Зборник радова са конференције

Стратешки и нормативни оквир Републике Србије за реаговање на савремене безбедносне ризике

Божидар Бановић
Ненад Стекић (ур.)

NEWSIMR&D
Funded by Science Fund of the Republic of Serbia
Фонд за науку Републике Србије

[ФБ]
УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ
UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

ЗБОРНИК РАДОВА
са конференције

Стратешки и нормативни оквир Републике Србије за реаговање на савремене безбедносне ризике

Проф. др Божидар Бановић
Др Ненад Стекић (ур.)

Београд,
Март, 2023.

ЗБОРНИК РАДОВА СА КОНФЕРЕНЦИЈЕ
СТРАТЕШКИ И НОРМАТИВНИ ОКВИР РЕПУБЛИКЕ СРБИЈЕ ЗА РЕАГОВАЊЕ НА САВРЕМЕНЕ БЕЗБЕДНОСНЕ РИЗИКЕ [1]

Издавач
Универзитет у Београду-Факултет безбедности

За издавача
Проф. др Владимир Н. Цветковић
Декан Факултета безбедности Универзитета у Београду

Уредници
Проф. др Божидар Бановић
Др Ненад Стекић

Лекторка
Љиљана Мирић

Техничко уређивање
Горан Мандић
Ана Нешић

Дизајн корице
Ненад Стекић

Тираж
100 (CD)

ISBN 978-86-80144-60-3

Штампа
Универзитет у Београду-Факултет безбедности, Господара Вучића 50, Београд

[1] Конференција се реализује у оквиру пројекта који финансира Фонд за науку Републике Србије у оквиру Програма "ИДЕЈЕ" - Management of New Security Risks - Research and Simulation Development, NEWSIMR&D, #7749151.

Научни одбор Конференције

Проф. др **Петар Станојевић**, редовни професор, Универзитет у Београду-Факултет безбедности, председник одбора

Проф. др **Владимир Н. Цветковић**, редовни професор, Универзитет у Београду-Факултет безбедности

Проф. др **Божидар Бановић**, редовни професор, Универзитет у Београду-Факултет безбедности

Проф. др **Младен Милошевић**, редовни професор, Универзитет у Београду-Факултет безбедности

Проф. др **Ненад Путник**, редовни професор, Универзитет у Београду-Факултет безбедности

Организациони одбор Конференције

Проф. др Божидар Бановић, председник одбора
Проф. др Горан Мандић
Проф. др Ана Ковачевић
Доц. др Александра Илић
Доц. др Божидар Оташевић
Пук. др Дејан Вулетић
Мср Александра Вуловић
Мср Милош Јовичић

Секретар организационог одбора
Мср Јана Марковић, докторанд

Списак рецензената

Проф. др **Божидар Бановић**, редовни професор, Универзитет у Београду-Факултет безбедности
Проф. др **Бранислав Ђорђевић**, редовни професор, Институт за међународну политику и привреду
Проф. др **Зоран Драгишић**, редовни професор, Универзитет у Београду-Факултет безбедности
Проф. др **Младен Милошевић**, редовни професор, Универзитет у Београду-Факултет безбедности
Проф. др **Ненад Путник**, редовни професор, Универзитет у Београду-Факултет безбедности
Проф. др **Петар Станојевић**, редовни професор, Универзитет у Београду-Факултет безбедности
Проф. др **Зоран Јефтић**, ванредни професор, Универзитет у Београду-Факултет безбедности
Проф. др **Ивана Бодрожић**, ванредни професор, Криминалистичко-полицијски универзитет
Проф. др **Александра Илић**, ванредни професор, Универзитет у Београду-Факултет безбедности
Доц. др **Иван Ракоњац**, доцент, Универзитет у Београду-Факултет безбедности

САДРЖАЈ

ПРЕДГОВОР

Пред читаоцима се налази Зборник саопштења са националне научне конференције „Стратешки и нормативни оквир Републике Србије за реаговање на савремене безбедносне ризике“. Зборник представља израз настојања за академским уобличавањем и приказом најновијих налаза истраживања у домену управљања ризицима у Републици Србији.

