованог аналитичког модела на националном нивоу. Док поједини процеси, попут Полицијско-обавештајног модела (ПОМ), представљају значајан напредак, укупни аналитички потенцијал није интегрисан, што онемогућава формирање кохерентне стратегијске безбедносне слике.

Упоредна анализа са моделима развијеним у државама с дугом традицијом интегрисаног обавештајног рада, као што је америчка обавештајна заједница, показује да ефикасна безбедносна аналитика почива на координацији, протоку података, стандардизованим процедурама и мултисекторској сарадњи. Ови принципи представљају референтни оквир и за развој националног модела у Србији.

Истраживање спроведено међу домаћим експертима потврђује висок степен подршке формирању институционализоване стратегијске безбедносне аналитике, као и потребу за

оснивањем централизованог аналитичког језгра које би интегрисало податке, методологије и експертизе различитих сектора безбедности. Испитаници са великим знањем и искуством су потврдили да је постојећи теоријски модел безбедносне аналитике добро утемељен, заснован на релевантним теоријским приступима и усклађен са савременим безбедносним потребама. Истовремено, наглашена је потреба за његовом операционализацијом и разрадом процедура, стандарда, сектора и интеграцијом аналитичких производа у процес доношења стратешких одлука.

Генерална хипотеза да теоријски модел безбедносне аналитике садржи доктрину (потребна знања о секторима безбедности), процедуре рада аналитичара и стандарде у овој области, те да се његова функционалност може јасно приказати на примеру супротстављања тероризму у потпуности је доказана. Она је потврђена кроз доказивање свих посебних хипотеза.

Посебно је важно истаћи да је, кроз анализу борбе против тероризма као комплексне и динамичне безбедносне претње, евидентно да теоријски модел безбедносне аналитике омогућава значајно унапређење процеса процене ризика, раног упозоравања и спречавања терористичких активности. Комбинација техничке архитектуре, процеса интеграције података, напредних аналитичких алата и усклађености са правним стандардима омогућава брже, прецизније и поузданије одлуке. Због тога је четврта хипотеза у потпуности потврђена: предложени модел може се практично и ефикасно применити у домену супротстављања тероризму и другим сложеним безбедносним претњама.

Република Србија, по површини територије и броју становника, спада у ред малих држава. Међутим, њену безбедност угрожавају бројни изазови, ризици и претње, који се ретко појављују самостално, већ делују као својеврсни облик интегралне кризе, односно кризе чији су узроци човек и природа. Стога, стратегијски ниво управљања системом националне безбедности мора располагати инофрмацијама о угрожавању безбедности у реалном времену. У том смислу, сепаратни облици аналитике у сфери безбедности треба да се интегришу у јединствен модел.

Развој интегрисаног теоријског модела безбедносне аналитике представља неопходан и остварив корак за унапређење управљања националним системом безбедности Републике Србије. Модел је теоријски утемељен, практично применљив и подржала га је стручна јавнос, а његова имплементација омогућила би стандардизован,

мултидисциплинарни, технолошки заснован и институционално координисан приступ анализи безбедносних претњи. Такав приступ значајно би повећао ефикасност у борби против савремених безбедносних ризика, нарочито тероризма и допринео формирању јединствене стратегијске безбедносне свести на националном нивоу.

У том смислу, резултати истраживања снажно указују на потребу за системском реформом и институционализацијом безбедносне аналитике као једне од кључних полуга националне безбедности у 21. веку.

Свако научно истраживање, које се званично прихвати, које потврди постављене хипотезе, отвара простор за његову доградњу, с једне, и примену у пракси, с друге стране. Ово истраживање, недвосмислено, потврдило је општу хипотезу о потреби и могућности креирања теоријског модела безбедносне аналитике. С друге стране, у раду је приказан теоријски модел безбедносне аналитике, дакле, приказ на општем нивоу, без конкретних решења. У том смислу, ово истраживање указује и на потребу нових научних истраживања. Принципијелно посматрано, даља научна истраживања требало би усмерити на сегменте који чине теоријски модел у овом истраживању, а што подразумева:

- научно превредновање савремених изазова, ризика и претњи безбедности,
- утврђивање јединственог модела процедура безбедносних аналитичара, са утврђеним скупом метода и техника које се примењују у развијеним државама, свакако подржаних савременом информационом технологијом,
- стандардизацију процеса безбедносне аналитике и
- дефинисање доктрине домаћег приступа јединственом моделу безбедносне аналитике, који би могао да се назове *Српски модел аналитике – СрбАн.*

Све то, у даљем, треба да се провери у пракси, за шта су полазишта: 1) да се донесе *закон о националној безбедности* (или *закон о систему националне безбедности*), те 2) да се безбедност експлицитно утврди и уреди као функција државе.

ЛИТЕРАТУРА

1. Achankeng, S. (2025). Analysis of prevention techniques against DDoS and SQL injection attack in network and cloud environment. *Journal of Cloud Computing*.
2. AJP-2.1 (2002). *Intelligence Procedures*. Brussels: NATO, pp. 2–13.
3. Алиспахић, Б. (2011).*Основи методике рада обавештајно-сигурносних служби*. Сарајево, Загреб: БТЦ Шахинпашић.
4. Allied Joint Intelligence (2003). *Counterintelligence and Security Doctrine*, AJP-2.
5. Anderson, B. (1991). *Imagined communities: reflections on the origin and spread of nationalism*. London: Verso.
6. Andrić, J., & Terzić, M. (2023). Intelligence cycle in the fight against terrorism with usage of OSINT data. *Journal of Information Systems & Operations Management, 17*(1), 1–17.
7. Андрић, Ј. и Ковач, М. (2021). Савремени тероризам као претња безбедности. *Безбедност, 63*(2), 107–121.
8. Andrić, J., & Tišma, M. (2022). New models of security analytics. *International Journal of Economics and Law, 11*(33), 26–40.
9. Арежина, В. (2010). *Проблем мерења еколошке безбедности*. Београд: МСТ Гајић.
10. Azinović, V. (2018). Regional report: Understanding violent extremism in the Western Balkans. *Extremism Research Forum*, 2–18..
11. Бајагић, М. (2010). Криминалистичко-обавештајне активности. *Ревија за криминологију и кривично право,* (3), 193–212.
12. Бајагић, М. (2015). *Методика обавештајног рада*. Земун: Криминалистичко-полицијска академија.
13. Балтазаревић, Р. и Балтазаревић, А. (2023). Тероризам у дигиталном окружењу. *Баштина*, *33*(60), 173–181.
14. Бановић, Б. (2001). *Криминалистичка методика*. Земун: ВШУП.
15. Barnett, J. (2001). *The meaning of environmental security: ecological politics and policy in the new security era*. London: Zed Books.
16. Биланџић, М. (2008). *Пословно-обавјештајно дјеловање: Business intelligence* у *пракси*. Загреб: АГМ.
17. Bizer, C. (2009). The emerging web of linked data. *IEEE Intelligent Systems*, *24*(5), 87–92.
18. Благојевић, С. (2019). Социјални инжењеринг и лични подаци. *FBIM Transactions*, *7*(1), 20–28.
19. Благојевић С., Зоговић М. и Пајовић М. (2015), Политика односа са јавношћу у систему одбране, *Војно дело, 67*(5), 133–145.
20. Богати, Ј. и Вук, Д. (2012). ИДЕФ методологија моделирања информацијских сустава. *Практични менаџмент, III*(4), 93–99.