Једнодневна научна конференција организована је 16. децембра 2022. године на Факултету безбедности, у оквиру пројекта „Управљање новим безбедносним ризицима – истраживање и развој симулација – NEWSIMR&D“ који имплементира пројектни тим Факултета безбедности Универзитета у Београду, заједно са Криминалистичко-полицијским Универзитетом, Факултетом инжењерских наука Универзитета у Крагујевцу и Институтом за стратегијска истраживања Универзитета одбране. Циљ пројекта је оснивање Националног симулационог центра у оквиру ког ће се вршити софтверско симулирање свих врста безбедносних ризика, као и израда стратегија за ефикасно управљање кризама. Пројекат финансира Фонд за науку Републике Србије у оквиру Програма ИДЕЈЕ.

Главна новина овог пројекта је интердисциплинарни и трансдисциплинарни приступ анализама безбедносних феномена, као што су сајбер криминал, миграциона криза, манипулација личним подацима, савремени друштвени поремећаји, глобалне епидемије (пандемије), енергетска безбедност и др. Пројекат подстиче интердисциплинарни приступ и сарадњу између истраживача различитих профила – друштвених, хуманистичких, инжењерских и технолошких наука.

Овај Зборник обухвата 14 чланака који су саопштени у оквиру два тематска панела Конференције – први под називом „Стратешки документи и нормативни оквир за реаговање на савремене безбедносне ризике“ и други у оквиру ког су представљене студије случаја. Зборник је организован тако да прати тематске панеле Конференције.

У оквиру прве тематске целине Зборника, радови проучавају проблематику савремених ризика по безбедност државе али и читавог човечанства. Владимир Н. Цветковић пише о суверености, правди и опстанку као варијаблама које се преплићу кроз призму идентификовања нових безбедносних ризика. Аутор уочава рањивост јавних институција, илегалне миграције и идентитетске претње као три проблема који заврђују додатну пажњу у будућим анализама ризика. Ненад Путник нуди приказ методологије израде Стратегије националне безбедности Републике Србије. Он разматра основна стратешка документа из области безбедности у Републици Србији и пружа препоруке за њихову евентуалну ревизију или допуну, у односу на актуелне спољне и унутрашње изазове, и

по узору на методологију израде безбедносних стратегија земаља чланица ЕУ.

У оквиру настојања да пруже академски подстицај унапређењу стратешког оквира Републике Србије за спречавање и сузбијање организованог криминала, Божидар Бановић и Ненад Стекић усредсређују се на приказ недостатака правног регулисања ове материје и могућности унапређења постојећег стања. Они анализирају позитивноправне норме у овој области и нуде приказ могућег модела стратешког и нормативног корпуса аката Републике Србије по узору на решења из Народне Републике Кине. Идентификујући поједине елементе стратешко-нормативног одговора Републике Србије у сфери сузбијања тероризма, Александра Илић наводи два важна аспекта – први, организацију и надлежности државних органа у сузбијању тероризма, и са друге стране, специфичност кривичноправног реаговања, које се према њеном становишту огледа и у контексту извршења казне затвора. Јана Марковић приказује анализу стратегија националне безбедности Републике Србије усвојених 2009. и 2019. године, и то са аспекта унутрашње безбедности. Она узима унутрашњу безбедност као полазну основу и перспективу анализе с обзиром на то да је њено разумевање предуслов разумевања стратешких аката као и делатности надлежних органа државне управе и рад правних лица, предузетника и физичких лица који врше послове приватног обезбеђења. Стратегија националне безбедности и приватно обезбеђење су две варијабле у чланку Горана Мандића. Он упућује на мањкавости Стратегије националне безбедности Републике Србије из 2019. године у којој постоји другачији приступ према приватном обезбеђењу с обзиром на одсуство дефинисања сарадње приватног обезбеђења са субјектима националне безбедности.

Постављајући хипотезу да је ефикасна (национална) логистика неопходан услов за функционисање друштва, као и за реализацију мисија и задатака управљачког и извршног дела система безбедности у миру, а нарочито у периоду криза или оружаних сукоба, Дејан Вулетић анализира обухват националне логистике у стратегијским документима планирања одбране Републике Србије. У свом раду, он закључује да национална логистика као термин није препозната у стратегијским документима планирања одбране, већ само њени одређени елементи који су разматрани, углавном, у мањој мери.

Други сегмент овог Зборника у ком су приказане студије случаја, почиње чланком Милоша Јовичића који упућује на концепт стратешких нафтних резерви као алата за сузбијање низа дисрупција у одрживом снабдевању нафтом и нафтним дериватима. Циљ његовог истраживања је проналажење оптималног приступа у моделирању националног ланца снабдевања

нафтом и структуре стратешких нафтних резерви. Предмет рада Петра Станојевића обухвата логистику нафте и нафтних деривата на подручју Републике Србије. Након спроведеног истраживања, овај аутор је потврдио претпоставку да логистика нафте и снабдевање нафтним дериватима у Србији имају уско грло у Јадранском нафтоводу, и понудио могуће алтернативне правце и изворе снабдевања.

Ана Ковачевић испитује могућности примене машинског учења на сајбер безбедност. У свом раду ауторка нуди одговоре на нека од питања попут могућности машинског учења да убрзају сајбер нападе као и предности овог вида вештачке интелигенције у обради великог скупа података. Казненоправни оквир заштите података у Републици Србији приказан је у чланку Младена Милошевића. Аутор даје аргументовану оцену законодавчевог приступа и сугерише да су неопходне измене и допуне појединих прописа у циљу њиховог међусобног усаглашавања и изградње солиднијег правног оквира.

Божидар Оташевић указује на законодавни оквир контроле канабиса у Србији и на криминалистичко-форензичку обраду места кривичног догађаја на ком се налази илегални засад канабиса, са посебним акцентом на значај материјалних доказа у сузбијању ове врсте криминалитета. У раду су посебно описани трагови карактеристични за засад канабиса, њихово проналажење, фиксирање, узорковање, паковање и слање на различита лабораторијска вештачења. Последњи чланак у Зборнику написала је Александра Вуловић. Чланак третира примене симулација у кризним ситуацијама, а посебан осврт је дат на њихову тренутну примену у кризним ситуацијама које су изазване природним непогодама – земљотресима и поплавама. Ауторка је ове кризне ситуације изабрала због учесталости последњих година на нашим просторима као и због чињенице да представљају веома велики ризик, како за јавну инфраструктуру, тако и за живот људи.

Верујемо да ће ваљана научна обрада сложених проблема која је представљена у оквиру овог Зборника, бити инспирација за даља истраживања и наставак блиске сарадње међу академским ауторима у земљи и иностранству у области управљања ризицима, као и за успешан наставак имплементације пројекта NEWSIMR&D.

У Београду,
Март, 2023.

Уредници
Проф. др Божидар Бановић
Др Ненад Стекић

ОПСТАНАК, СУВЕРЕНОСТ И ПРАВДА У КОНТЕКСТУ НОВИХ БЕЗБЕДНОСНИХ ИЗАЗОВА (РАЊИВОСТ ЈАВНИХ ИНСТИТУЦИЈА, ИЛЕГАЛНЕ МИГРАЦИЈЕ И ИДЕНТИТЕТСКЕ ПРЕТЊЕ)

Владимир Н. Цветковић[1]

Апстракт

Сврха безбедности државе јесте обезбеђивање опстанка (достојанствено преживљање), независности (сувереност) и правичне стабилности (легитимност). Они се обликују унутар конкретног историјског и политичког контекста који одређује смисао појединачних егзистенција и колективног живота. Имајући у виду дати концептуални оквир, аутор предлаже израду интерактивних дигиталних мапа Србије и окружења које би омогућиле процену безбедносних ризика од различитих врста претњи, посебно оних које се односе на угрожавање јавних институција у области образовања, здравства и правосуђа (болнице, школе, судови), неконтролисане миграционе токове (избеглице и илегалне миграције), као и на потирање културног, односно националног српског идентитета.

Кључне речи: Србија, опстанак, суверенитет, правда, безбедносне претње, јавне институције, миграције, национални идентитет.

Увод

Сваки безбедносни проблем представља јединствени збир аутентичних изазова, потенцијалних ризика и конкретних претњи који су детерминисани економским и политичким интересима, као и идеолошким вредностима које се бране или нападају у датом историјском контексту. Безбедносни *изазов*, као начелно

[1] Факултет безбедности, Универзитет у Београду, e-mail: vcvetkovic@fb.bg.ac.rs

Рад је настао у оквиру пројекта Фонда за науку Републике Србије „Идеје“ – Пројекат акцелерације иновација и подстицања раста предузетништва у Републици Србији – Management of New Security Risks – Research and Simulation Development – NEWSIMR&D, #7749151.