21. Бошковић, М. (1998). *Криминалистичка методика I* (2, допуњено издање). Београд: Полицијска академија.
22. Бошковић, М. В. (1996). Аналитика у савременим обавештајно-безбедносним системима. *Војно дело, 48*(3), 119–134.
23. Bundesministerium der Verteidigung (2006). *White paper 2006 on German security policy and the future of the Bundeswehr,* 18–20. Berlin: Author.
24. Buzan, B. (1983). *People, states and fear: the national security problem in international relations.* Chapel Hill: The University of North Carolina Press.
25. Buzan, B. (1991). *People, states and fear: an agenda for international security studies in the post-cold war era*. London: Harvester Wheatsheaf.
26. Buzan, B., Wæver, O., & De Wilde, J. (1988). *Security: a new framework for analysis*. London: Linne Rienner Publishers.
27. Carter, D. (2009). *Law enforcement intelligence: a guide for state, local, and tribal law enforcement agencies*. U.S. Department of Justice.
28. Carter, J., & Carter, D. (2009). Law enforcement intelligence: implications for self-radicalized terrorism. *Police Practice and Research, 13*(2), 138–154.
29. Carter, J. G., & Phillips, S. W. (2015). Intelligence-led policing and forces of organisational change in the USA. *Policing and Society, 25*(4), 333–357. https://doi.org/10.1080/10439463.2013.865738
30. Central Intelligence Agency (n.d.). *Center for the Study of Intelligence*. Retrieved January 15, 2024 From https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html
31. Chalecki, E. L. (2002). *Environment and security.* Oakland: Pacific Institute for Studies in Development.
32. CNN, from https://www.cna.org/, 20. 6. 2025
33. Collier, M. W. (2005). A pragmatic approach to developing intelligence analysts. *Defence. Intelligence Journal, 14*(2), 30–31.
34. Corkill, J. D., Cunow, T. K., Ashton, E., & East, A. (2015). *Attributes of an analyst: What we can learn from the intelligence analysts job description*, from https://doi.org/10.4225/75/57a83ad2d2cf7
35. Council of the European Union (2010). *Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime.* 3043rd Justice and Home Affairs Council meeting, Brussels, November 8–9.
36. Цветковић, В., Милојковић, Б. и Стојковић, Д. (2014). Анализа геопросторне и временске дистрибуције земљотреса као природних катастрофа, *Војно дело, 66*(2), 166–185.
37. Dach, Z. (2009). *Globalizacja – wyzwania i zagrożenia. In Z. Dach (Ed*.), Polska wobec procesów globalizacji (13–29). Kraków: Polskie Towarzystwo Ekonomiczne.
38. Даниловић, Н. и Милосављевић, С. (2008*). Основе безбедносне аналитике*. Београд: Службени гласник.
39. Даниловић, Н., Милосављевић, С., Манојловић, Д., Милутиновић, О. и Јовић, В., (2018). *Безбедносна аналитика*. Београд: Беосинг.
40. Danilović, N., Manojlović, D., & Gajić, D. (2023). Scientific basis of criminalistic, analytical – operational knowledge. *Social Communications: Theory and Practice, 15*(2), 118–132.

41. Даниловић, Н., Манојловић, Д., (2024), *Аналитичка истраживања у безбедности*. Beograd: Универзитет МБ.
42. Дашић, Б., Дашић, Д. и Тркља, Р. (2017). Међународна оријентација пословања као чинилац економске стабилности и националне безбедности. *Војно дело*, (2/2017), 311–321.
43. Deflem, M. (2024). The declining significance of Interpol: Policing international terrorism after 9/11. *International Criminal Justice Review, 34*(1), 5–19.
44. Deutsche Welle (2024, June 20). Светски дан избеглица: расељавање достиже нови максимум: https://www.dw.com/sr/svetski-dan-izbeglica-raseljavanje-dosti%C5%BEe-novi-maksimum/a-69418850 (29. 11. 2024)
45. Dictionary.com. (n.d.). *Intelligence*. Retrieved January 15, 2024, from http://www.dictionary.com/browse/intelligence
46. Dillerup, R. & Stoi, R. (2006*). Basic management*. Vahlen.
47. Добовшек, Б. и Јунг, Е. (2013). *Супротстављање савременом организованом криминалу и тероризму.* Љубљана: Факултет за друштвене науке.
48. Đorđević, I., & Keković, Z. (2023*).* The impact of international standards on the quality of people's life. *International Journal for Quality Research, 17*(4), 1025–1040.
49. Драгишић, З. и Радојевић, К. (2014). *Безбедносни менаџмент*. Београд: Факултет безбедности.
50. Дворшек, А. (н.д.). *Криминалистички обавештајни рад и његове перспективе у криминалистици*. Марибор: Факултет за варностне веде, Универза в Марибору.
51. Ђурђевић, З. и Милић, Н. (2020). Значај аналитичке подршке у супротстављању савременим облицима криминалитета у условима европских интеграција. *Безбедност, 62*(1), 84–101.
52. Ђурђевић, З. и Радовић, Н. (2012). *Криминалистичка оператива*. Београд: Криминалистичко-полицијска академија.
53. Ђурђевић, З. и Радовић, Н. (2017). *Криминалистичка оператива* (2. изд.). Београд: Криминалистичко-полицијска академија.
54. Ејдус, Ф. (2024). *Међународна безбедност: теорије, сектори, нивои*. Београд: Факултет политичких наука.
55. Ericson, R. V., & Haggerty, K. D. (1997). *Policing the risk society*. Toronto: University of Toronto Press.
56. European Parliament & Council of the European Union (2019). Directive (EU) 2019/1024 on open data and the re-use of public sector information (recast). *Official Journal of the European Union, L 172*, 56–83.
57. Европски покрет у Србији (2011). *Слобода, безбедност, правда*. Београд: Европски покрет у Србији.
58. Филозофија ГСМ (2019). Обим и садржај сазнања у процесу безбедносне аналитике. https://filozofijagsm.files.wordpress.com/2019/09/obim-i-sadrzaj-1.pdf (12. 1. 2024)
59. Фатић, А. (2009). *Прислушкивањем до безбедности*. *Ревија за безбедност*, (1), 5–18.
60. Форца, Б. (2003), *Војни фактор међународних односа и његов утицај на развој Војске Југославије*. Докторска дисертација. Београд: Војна академија.

61. Форца, Б. (2022). *Савремене теорије безбедности*. Факултет за пословне студије и право.

62. Форца, Б. (2014). Условљеност изградње оперативних способности од развоја доктрине Војске Србије. *Војно дело, 66*(1), 210–223.
63. Форца, Б. (2017). Од стратегије до стратегологије. У *Зборник радова са националног научног скупа „Савремени проблеми стратегије и стратегијског менаџмента“*. Факултет за пословне студије и право.
64. Форца, Б. (2021). *Системи безбедности* (2. изд.). Београд: Факултет за пословне студије и право.
65. Форца, Б. (2022а). *Теоријски допринос утврђивању функција система националне безбедности Републике Србије*. Београд: Факултет за пословне студије и право.
66. Форца, Б. (2022б). *Теоријски и упоредни аспект анализе стратегије националне безбедности Републике Србије*. Београд: Факултет за пословне студије и право.
67. Форца, Б. (2024). *Европски безбедносни чвор*. У *Тематски зборник „Европа на раскрсници – безбедносна аналитика“*. Београд: Факултет за пословне студије и право.
68. Форца, Б. и Аночић, Б. (2018). *Безбедносна аналитика*. Београд: Факултет за пословне студије и право.
69. Форца, Б. и Жупац, Г. (2025), *Кризни менаџмент у систему безбедности*. Београд: Факултет за пословне студије и право.
70. Форца, Б., Крстић, С. и Станковић, В. (2023). *Заједничка спољна и безбедносна политика Европске уније и Република Србија*. Београд: Факултет за пословне студије и право.
71. Fuentes, J. R. (2006). *Practical guide to intelligence-led policing*. New York: Center for policing terrorism at the Manhattan Institute.
72. Гаћиновић, Р. (2005). *Антитероризам*. Београд: Драспар партнер.
73. Geneva Centre for Democratic Control of Armed Forces (2006). *DCAF backgrounder: Obavještajne službe*. Geneva: Geneva Centre for Democratic Control of Armed Forces.
74. Gottlieb, S., Arenberg, S., & Singh, R. (1994). *Crime analysis: from first report to final arrest.* Montclair: Alpha Publishing.
75. Гудовић, А. (2019). *Миграције становништва као изазов, ризик и претња безбедности.* Београд: Факултет за пословне студије и право.
76. Хампсон, Ф. О. (2012). *Људска безбедност*. У Д. П. Вилијамс (Ур.), *Увод у студије безбедности*. Службени гласник.
77. Хармон, Ц. (2002). *Тероризам данас*. Голден маркетинг.
78. H-Alter, *ЕУ: кохезија и депопулација* са https: //h-alter.org/europa/eu-kohezija-i-depopulacija/ (29. 11. 2024).
79. Хемлин, Д. В. (2001). *Теорија сазнања* (М. Анђелковић, Прев.). Никшић: Јасен.
80. Heuer, R. J., Jr., & Pherson, R. H. (2015). *Structured analytic techniques for intelligence analysis.* Washgton, DC: CQ Press.
81. Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies.
82. Homeland Security Digital Library (HSDL). *Collections and resources.* https://www.hsdl.org/c/ (2. 9. 2024)
83. Hough, P. (2004). *Understanding global security*. New York: Routledge.

84. Hughbank, R., & Githens, D. (2010). Intelligence and Its Role in Protecting Against Terrorism. *Journal of Strategic Security, 3*(1), 31–38.
85. Иветић, М. (2017). Рад полиције у заједници између стратегије и основне полицијске обуке у Србији. *Безбедност, 59*(2), 130–152.
86. Institute for Economics and Peace (2024). *Global Terrorism Index*. Vision of Humanity. Dostupno na: https://www.visionofhumanity.org/maps/global-terrorism-index/#/ (29. 1. 2025)
87. Институт за савремену историју (б. г.). *Пројекат ИСС 104420*. Доступно на: https://iss.rs/sr_Cyrl/project/show/iss:proj:104420, (29. 11. 2024)
88. INTERPOL (n.d.). Databases. Dostupno na: https://www.interpol.int/en/How-we-work/Databases (29. 1. 2025)
89. ISME (n.d.). *Project ISO 65037*. From: https://isme.me/sr_ME/project/show/iso:proj:65037 (6. 12. 2024)
90. ISO (n.d.). *Committee 54808*. https://www.iso.org/committee/54808.html (4. 12. 2014)
91. ISO standardi (n.d.). ISO *22301*. https://iso-standardi.rs/standardi/iso-22301/ (4. 12. 2024)
92. ISS (n.d.). *Project ISS 59127*. https://iss.rs/sr_Cyrl/project/show/iss:proj:59127 (6. 12. 2024)
93. ISS (n.d.). *Project ISS 59131*. https://iss.rs/sr_Cyrl/project/show/iss:proj:59131 (4. 12. 2024)
94. JP 2-01 (2012). *Joint and national intelligence support to military operations*. U.S. Department of Defense.
95. JSTOR. *Digital library of academic journals*. https://www.jstor.org/ (2. 9. 2024).
96. Кековић, З. (2011). *Системи безбедности.* Београд: Факултет безбедности.
97. Kelling, G. L., & Bratton, W. J. (2006*).* Policing terrorism. *Civic Bulletin*, (43), 1–8.
98. Копал, Р., Бартош, В. и Бринцика, Ж. (2003). *Увод у криминалистичку обавештајну аналитику.* Загреб: Министарство унутарњих послова Републике Хрватске.
99. Kotis, K., Athanasakis, I., & Vouros, G. (2014). *Semantic integration & single-site opening of multiple governmental data sources*. arXiv. https://arxiv.org/abs/1407.0481
100. Ковач, М. (2001). Теоријске основе израде доктринарних докумената. *Војно дело*, *53*(1), 5–21.
101. Краљ, Р. (2019). *Криминалистичко-обавештајна делатност*. Универзитет у Ријеци.
102. Kremlin (n.d.). *Dokument o događajima*. http://static.kremlin.ru/media/events/files/ru/QZw6hSk5z9gWq0plD1ZzmR5cER0g5tZC.pdf (9. 1. 2024)
103. Кривокапић, В. (2012). Тероризам као облик организованог криминалитета и мере супротстављања. *Безбедност, 5*(2), 52–69.
104. Крстић, О. (2003). *Прогностика криминалитета*. Београд: Полицијска академија.
105. Крштенић, А. и Матијашевић, М. (2014). Проблеми обавештајних служби у процесу прилагођавања савременим изазовима, ризицима и претњама. *Војно дело, 66*(1), 105-125.
106. Куљић, Ђ. (2018). Унутрашња безбедност ЕУ и савремена мигрантско-избегличка криза. *Политичка ревија*, *56*(2), 119–132.

107. Кузмановић, Б. и Благојевић, С. (2021). Значај политичке димензије оружане побуне на примеру Северне Ирске. *Безбедност, 63*(3), 97–112.
108. Лазаревић, И. (2015). *Биг дата у медицини и фармацији*. ББ-ИНФОРМАТОР, (242), 15–18.
109. Lippmann, W. (1943). U.S. foreign policy. *The Hispanic American Historical Review, 23*(4), 664-667.
110. Lukić, R. (1979). *Politička teorija države*, Zavod za udžbenike i nastavna sredstva.
111. Maguire, M. & John, T. (2006). Intelligence-led policing, managerialism and community engagement: Competing priorities and the role of the National Intelligence Model in the UK. *Policing and Society, 16*(1), 67–85.
112. Мак, А. (2023). *Специфичности обавештајно-безбедносне функције политичког система Републике Србије*. Докторска дисертација. Београд: Војна академија.
113. Мандић, Г. (2012). *Основи система обезбеђења правних лица*. Београд: Факултет безбедности.
114. Манојловић, Д. (2008). *Криминалистичка аналитика*. Београду: Факултет безбедности.
115. Маринковић, Д. и Ђурђевић, З. (2013). *Криминалистички аспекти супротстављању тероризму.* Криминалистичко-полицијска академија.
116. Маринковић, Д. и Тасић, М. (2023). О симулованим истражним радњама у криминалистици. *Безбедност, 65*(1), 43–63.
117. Марковић, С. (2019). Стратешко одлучивање у полицији и примена полицијско-обавештајног модела. *Безбедност, 61*(3), 160–178.
118. Машуловић, И., Савић, А. и Чрнчец, Д. (2016). *Евроатлантске интеграције система безбједности.* Подгорица: Универзитет Доња Горица.
119. Матић, Г. и Милошевић, М. (2006). Концепти и стратегије борбе против тероризма. *Наука, безбедност, полиција, 12*(1), 31–50.
120. Матијашевић-Обрадовић, Ј. и Обрадовић, А. (2014). Угрожавање безбедности савременог друштва у светлу угрожавања еколошке безбедности. *Култура полиса, 11*(23), 259–276.
121. McDonald, M. (2012). Ekološka bezbednost. U P. Vilijams (Ur.), *Uvod u studije bezbednosti*. Beograd: Službeni glasnik.
122. McGarrell, E. F., Freilich, J. D., & Chermak, S. (2007). Intelligence-led policing as a framework for responding to terrorism. *Journal of Contemporary Criminal Justice, 23*(2), 142–158.
123. Михаљишин, М. (2010). *Моделирање и симулација: Систем за управљање базом података – Увод* (Приручник за интерну употребу). Доступно на: https://razno.sveznadar.info/10-doc-PDF/T1_2_modeli_UvodBP.pdf (28. 11. 2024)
124. Мијалковић, С. (2010а). Обавештајне структуре терористичких и криминалних организација. *Наука, безбедност, полиција 15*(2), 101–114.
125. Мијалковић, С. (2010б). Унутрашња безбедност Републике Србије у условима европских интеграција. У *Безбедносни и одбрамбени аспекти прикључења Републике Србије Европској унији*. Институт за стратешка истраживања; Мисија ОЕБС у Србији.

126. Mijalković, S., & Arežina, V. (2024). Qualitative, quantitative and mixed methods in researching security and political phenomena. *Bezbednost, 66*(3), 23–40.
127. Милашиновић, Р. и Мијалковић, С. (2005). *Тероризам као савремена безбедносна претња*. Криминалистичко-полицијска академија.
128. Милићевић, М. (2014). *Експертско оцењивање*. Београд: Медија центар „Одбрана“.
129. Милисављевић, Б. (2019). Место и улога војних аташеа у позитивном дипломатском праву. *Безбедност, 61*(2), 12–27.
130. Милојевић М. и Милојковић, С. (2009). *Основи полицијске тактике*. Београд: Криминалистичко-полицијска академија.
131. Милосављевић, Б. (2019). *Безбедносна процена као чинилац стратегије националне безбедности Републике Србије*. Докторски рад. Београд: Факултет безбедности.
132. Милосављевић, С. (1980). *Истраживање политичких појава*. Институт за политичке студије.
133. Милосављевић, С. и Радосављевић, И. (1975). *Репетиторијум из методологије друштвених истраживања*. Институт за политичке студије. ФПН.
134. Миљевић, М. (2007). *Методологија научног рада*. Источно Сарајево: Филозофски факултет Универзитета у Источном Сарајеву.
135. Министарство безбједности Босне и Херцеговине (2010). *Рад полиције у заједници: Приручник.* Сарајево: ЦПУ.