вредносно-неутрални друштвени феномен, садржи нејасно одређен безбедносни *ризик* од мање-више отворених безбедносних *претњи* чији је услов постојања политичке субјективизације коју чине организоване политичке заједнице (државе) и друштвене групе (политичке странке, покрети, организације). Њихово постојање обележено је историјски структурисаним системом потреба, интереса и вредности које се бране или намећу другима. Због тога сваки концепт безбедности има своју *одбрамбену* – миротворну и/или „конзервативну“ и ону *нападачку* – по властитом саморазумевању „прогресивну“, а по учинцима агресивну страну. У привидној противуречности одбране и напада очитују се предности и ограничења разноликих аналитичких концепата наука безбедности које обухватају релативно ново научноистраживачко или тематско подручје унутар већ етаблираног поља друштвених наука.[2]

Насупрот охолој наивности идеолошке мантре о „крају историје“ која је доминирала у време настанка и сазревања наука безбедности (Цветковић, 2022), данас је напросто глупо негирати чињеницу да је сваки безбедносни изазов, био он „стари“ или „нови“, локални, регионални или глобални, увек непосредни израз конкретне *друштвене* историје и њене (за безбедност) одлучујуће *политичке* димензије. Целовито разумевање безбедносног изазова и примерено процењивање могућности да он постане конкретна безбедносна претња (опасност) подразумева поседовање дискурзивног знања о историјској генези друштвених околности, интересима и вредностима политичких и других актера који обликују структуру друштвеног контекста. На том основу се гради процена безбедносног ризика која није ништа друго до одређивање степена вероватноће преображаја начелног „изазова“ у стварну, тј. конкретну „претњу“ (Цветковић, 2020).

Први и основни гносеолошки проблем са којим се овде суочавамо јесте избор, односно креирање појмовног речника. У том погледу још увек болујемо од карактеристичних „дечјих болести“ младих научних дисциплина. Захваљујући упорном и некритичком коришћењу термина и „стандарда“ из појмовног НАТО вокабулара који се наметнуо логиком старијег и јачег „партнера“, у стручној литератури је створена прилична конфузија у тумачењу безбедносних феномена, при чему се фамозна синтагма „изазови, ризици и претње“ обично третира као еволутивни низ од мање ка већој опасности, при чему служи и као образац или формула за израду безбедносних процена. Независно од епистемолошких домета

---

[2] Захваљујући научном и стручном ангажману наставника и сарадника Факултета безбедности, „науке безбедности“ су одлуком Националног савета за високо образовање признате као посебна *научна област* унутар научног поља „друштвено-хуманистичке науке“ (*Правилник о научним, уметничким, односно стручним областима у оквиру образовно-научних, односно образовно-уметничких поља*, 2019).

такве праксе, а посебно њене (зло)употребе којој су склони бројни самозвани „експерти“ на домаћој и међународној сцени,[3] извесно је да процена безбедносног ризика било ког предмета анализе (од сигурности појединаца, друштвених група и државе, до корпоративне, еколошке и међународне безбедности) не може бити валидна ако није плод дискурзивне анализе трансформације изазова у претњу. Сагледати, разумети, објаснити и проценити конкретни безбедносни ризик значи показати/приказати *када и у којој мери* нејасни друштвени изазов постаје отворена безбедносна претња. За тако нешто од суштинске је важности *познавати генезу идеолошких начела, мотива, интереса и делатне способности* непосредних друштвених и/или политичких актера да одржавају (оправдавају) или урушавају (негирају) постојећи друштвени поредак и своје место у њему. Утолико безбедносна анализа подразумева густо исткану појмовну мрежу, теоријску матрицу способну да у историјској перспективи препозна друштвене потребе, економске интересе и идеолошке мотиве политичких актера (организација и личности) да својим (не)чињењем конституишу безбедносни изазов и тако провоцирају настанак безбедносне претње.

*

Знање о актерима безбедносних ризика артикулише се одговарајућим концептом безбедности који нужно укључује одређене темељне вредности и/или циљеве: одржање, односно **опстанак** политичке заједнице,[4] њена *независност и самосталност*, односно **суверености**, и најзад успостављање унутрашње стабилности кроз институционализацију *слободе и једнакости,* дакле

[3] Слепо подражавање и некритичко преузимање туђих институционалних норми и „стандарда“ по правилу води у незнање и друштвено потчињавање чије епигонство стоји у директној супротности спрам прокламованих епистемолошких циљева и (не)изречених политичких императива.