Министарство спољних послова Републике Србије. (б. г.). *Заједничка безбедносна и одбрамбена политика ЕУ*. https://www.mfa.gov.rs/spoljna-politika/bezbednosna-politika/zajednicka-bezbednosna-i-odbrambena-politika-eu (9. 1. 2024)

136. Министарство унутрашњих послова (2009). *Методологија рада криминалистичко-оперативне аналитике у електронској обради података*. Београд: МУП.
137. Министарство унутрашњих послова Републике Србије (2016). *Полицијско-обавештајни модел*: *Приручник*. Београд: Гласник.
138. Министарство унутрашњих послова Републике Србије (б. г.). *Управа криминалистичке полиције: СЗКА*. Са mup.rs (22. 11. 2023)
139. Moore, D. T. (2006). *Critical thinking and intelligence analysis* . Washington, DC: Joint Military Intelligence College.
140. Moore, D. T. (2007). *Critical thinking and intelligence analysis* (2nd printing, rev.). Washington, DC: National Defense Intelligence College.
141. Мучибабић, С. (2001). Садржај војне доктрине, начин њеног формулисања и примена. *Војно дело, 49*(6), 105–117.
142. Naone, E. (2011, August 22). *The new big data*. MIT Technology Review. technologyreview.com
143. National Consortium for the Study of Terrorism and Responses to Terrorism (n.d.). *Global Terrorism Database*. From https://www.start.umd.edu/gtd/ (29. 8. 2024)
144. Николић, Г. (2007). Институционални оквир МОКП – Интерпол. *Безбедност, 49*(4), 33–57.
145. Noble, R. K. (2008, October). *Fusion Task Force – Project Middle East: Third operational working group meeting.* INTERPOL.
146. NSI (2025, June 20). *Home page*. https://www.nsiteam.com/

147. Nye, J. S. (2021). Soft power: The evolution of a concept. *Journal of Political Power 14*,(1), 196–208. From https://doi.org/10.1080/2158379X.2021.1879572
148. Office of the Director of National Intelligence (n.d.). *Intelligence.gov*. https://www.intelligence.gov (24. 12. 2024)
149. Organization for Security and Co-operation in Europe (2017, June). *OSCE guidebook on intelligence-led policing*. OSCE Secretariat.
150. Османагић Беденик, Н. (2007). *Криза као шанса: Кроз пословну кризу до пословног успјеха*. Загреб: Школска књига.
151. Ozdemir, H. (2011, March). *Compstat: Strategic police management for effective crime deterrence in New York City* (Working Paper No. 30). International Police Executive Symposium; Geneva Centre for the Democratic Control of Armed Forces.
152. Petković, D. (2025). Applying text-to-SQL to SQL/OLAP using LLMs. In *Proceedings of the 8th International Conference on Machine Learning and Natural Language Processing (MLNLP 2025)*. Hangzhou: Monclair Publishing.
153. Петровић, П. (2020). *Реформа службе безбедности у Србији 2000–2017*. Докторска дисертација. Београд: Факултет политичких наука.
154. Практична екологија (2021, Април 13). Поплаве – последице на животну средину са https://www.prakticnaekologija.rs/2021/04/13/poplave-posledice-na-sredinu/ (4. 7. 2024)
155. Project Management Srbija (n.d.). *Standardi i standardizacija*. From: https://project-management-srbija.com/upravljanje-kvalitetom/standardi-i-standardizacija (29. 11. 2024)
156. Пророковић, Д. (2018). *Ера мултиполарности*. Београд: Службени гласник.
157. ProQuest Central (n.d.). *Database profile.* From: https://about.proquest.com/en/products-services/ProQuest_Central/ (2. 9. 2024)
158. Pujari, A. (2016). *Cyber terrorism*: World wide weaponisation! *TN Police Sesquicentennial Anniversary Souvenir*, 114–125.
159. Раденковић, Б., Станојевић, М. и Марковић, А. (1999). *Рачунарска симулација*. Београд: Факултет организационих наука.
160. Рацић, И. (2018). Значај аналитичких организационих јединица сектора за аналитику, телекомуникационе и информационе технологије у примени полицијско-обавештајног модела. *Безбедност, 60*(3), 138–152.
161. Рацић, И. (2023). *Полицијско-обавештајни модел у Републици Србији – предуслови за организационо прилагођавање*. Институт за криминалолошка и социолошка истраживања.
162. Рацић, И. М. и Достић, С. Р. (2024). Прикупљање података као извршна функција у криминалистичко-обавештајном раду у полицији Републике Србије. *Баштина, 62*, 101-113.
163. Ratcliffe, J. H. (2003). Intelligence-led policing. *Trends & Issues in Crime and Criminal Justice*, (248).
164. Ratcliffe, J. H. (2008). *Intelligence-led policing*. Cullompton: Willan Publishing.
165. Ratcliffe, J. H. (2016). *Intelligence-Led Policing* (2nd ed.). Routledge. DOI: 10.4324/9781315717579
166. Real Instituto Elcano (n.d.). Europol and the European Criminal Intelligence Model: A non-state response to organised crime. From

https://www.realinstitutoelcano.org/en/analyses/europol-and-the-european-criminal-intelligence-model-a-non-state-response-to-organised-crime-ari/ (27. 11. 2023)
167. Ren, J. & Sovacool, B. K. (2014). Quantifying, measuring, and strategizing energy security from Determining the most meaningful dimensions and metrics. *Energy*, *76*(1), 838–849. https://doi.org/10.1016/j.energy.2014.08.083
168. Republika Hrvatska (2017). Zakon o sustavu domovinske sigurnosti. *Narodne novine*, br. 108/17. https://www.zakon.hr/z/955/Zakon-o-sustavu-domovinske-sigurnosti
169. Република Србија и Црна Гора (2004). Стратегија одбране Државне заједнице Србија и Црна Гора. *Службени лист СЦГ*, бр. 55/2004*55/2004*.
170. Република Србија (2002). Закон о Безбедносно-информативној агенцији. *Службени гласник РС*, бр. 42/2002, 111/2009, 66/2014, члан 2.Република Србија (2006). Устав Републике Србије. *Службени гласник РС*, бр. 98/2006, чл. 97, т. 4.
171. Република Србија (2007a). Закон о одбрани. *Службени гласник РС*, бр. 116/2007, 10/2015, 36/2018, чл. 4, т. 14, т. 16.
172. Република Србија (2007b). Закон о основама уређења служби безбедности Републике Србије. *Службени гласник РС*, бр. 116/2007, 72/2012.
173. Република Србија (2009a). Закон о тајности података. *Службени гласник РС*, бр. 104/2009, чл. 87.
174. Република Србија (2009b). Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији Републике Србије. *Службени гласник РС*, бр. 88/2009, 55/2012 (УС), 17/2013.
175. Република Србија (2009c). Стратегија националне безбедности Републике Србије. *Службени гласник РС*, бр. 88/2009.
176. Република Србија (2017). Национална стратегија за спречавање и борбу против тероризма за период 2017–2021. *Службени гласник РС*, бр. 94/2017.
177. Република Србија (2019). Стратегија националне безбедности Републике Србије. *Службени гласник РС*, бр. 94/2019.
178. Ронин, Р. (2009). *Обавештајни рад.* Београд: Службени гласник; Факултет безбедности.
179. SAGE Journals (n.d.). *Academic journals platform*. From https://journalsuk.sagepub.com/ (2. 9. 2024)
180. Сакан, М. (2006). *Методологија војних наука*. Београд: Војноиздавачки завод.
181. Савић, А., Делић, М. и Бајагић, М. (2002). *Безбедност света: Од тајности до јавности.* Институт безбедности.
182. Сивачек, Ј. (2006). *Научна утемељеност војне доктрине.* Докторска дисертација. Београд: Војна академија.
183. Симеуновић, Д. (2009). *Тероризам*. Београд: Правни факултет.
184. Симић, Б. и Никач, Ж. (2010). Место и улога Европола у међународној сарадњи. *Наука, безбедност, полиција*, *15*(2), 61–70.
185. Симић, Д. (2002). *Методе науке и техничког развоја*. Крагујевац: dsp-mecatronic.
186. Симоновић, Б. (2004). *Криминалистика*. Крагујевац: Правни факултет.
187. Smith, S. & Baylis, J. (2001). The *globalization of world politics*. London: Oxford University Press.

188. Стајић, Љ. (2008, 2013, 2021). *Основи система безбедности*. Нови Сад: Правни факултет.
189. Стајић, Љ. Гаћиновић, Р. (2007). *Увод у студије безбедности*. Београд: Драслар партнер.
190. Стајић, Љ., Радивојевић, Н. и Мирковић, В. (2017). Неки аспекти политике унутрашње безбедности као дела стратегије националне безбедности Републике Србије. *Зборник радова Правног факултета у Новом Саду*, 54(4), 1325–1342.
191. Стевановић, О. (2019). *Безбедносни менаџмент*. Београд: Криминалистичко-полицијски универзитет.
192. Стојановић, А. (2024). *Национална или државна безбедност*? Југпрес. Са https://jugpress.com/nacionalna-ili-drzavna-bezbednost/, 2. 1. 2024
193. Ступар, Т. и Ступар, Д. (2024). Превеницција криминалитета кроз дизајн окружења – пут ка стандардизацији. *Журнал за безбједност и криминалистику, 6*(2), 55-65.
194. Термиз, Џ. и Милосављевић, С. (2008). *Аналитика I*. Лукавац.
195. TOC Search (н.п.). Dostupno na: tocsearch.com
196. Tišma, M., & Andrić, J. (2021*).* Importance of cyber security awareness and e-learning motivation for cyber security in reshaping the education. *Journal of Information Systems & Operations Management, 15*(2), 284-296.
197. Тодоровић Радановић, М. (2015). *Значај аналитике у обавештајном раду*. Мастер рад. Београд: Универзитет у Београду.
198. Томашевић, К. и Рацић, И. (2019). Рад полиције заснован на примени полицијско-обавештајног модела у развијеним земљама са посебним освртом на полицију Републике Србије. *Безбедност, 61*(3), 82–100.
199. Трипковић, Б. (2004). Политичка права и слободе – међународни стандарди и њихова имплементација у домаћем праву. *Зборник радова Правног факултета у Новом Саду, 38*(2), 95–120.
200. Шебек, В. (2017). Доминантне карактеристике развијених криминалистичко-обавештајних модела и њихов утицај на полицијско-обавештајни модел у Републици Србији. *Безбедност , 59*(1), 16–35.
201. Шешић, Б. (1974). *Општа методологија*. Београд: Научна књига.
202. United Nations Development Programme (1994). *Human Development Report* (pp. 24-33). Oxford: Oxford University Press.
203. United Nations Office on Drugs and Crime (2011). *Criminal intelligence: Manual for managers.* New York: United Nations.
204. University of Novi Sad. (n.d.). *Logika istraživačkog rada*. https://www.ef.uns.rs/Downland/metodologija_nir/02%20logika.pdf (25. 11. 2024)
205. *Уредни лист Републике Словеније* (2019). *Uradni list RS*, št. 59/2019.
206. U.S. Department of Justice (2005). *Office of Justice Programs annual report*.
207. Вилијамс, Д. П. (Ур.) (2012). *Увод у студије безбедности*. Београд: Службени гласник.
208. Вилсон, Џ. Х. (2013). *Грешке и заташкавања војнообавештајних служби* (Б. Аночић, Прев.). Београд: Albion Books.
209. Вишњић, Д. (1995). Однос стратегије и војне доктрине. *Војно дело*, (5), 45–62.

210. Влада Црне Горе (б. г.). *Интернет портал*. Доступно на: http://www.gov.me (21. 4. 2022)
211. Војска Србије (2010). *Доктрина Војске Србије*. Београд: Медија центар „Одбрана“.
212. Војска Србије (2012). *Израда доктринарних докумената у Војсци Србије – Упутство*. Београд: Генералштаб Војске Србије.
213. Wæver, O. (1989), *Security the speech act, analysis the politics of a word* (Working paper No. 19.) Copenhagen: Centre for Peace and Conflict Research.
214. Wæver, O. (1995). Securitization and desecuritization. U R. D. Lipschutz (Ur.), *On security* (pp. 46–86). New York: Columbia University Press.
215. Wæver, O. (2008). The changing agenda of societal security. U G. Brauch, H. et al. (Ur.), *Globalization and environmental challenges: Reconceptualizing security in the 21st century* (pp. 581–593). Berlin: Springer.
216. Wæver, O., Buzan, B., Kelstrup, M., & Lemaître, P. (1993). *Identity, migration and the new security agenda in Europe*. London: Pinter.
217. Wiktionary (n.d.). Αναλυτικά. U *Wiktionary, the free dictionary*. Preuzeto 18. oktobra 2022. sa: https://en.wiktionary.org/wiki/αναλυτικά
218. Wolf, Y., & Frankel, O. (2007). Terrorism: Toward an overarching account and prevention with a special reference to pendulum interplay between both parties. *Aggression and Violent Behavior, 12*(3), 259–279.
219. Wolfers, A. (1952). “National Security” as an ambiguous symbol. *Political Science Quarterly, 67*(4), 481–502.
220. Зорић, М. (2010). Међународне кризе. *Војно дело, 62*(4), 292–333.
221. Жерајев, Ц. (1986). *Криминалистика*. Загреб: Вартекс.
222. Жигић, Д., Јаношевић-Дотлић, С., Иванковић, Д., Пертот, В. и Константиновић, Д. (1992). *Методологија научног истраживања*. Београд: Српско лекарско друштво.

ПРИЛОЗИ

Прилог 1. Упитник за усмерени интервју: *Креирање теоријског модела безбедносне аналитике на примеру супротстављања тероризму*

УНИВЕРЗИТЕТ ОДБРАНЕ У БЕОГРАДУ
ВОЈНА АКАДЕМИЈА
ДОКТОРСКЕ СТУДИЈЕ *МЕНАЏМЕНТ У ОДБРАНИ*

УСМЕРЕНИ ИНТЕРВЈУ
ИСТРАЖИВАЊЕ ЗА ДОКТОРСКУ ДИСЕРТАЦИЈУ

КРЕИРАЊЕ ТЕОРИЈСКОГ МОДЕЛА БЕЗБЕДНОСНЕ АНАЛИТИКЕ НА ПРИМЕРУ СУПРОТСТАВЉАЊА ТЕРОРИЗМУ

ДОКТОРАНД:
Јасмина Андрић

Београд, 2024

Поштовани/а,

Ја сам докторанд на Војној академији Универзитета одбране у Београду и у процесу сам израде докторске дисертације на тему „Креирање теоријског модела безбедносне аналитике на примеру супротстављања тероризму“.
Основна идеја моје дисертације је да се познати модели аналитике, препознатљиви по називима Обавештајна аналитика, Криминалистичка аналитика, Криминалистичко-обавештајна аналитика и други обједине у један теоријски модел, под јединственим називом Безбедносна аналитика.
Тај теоријски модел безбедносне аналитике бих проверила на примеру супротстављања тероризму, што је моја дугогодишња окупација у научном смислу и за шта сам едукована у земљи и иностранству. Једна од метода које примењујем у истраживању јесте испитивање, а техника усмерени интервју са експертима из предметних области.
Стога Вас, као препознатог експерта из предметних области, молим да учествујете у овом истраживању тако што ћете одговорити на питања која се налазе у наставку.
Искрено Вам захваљујем на сарадњи.

Јасмина Андрић

А. ПОДАЦИ О ИСПИТАНИКУ

Подаци о испитанику су анонимни за јавност и користе се само у сврху истраживања. Молимо Вас да дате одговоре дописивањем или заокруживањем понуђених.

1. Име и презиме:_____

2. Школска спрема:

   а) Висока
   б) Магистар/мастер
   в) Доктор наука
   г) Друго (навести)_____

3. Пол : М Ж

4. Старосна доб:

   а) до 30 година
   б) од 30 до 40 година
   в) од 40 до 55 година
   г) рреко 55 година

5. Да ли сте у склопу Вашег образовања имали прилике да изучавате тематику везану за безбедносну аналитику (кроз предмете, наставу, практичну наставу и слично)?