[4] Данас се обично користи израз „одрживост заједнице“, што је директна последица идеологије глобализма која, не случајно, још увек доминира у појмовном језику друштвених наука. Термин се први пут појавио 1987. године у извештају под називом „Наша заједничка будућност“ коју је сачинила Светска комисија за животну средину и развој УН. Познат и као „Бруталанд извештај“ (према имену норвешке министарке која је била председник комисије), препун маркентишки стандардизованих „мисија“, „визија“ и „принципа“, речени извештај се залаже за пројектовање глобалног развоја који неће омести будуће генерације. Пре тога, у првом извештају транснационалне невладине организације Римски клуб („Границе раста”, 1972) коришћен је сличан, али мање политизован термин „глобална равнотежа“. Концептуални, битно утопистички смисао обе појмовне синтагме јесте обезбеђивање уравнотеженог развоја „еко/био“ и „техно“ сфере. Конкретна имплементација таквог концепта предмет је бројних контроверзи које не долазе из сфере привреде, већ из сфере идеологије, унутрашње и посебно међународне политике.

правичност.[5] Историјска посредовања унутар датог појмовног троугла (опстанак – сувереност – правичност) обележена су градњом или урушавањем друштвених хијерархија и политичких институција које обликују самопоимање и усмеравају деловање друштвених актера. Безбедност се утолико показује као искон и исходиште политичког живота који чини огледало историјског смисла појединачног и заједничког живота. Зато је свако методолошко занемаривање историјског контекста, поготово ако инсистира на раздвајању безбедности друштва/државе од безбедности појединца/грађана, сигуран пут у „експертски" фах-идиотизам и могућу идеолошку затуцаност препуну црно-белих представа о свету (Цветковић, 2010, стр.11–13).

Како год, као почетни услов разумевања и успостављања безбедности, *концепт опстанка* (преживљавања) везан је уз стриктно политичка или културолошка значења различитих форми, субјеката и идеала политичке заједнице. У том видокругу постављају се питања о преживљавању краљевства, царства, вере и народа (кључне референтне тачке у предмодерним политичким заједницама), односно државе, нације, цивилизације (тако у модерним политичким заједницама). Најзад, такорећи недавно, захваљујући пузајућем развоју идеологије глобализма, опстанак је добио и своју „онтолошку", тј. *еколошку* димензију, изједначивши се са наизглед идеолошки неутралном „зеленом причом" о одржавању животне средине и обуздавању индустријског развоја. Настала током прве велике привредне кризе за време Хладног рата (руинирање нафтног тржишта и настанак петродолара у раним седамдесетим годинама прошлог века), дата идеолошка приповест доживљава свој преображај у потоњем таласу неолиберализма када губи свој дотадашњи фокус (критика глобалног корпоративног система) и постаје маркетиншка алатка високе политике у служби финансијског капитала.[6] У XXI веку „зелена агенда" се обогаћује додатним

[5] Све донедавно (крај 20. века) концепт једнакости је подразумевао политичку и (делимичну) економску равноправност људи (грађана, држављана), да би она последњих година, првенствено на „колективном Западу" (САД, Канада, ЕУ, Аустралија и Нови Зеланд), била замењена наративом о родној и/или сексуалној „недискриминацији". Первертирана значења једнакости и (не)дискриминације свој корен имају у неолибералној идеологији глобализма која пуне две деценије континуирано ради на томе да традиционална значења слободе и једнакости измести из изворне економско-политичке димензије у трансформисану родно-сексуалну идеолошку раван.

[6] Најбољи пример: председничка кампања Ал Гора, кандидата Демократске странке на изборима у САД (2000. године). За свој горљиви еколошки активизам, посебно у вези са климатским променама, Гор (потпредседник САД у време бомбардовања Србије и Црне Горе; оснивач и сувласник инвестиционог фонда у Лондону, члан Управног одбора у

идеолошким наративом о постиндустријском друштву које креира нову (виртуелну) стварност и нова друштвена „правила“ глобалне контроле и надзирања становништва, укључујући и подразумевајуће ограничавање природног прираштаја човечанства.[7] Тако је „опстанак“ постао синоним за „преживљавање“, истина не свих, већ оних који знају, могу и хоће да се прилагоде новим безбедносним изазовима.