   а) Да
   б) Да, индиректно
   в) Не

6. Да ли сте кроз образовање или приликом заснивања радног односа имали прилике да прођете неку врсту обуке за обављање послова из домена безбедносне аналитике?

   а) Да
   б) Не

7. Који је Ваш професионални статус?

   а) Активни припадник служби безбедности (Војска, МУП, БИА)
   б) Пензионисани припадник служби безбедности (Војска, МУП, БИА)
   д) Остало (навести): _____

8. Да ли сте се у професионалној служби бавили безбедносном аналитиком?

а) Да
б) Не

9. Уколико сте у претходном питању одговорили са ДА, молим да прецизирате временски период бављења безбедносном аналитиком?

а) До 5 година
б) Од 5 до 10 година
в) Преко 10 година

10. Од испод понуђених, заокружите начин на који сте се бавили безбедносном аналитиком (може више од 1 одговора)?

а) Професионална надлежност
б) Истраживање
в) Настава
г) Остало (навести)_____

11. Уколико сте се бавили безбедносном аналитиком као професионалном надлежношћу, наведите у којој институцији (може више од 1 одговора)?

а) У командама Војске
б) У организационим јединицама МУП-а
в) У БИА
в) У ВБА
г) У ВОА
д) Остало (навести):_____

12. Уколико сте се бавили безбедносном аналитиком као професионалном надлежношћу, наведите у ком периоду сте били ангажовани на тим пословима (може више од 1 одговора)?

а) До 1992. године (пре распада Југославије)
б) Између 1992. и 1999. године
в) Између 1999. и 2009. године
г) Након 2009. године

13.Да ли сте пре ступања на своје дужности (за оне који су радили у обавештајном сектору) били упознати са аналитичким алатима и техникама које би Вам олакшале рад попут брејнсторминга, креирања индикатора или анализе супротстављених хипотеза?

а) Не, нисам упознат/а са наведеним техникама нити сам исте користио/ла у свом раду.

б) Да, упознат/а сам са наведеним техникама али их нисам користио/ла у свом раду.
в) Да, упознат/а сам са наведеним техникама и користио/ла сам их у свом раду.

ИНТЕРВЈУ

Усмерени интервју чине три дела: 1) питања из опште, претежно националне безбедности, 2) питања везана за безбедносну аналитику и 3) питања везана за теоријски модел безбедносне аналитике.
Молим Вас да на доле наведена питања дате Ваш одговор, став, дилему или предлог, у зависности од тога како је питање формулисано. Такође, молим Вас да уколико сматрате да је нешто значајно изостављено у постављеним питањима да то сугеришете.

А) ПИТАЊА ОПШТЕ (НАЦИОНАЛНЕ) БЕЗБЕДНОСТИ

1. У теорији постоји став да је појам национална безбедност остао недефинисан. Од понуђених одговора подвуците онај који одговара Вашем ставу, или допишите Ваш став, ако се не слажете са понуђеним.

а) Национална безбедност је безбедност нације
б) Национална безбедност је безбедност народа
в) Национална безбедност је безбедност државе
г) Национална безбедност је безбедност државе и грађана
д) _____

2. Концепти безбедности се успостављају у односу на референтни објект безбедности. Шта је по Вама референтни објекат националне безбедности (заокружите или допишите одговор):

а) Територија државе (границе)
б) Националне вредности, интереси и циљеви
в) _____

3. Копенхашка школа безбедности је, осим војног, утврдила и друге секторе безбедности: политички, економски, војни, социјетални (друштвени) и еколошки сектор. Слажете ли се да се тиме исцрпљује поље безбедности, или имате другачије гледиште, односно додатак наведеним секторима? (Заокружите одговор и ако имате додатак допишите)

а) Слажем се
б) Не слажем се
Додао/ла бих: _____

4. У теорији постоји класификација битних чиниоца (компоненти) националне безбедности на унутрашњу, спољашњу и интегралну безбедност. Да ли се слажете да наведени чиниоци представљају структуру система безбедности:

а) Да

б) Не Ако не, наведите који су:

_____

_____

_____

_____

5. Опис стања националне безбедности као целине, а узимајући у обзир ставове из претходних питања 3 и 4, могуће је дати:

а) описом сектора безбедности

б) описом компоненти/чинилаца безбедности аналитичким приступом

в) заједничким описом сектора и компоненти/чинилаца безбедности аналитичко-синтетичким приступом

6. У очувању безбедности једне државе значајна ставка су изазови, ризици и претње којима је поједина држава изложена. Изазови, ризици и претње се обично налазе у стратегијама безбедности. Иако је свака држава спецификум за себе неке претње попут тероризама се налазе у већини стратегија и препознате су као глобалне претње. Да ли се слажете да тероризам представља опасност за све државе света без изузетка?

а) Да

б) Нисам сигуран/а

в) Не

7. Да ли се слажете са следећом тврдњом: „Тероризам увек функционише у домену политике и спада у сложене облике политичког насиља“?

а) Да

б) Нисам сигуран/а

в) Не

8. Често тежимо да утврдимо просторни распоред терористичких напада, њихове последице, смртност, порекло и финансирање терористичких организација и сличне податке. Стога, да ли сматрате да је обавештајни рад значајан за супротстављање савременом тероризму као претњи безбедности?

а) Да, изузетно значајан

б) Нисам сигуран/а

в) Не

Б) ПИТАЊА ИЗ ДОМЕНА БЕЗБЕДНОСНЕ АНАЛИТИКЕ

1. Да би прикупљени подаци били веродостојни морају се проверити кроз најмање 3 различита извора. Да ли је наведена тврдња истинита?

а) Да
б) Нисам сигуран/а
в) Не

2. Како би се дошло до потпуних обавештајних података, на пример о питањима везаним за тероризам или стању безбедности једне државе, потребна је мултисекторска сарадња (полиција, војска, службе безбедности, цивилни сектор и слично). Да ли је наведена тврдња истинита?

а) Да
б) Нисам сигуран/а
в) Не

3. Да ли сте кроз свој рад упознати са полицијско-обавештајним моделом (ПОМ)?

а) Да
б) Знам шта је ПОМ, али нисам имао/а практична искуства
в) Не, нисам сигуран/а шта је ПОМ

4. Уколико је ваш одговор на претходно питање ДА, да ли мислите да ПОМ може бити један од чинилаца који доприноси развоју безбедносне аналитике?

а) Да
б) Нисам сигуран/а
в) Не

5. Безбедносна аналитика је уједно и мултисекторска вештина и мултидисциплинарна област јер обухвата више различитих сектора безбедности и има мултидисциплинарну примену у истраживању области безбедности. Да ли је наведена тврдња истинита?

а) Да
б) Нисам сигуран/а
в) Не

6. Да ли сте сагласни са ставом да израз „безбедносна аналитика“ примењује у пракси под тим називима Обавештајна аналитика, Криминалистичка анализа, Криминалистичко-обавештајна аналитика и другим?

а) Да
б) Не

Ако сте одговорили са НЕ, образложите Ваш став:

_____
_____
_____
_____
_____
_____
_____

7. Уобичајено је да се „аналитике“ наведене у претходном питању одвијају као део ширег процеса именованог као обавештајни циклус. У наредној табели дати су ставови из теорије који указују на фазе обавештајног циклуса. Молимо Вас да се определите за неки од предлога (заокружите број), или да допишете шта Ви сматрате као фазе обавештајног циклуса

Бр.		**САДРЖАЈИ ОБАВЕШТАЈНОГ ЦИКЛУСА**
1.		- Појава обавештајног проблема који заслужује пажњу стратегијских обавештајних служби - Анализирање обавештајног проблема и детаљно сагледавање свих његових страна - Разматрање расположивих и прикупљање нових података - Критичко процењивање података - Проучавање процењних података, као предуслов за одређивање хипотеза - Прикупљање података у правцима које одређују постављене хипотезе - Излагање – утврђивање веродостојности једне или више хипотеза

2.		- Прикупљање „сирових обавештајних података“ - Процењивање и производња тј. проверавање, разврставање и процењивање веродостојности прикупљених информација, извлачење значајних закључака и њихово тумачење у складу са потребама корисника - Уступање обавештајних сазнања корисницима у најприкладнијој форми
3.		- Планирање - Прикупљање информација - Обрада и анализирање информација - Уступање информација
4.		- Планирање и усмеравање - Прикупљање информација - Обрада информација - Анализа информација и продукција - Уступање (дисеминација) аналитичких производа
5.		- Управљање обавештајним радом - Прикупљање обавештајних информација - Анализа - Производња завршних обавештајних сазнања - Уступање производа - Повратна спрега
6.		- Уочавање безбедносног проблема - Утврђивање обавештајних потреба - Преношење обавештајних захтева - Иницијатива - Планирање и организовање обавештајног истраживања - Прикупљање сирових обавештајних информација - Обрада информација - Израда сирових обавештајних докумената - Уступање завршних обавештајних докумената - Техничка интерпретација завршних обавештајних сазнања - Повратна спрега
7.	Став испитаника	

8. Аналитика као део Обавештајног циклуса негде се (нпр. у полицији) именује као анализа. Да ли сматрате да је употреба појма анализа уместо аналитика коректна?

а) Да
б) Не

9. У оцени веродостојности информације и поузданости извора користе се модели „4 x 4“ (Србија, ЕУ), „5 x 5“ (Велика Британија) и „6 x 6“ (САД) приказани у табелама испод. Који је

по Вама модел најкомплекснији и најприхватљивији за нашу теорију и праксу (заокружите одговор)?

а) „4 x 4“
б) „5 x 5“
в) „6 x 6“

Табела *Модел САД („6 x 6“)*

Поузданост извора		**Тачност податка**	
A	потпуно поуздан	**1**	потврђен из других извора
B	углавном поуздан	**2**	вероватно тачан
C	прилично поуздан	**3**	могуће тачан
D	углавном непоуздан	**4**	сумњив
E	Непоуздан	**5**	није вероватан
F	поузданост се не може оценити	**6**	истинитост се не може оценити

Табела *Наш модел („4 x 4“)*

Поузданост извора		**Тачност податка**	
A	Поуздан	**T**	тачан
B	углавном поуздан	**V**	вероватан
C	углавном непоуздан	**S**	сумњив
D	Непоуздан	**L**	лажан

Табела *NIM систем „5 x 5“ (Велика Британија)*

Процена извора	**A** *Увек поуздан*	**B** *Углавном поуздан*	**C** *Понекад поуздан*	**D** *Непоуздан извор*	**E** *Неиспитан извор*
Процена информације	**1** *Тачна без сумње*	**2** *Информација позната извору*	**3** *Информација није лично позната извору*	**4** *Не може се проценити информација*	**5** *Постоји сумња у неистинитост информације*
Кодови за руковање информацијама	**1** *Ширење дозвољено у полицијским организација-ма Велике Британије и другим агенцијама за спровођење закона које су наведене*	**2** *Ширење дозвољено другим странама (партнерима) које немају овлашћења кривичног гоњења*	**3** *Ширење дозвољено Међународним агенцијама за спровођење закона (ван ЕУ)*	**4** *Ширење само у оквиру агенције из које потиче информација (са навођењем разлога или интерног примаоца)*	**5** *Дозвола ширења, али под условима да пријемна агенција поштује постављене услове*

Извор: *Форца и Аночић, 2018.*

10. У теорији постоје различити ставови какве особине треба да има безбедносни (обавештајни) аналитичар. На основу Вашег искуства изнесите став о томе које су пожељне особине које треба да одликују обавештајног (безбедносног) аналитичара?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

11. Базе података имају велику улогу у раду безбедносних (обавештајних) аналитичара. Каква су Ваша искуства у раду са базама података?

_____
_____
_____
_____
_____
_____
_____
_____
_____

12. Да ли сте упознати са подацима доступним из јавних извора, односно ОСИНТ (open source intelligence) подацима?

а) Да
б) Не

13. Да ли сте у свом раду користили јавно доступне научне базе попут Глобалног индекса тероризма Института за економију и мир из Њујорка или неку сличну базу?

а) Да
б) Упознат/а сам са овом (или сличном) базом података али је у свом раду нисам користио/ла
в) Не

14. Да ли сматрате да је безбедносна аналитика значајна за супротстављање савременим претњама безбедности попут тероризма?

а) Да
б) Нисам сигуран/а
в) Не

15. Сматрате ли да је могуће да се успостави јединствена безбедносна аналитика на нивоу националне (безбедност државе) безбедности?

а) Да
б) Не

Молим да образложите одговор:

16. Какав је Ваш став о потреби да се формира јединствени центар у оквиру служби безбедности, који би обједињавао досадашње моделе аналитика (обавештајна, криминалстичка…), односно био кров за те аналитике (заокружите и образложите одговор)?

а) Да, то би било добро решење
б) Не

Молимо да образложите Ваш одговор:

_____
_____
_____
_____
_____
_____
_____
_____

17. У разним врстама аналитике, поготово у страним државама, користе се одређени стандарди. Молим Вас да укратко наведете какав је Ваш став о коришћењу стандарда у разним врстама аналитике у нашој земљи?

18. Да ли сте упознати са ISO стандардом 27001 – Систем управљања безебедношћу информација (заокружите одговор)?

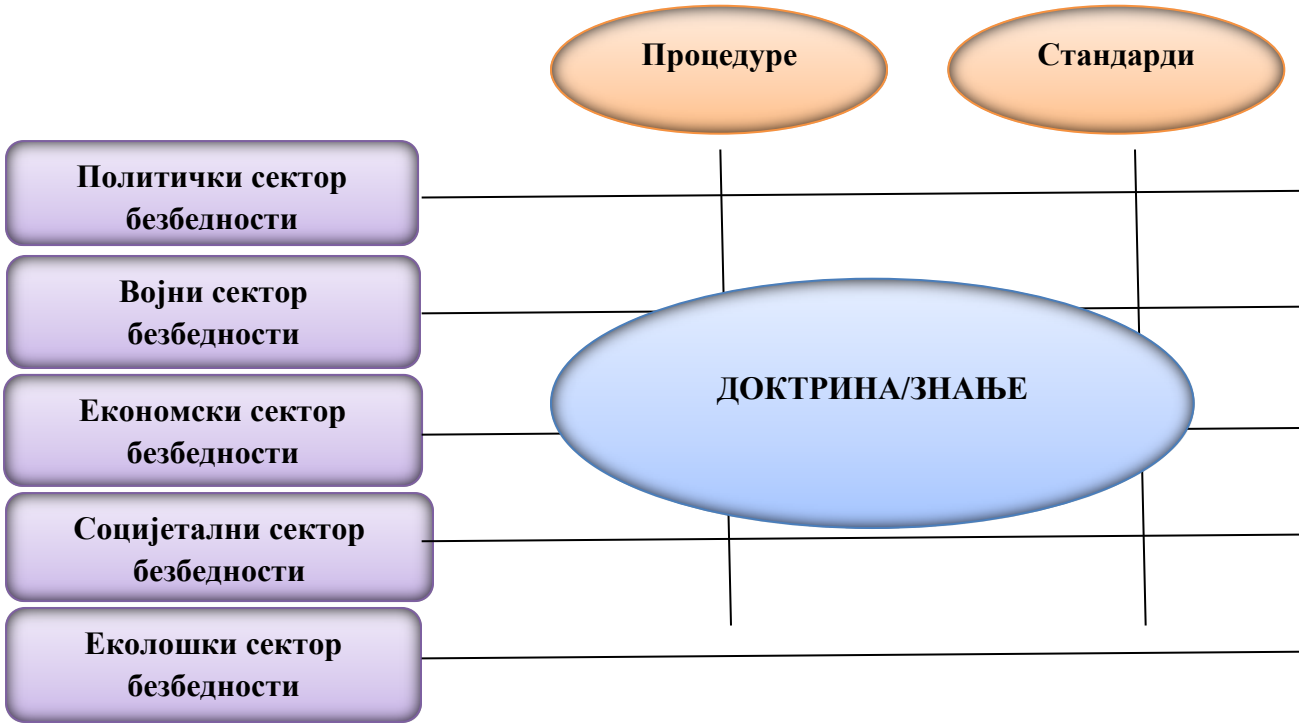
а) Да
б) Не

19. Да ли сте упознати са ГДПР уредбом Европске уније (Општа уредба о заштити података о личности) којој и Србија као кандидат за чланство подлеже (заокружите одговор)?