Нема сумње да је опстанак у основи сваке безбедности (Савић, 2010). Међутим, опстанак политичке заједнице сам по себи мало или ништа не значи. За модерну политичку заједницу (државу), баш као и за појединца (грађанина) релевантан је само „достојанствени опстанак“, онај који даје *смисао* индивидуалној и колективној егзистенцији. Опстанак лишен достојанства, „пуко преживљавање“ или „голи живот“, обесмишљава чак и саму безбедност која јесте нужан, али не и довољан разлог живота. Као и све друге самодовољне ствари из домена људске егзистенције, тако је и некаква самодовољна „безбедност“ не само мањкава (и као таква погрешна) већ и немогућа. Разуме се, у појединим ванредним и/или граничним егзистенцијалним ситуацијама (за појединце и заједницу) живот сам по себи јесте вредност, но то бива само тренутно, тј. у ограниченом (кратком) времену. Самодовољно биолошко трајање, живот као такав – без садржаја слободе и правде, горка је мука и терет на ивици подношљивог. Зато су колективна и индивидуална сувереност истинске мере достојанствености, правде и/или правичне безбедности појединаца и политичких заједница. У том контексту чак је и мање важно о ком концепту достојанствености, тј. правде и правичности, аутономије и независности је реч, битно је да он као такав постоји и да обезбеђује вредност (значење) појединачном (личном) и заједничком (политичком) животу. Безбедност појединца незамислива је без безбедности заједнице, баш као што је независност појединца аналогна суверености политичке заједнице у којој обитује,

Еплу (*Apple*), саветник у Гуглу (*Google*) итд.) добио је 2007. године Нобелову награду за мир (?!).

[7] У том духу треба разумети и промене друштвеног ангажмана „зелених активиста“: од ад хок организованих антимилитаристичких покрета против постављања америчких стратешких ракета у Европи (велики и дуготрајни протести у Великој Британији, Немачкој итд.) и група радикалних ентузијаста (попут *Green peace* који пресрећу танкере), активиста „цивилног друштва“ у земљама Варшавског блока и Југославији (и др.), све до формирања класичних политичких партија које временом постају део етаблиране политичке елите у којој се истичу својим праведничким гневом због постојања „ауторитарних поредака“ у свету. На том таласу некадашњи радикални антимилитаристи (најбољи пример: Зелена партија у Немачкој) постају одушевљени ратници за „праву ствар“, независно од стварних, дословно разорних последица свог одушевљеног активизма.

при чему су обе аутономије директно везане уз историјско наслеђе и/или традицију, тј. поступно обликовање представа, идеја, мњења и концепата о томе како и зашто ваља живети.

Исто важи и за *концепт праведности*. Његове предмодерне варијанте су традиционално биле саздана на идеји да свако ради оно што најбоље зна, односно оно што му „по природи припада“. Утолико су предмодерне политичке заједнице почивале на природним постулатима и јасно подељеним улогама: владари воде/управљају, ратници чувају/нападају, свештеници усмеравају, док сви други раде/производе. Тако устројена заједница обезбеђује прихватање и упражњавање опште прихваћених вредности као што су разборитост, храброст, мудрост и вредноћа (трудољубивост). Због тога су фактички све предмодерне политичке заједнице истовремено *штитиле* и *васпитавале* своје чланове. Насупрот томе, модерне политичке заједнице (државе) начелно не васпитавају, већ само бране своје чланове, а посебно су посвећене специфичном *надгледању*, односно *дисциплиновању* грађана ради њихове заједничке безбедности. Зато се начелно у либерализму, основном модерном идеолошком концепту који је изнедрио националну државу, обично не подстиче развој конкретних, циљаних вредности (свако такво прописивање се избегава или изричито забрањује), већ се принципијелно инсистира на поштовању правних *процедура* које обезбеђују правичност у виду коришћења људских права и слобода у широком, практично неограниченом опсегу те речи.

Да би се досегла жељена „вредносно-неутрална“ позиција државе, она начелно мора имати своју суверености која, да би уопште постојала, мора бити реципрочна – не сме угрожавати друге, такође суверене државе које имају принципијелно једнака права на независност свог унутрашњег поретка и исте обавезе спрам незадирања у туђу сувереност. Утолико *концепт суверености* подразумева да је свака држава свој властити господар: *успостављање правде и правичности (као одржавање легитимности поретка) директно је повезано са одбраном од напада непријатеља (обезбеђивање од спољних опасности)*. Одбрана од спољних опасности (војна инвазија, економска окупација и сл.) пре или касније ће нестати или посустати ако нема унутрашње стабилности (правичности) и *vice versa* (Цветковић, 2020).