а) Да
б) Не

В) ПИТАЊА ИЗ ДОМЕНА ТЕОРИЈСКОГ МОДЕЛА БЕЗБЕДНОСНЕ АНАЛИТИКЕ

1. На наредној Слици је приказана идејна скица о изградњи теоријског модела безбедносне аналитике:



Слика *Општа шема теоријског модела безбедносне аналитике*

Молимо Вас да прокоментаришете приказани предлог теоријског модела безбедносне аналитике:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Најсрдачније се захваљујем на сарадњи!

Прилог 2. Табела са подацима о експертској групи за оцену теоријског модела безбедносне аналитике

Табела *Експертска група за оцену теоријског модела безбедносне аналитике*

ИМЕ И ПРЕЗИМЕ	ЗВАЊЕ	КОМПЕТЕНЦИЈЕ
Андреја Савић	Редовни професор	Проф. др Андреја Савић целу своју професионалну каријеру провео је на пословима у полицији и службама безбедности, истовремено и као професор у високошколској настави. Значајније дужности: помоћника министра унутрашњих послова РС и начелника Ресора државне безбедности (2001-2002), а од јула 2002. до јануара 2003. и дужност првог директора новоформиране Безбедносно-информативне агенције Владе Републике Србије. Објавио је 12 уџбеника и

		монографија, примарно у домену безбедности, од којих нека у стручној јавности имају карактер капиталних дела.
Бранко Крга	Редовни професор	Генерал и професор Бранко Крга целу своју професионалну каријеру провео је у Војсци, највећим делом у органима обавештајне службе. Од значајнијих дужности истичу се: командант бригаде, војни изасланик у Москви, начелник Обавештајне управе ГШ; заменик начелника ГШ и начелник Генералштаба. Редовни је професор. Објавио је већи број научних радова из домена безбедности, а посебно се издваја монографија *Стратегија националне безбедности у теорији и пракси.*
Нђо Даниловић	Редовни професор	Проф. др Нђо Даниловић радни век је провео у Војсци. У научном усавршавању одбранио је две докторске дисертације. Доказани је експерт у домену методологије, примарно у сфери аналитике. У том смислу, посебно се бави безбедносном аналитиком. Написао је десетине научних радова, као и уџбенике *Основи безбедносне аналитике* (са проф.др Славомиром Милосављевићем, 2008) и *Безбедносна аналитика* (са групом професора, 2018) и *Аналитички процес у безбедности* (са проф. др Драганом Манојловићем, 2024). Активни је професор на Универзитету МБ где, између осталог, предаје и предмет *Безбедносна аналитика.*
Божидар Форца	Редовни професор	Генерал и професор др Божидар Форца целу своју професионалну каријеру провео је у Војсци. Најзначајније дужности су му биле: заменик директора Института ратне вештине, начелник управе за планирање ГШ, начелник Управе за стратегијско планирање МО. Још увек обавља послове универзитетског професора и начелник је Катедре безбедности на Факултету за пословне студије и право. Аутор више стотина научних радова, студија, монографија, уџбеника, пре свега у сфери безбедности. Дуго година се практично и теоријски непосредно бави безбедносном аналитиком, где је издао и уџбеник *Безбедносна аналитика,* а тај предмет предаје на Факултету на коме је запослен.
Илија Рацић	Доцент	Доцент др Илија Рацић је активни припадник МУП-а Србије са 20 година радног искуства. Први је доктор у историји Криминалистичко-полицијског универзитета на тему: *Организационо прилагођавање полиције потребама примене полицијско-обавештајног модела у Републици Србији*. Објавио је и монографију *Полицијски обавештајни модел у Републици Србији.* Експерт је у теорији и пракси примене полицијско-обавештајног модела, што доказују практично искуство, и бројни научни радови, реализација наставе из тог предмета, као и учешће у изради бројних стратешких националних докумената и међународних аката предметне проблематике.
Бранислав Аночић	Пуковник у пензији	Пуковник Бранислав Аночић је члан експертског тима као лице – експерт из праксе. Најзначајније дужности у војној каријери јесу: начелник обавештајне управе Генералштаба и војни изасланик у Мађарској и у САД. Поред неколико деценија рада непосредно везаног за праксу у безбедносној (обавештајна) аналитици, коаутор

		је уџбеника *Безбедносна аналитика* (са проф. др Божидаром Форцом) и преводилац значајних страних дела из те проблематике као, на пример: Џон Хјуз Вилсон, *Грешке и заташкавања војно-обавештајних служби,* Albion-Books, Београд, 2013.

Прилог 3. Дијаграм базе података за безбедносну аналитичку платформу (тероризам)

PSEUDOKOD

```
WITH incidents_joined AS (
    SELECT
        inc.incident_id,
```

```
        inc.agency_id,
        inc.date_id,
        inc.location_id,
        inc.type,
        inc.severity,
        inc.casualties,
        inc.source_confidence,
        loc.country,
        loc.region,
        age.data_sensitivity_level
    FROM analyst_inteligence.Fact_Incidents AS inc
    LEFT JOIN analyst_inteligence.Dim_Location AS loc ON inc.location_id = loc.location_id
    LEFT JOIN analyst_inteligence.Dim_Agency AS age ON inc.agency_id = age.agency_id
)

SELECT
    date_id,
    location_id,
    agency_id,
    country,
    region,
```

```
    data_sensitivity_level,

    COUNT(incident_id) AS total_incidents,
    SUM(casualties) AS total_casualties,

    AVG(CASE
        WHEN severity = 'Critical' THEN 3
        WHEN severity = 'High' THEN 2
        WHEN severity = 'Medium' THEN 1
        ELSE 0
    END) AS avg_severity_score,
    AVG(source_confidence) AS avg_source_confidence
FROM incidents_joined
GROUP BY 1, 2, 3, 4, 5, 6
```

Псеудокод, који бисмо направили у фајлу dim_operation_risk.sql, који треба да направи поглед који има сврху анализе исхода операција према нивоима ризика, при праћењу трендова кроз податке.

```
SELECT
    op.operation_id,
    op.agency_id,
```

```
    op.type,
    op.risk_level,
    op.outcome,

    time.year,
    time.quarter,

    CASE WHEN op.outcome = 'Success' THEN 1 ELSE 0 END AS is_successful,
    CASE WHEN op.risk_level = 'High' THEN 1 ELSE 0 END AS is_high_risk,
      CASE op.risk_level
      WHEN 'Extreme' THEN 5
      WHEN 'High' THEN 4
      WHEN 'Medium' THEN 3
      WHEN 'Low' THEN 2
      ELSE 1
    END AS risk_score
FROM analyst_inteligence.Fact_Operations AS op
LEFT JOIN analyst_inteligence.Dim_Time AS time ON op.operation_id = time.date_id
```

Модел који правимо у фајлу int_consolidated_threat_feed.sql има сврху да укрсти податке о инцидентима са обавештајним извештајима, то јесте праве догађаје са потенцијалним претњама.

```
WITH incident_base AS (
```

```
    SELECT
        inc.incident_id,
        inc.type AS incident_type,
        inc.severity AS incident_severity,
        inc.date_id,
        loc.city,
        loc.country
    FROM analyst_inteligence.Fact_Incidents AS inc
    LEFT JOIN analyst_inteligence.Dim_Location AS loc ON inc.location_id = loc.location_id
),
report_base AS (
    SELECT
        report_id,
        keywords,
        topic,
        threat_score
    FROM analyst_inteligence.Fact_Intelligence_Reports)
SELECT
    inc.incident_id,
    inc.incident_type,
    inc.incident_severity,
```

```
    inc.date_id,
    inc.city,
    inc.country,

    rep.report_id AS associated_report_id,
    rep.topic AS report_topic,
    rep.threat_score,

    (inc.incident_severity + rep.threat_score) AS blended_threat_score
FROM analyst_inteligence.incident_base AS inc
LEFT JOIN analyst_inteligence.report_base AS rep
    ON ARRAY_CONTAINS(rep.keywords, inc.incident_type::VARIANT)
    OR rep.topic = inc.incident_type
```

Прилог 4. *Шема могуће структуре Координационог центра за безбедносну аналитику*