Подразумева се да идеални баланс унутрашњих обавеза (политичка стабилност) и спољашњих дужности (безбедност) није лако остварив, ако је уопште и могућ, с обзиром на то да у међународним и унутрашњим односима свагда постоји напетост која нагриза безбедност државе. То важи за све идеолошко-политичке облике које модерне државе добијају у зависности од историјских околности. Због тога било која либерална држава, упркос слободарској реторици и претпостављеној правној уређености, на искуственом нивоу нема нити може имати обезбеђено првенство или вођство у односу на све друге, чак и оне

тоталитарне. Државе које се упркос свему намећу другима као самозвани лидери (слободног или неког другог света) пре или касније постаће агресори. Директна војна „интервенција", „кампања" или „операција" нужно провоцира сличан насилан одговор. Отуда и све могуће врсте тињајућих сукоба и отворених конфронтација између суверених држава чије оправдање функционише само као мање или више добро обликовани софизам воље за моћ. Идеолошко легитимисање међудржавних сукоба прикрива стварне разлоге (мотиве) сукобљавања *унутар* и *између* политичких заједница, а они су стари колико и сама цивилизација: господарити људима и располагати природним и друштвеним богатствима – свим средствима и у сваком тренутку.

* * *

Уколико се руководимо наведеним начелним полазиштима, највећи безбедносни изазови у Србији, од којих многи већ јесу или ће ускоро постати безбедносна претња, званично се своде на следеће конкретне теме или области: прво и основно – „*сецесија Косова"*, затим „*тероризам, сепаратизам, национални и верски екстремизам*", баш као и „*организовани криминал, хемијске, биолошке, нуклеарне диверзије, елементарне непогоде, техничке и технолошке несреће и сајбер диверзије*".[8] Тако бар, с већим или мањим оправдањем, несистематично и недиференцирано стоји у *Стратегији одбране Републике Србије,* домаћем кровном безбедносном програмском документу који је усвојен још давне 2009. године. У међувремену, међународни контекст и домаће безбедносне (не)прилике значајно су се променили и сада је у најмању руку потребно преиспитати наведени и друге документе којима се институционално регулише безбедност Србије.[9]

---

[8] Види: 2. Изазови, ризици и претње одбрани Републике Србије. У: *Стратегија одбране Републике Србије* (2009). Поред наведених изазова, *Стратегија* препознаје и друге врсте ризика и/или претњи, као што су „транзициони проблеми, обавештајна делатност и злоупотреба научних достигнућа у областима генетског инжењеринга, медицине, метеорологије и другим областима", при чему се констатује да се сваки од њих појављује „са различитом вероватноћом препознавања и испољавања".Симптоматично је да се овде, као и у многим другим документима (али и стручној литератури), појмовно бркају и неутешно преплићу „изазови", „ризици" и „претње". Више о академским разлозима и посредно конкретним (политичким) последицама дате конфузије види *Ризик, моћ и заштита – Увођење у науке безбедности* (2010) и *Науке безбедности – Врсте и облици* (2020).

[9] У том смислу су одређени помаци већ учињени 2021. год. доношењем стратешких докумената из области јавне безбедности: *Стратешка процена јавне безбедности* и *Стратешки план полиције за период од 2022. до 2025*. Овом приликом остављамо по страни емпиријски много пута потврђену чињеницу да стратешки документи у Србији, за разлику од сличних програмских аката „озбиљних држава", нису праћени

Не улазећи у домен ревизије наведених приоритета званичне безбедносне политике (они се по природи ствари мењају у складу са променама у међународној политици, унутрашњим друштвеним односима и иновацијама у технологији), поврх хроничне и акутне косовске кризе која представља недвосмислену претњу безбедности Србије (и то у све три димензије безбедности: достојанствени опстанак, спољашња независност и унутрашња правичност), постоји још читав низ других, можда само за нијансу мање значајних безбедносних проблема са којима се Србија суочава. Између осталих, издвајамо три веће, сложене и релативно независне групе чији су „изазови“ већ увелико досегли статус „претњи“, односно ризика које ваља појмовно обликовати/разумети, тј. одредити и континуирано пратити индикаторе, проценити штету и најзад – решавати:

1. *Крхкост критичне инфраструктуре*, посебно јавних институција (сајбер безбедност, употреба вештачке интелигенције и др.);
2. *Демографски дефицит* (опустошени географски простори и пренапуњеност градова; избеглице и илегалне миграције);
3. *Идентитетска претња* (угрожавање културног и/или националног идентитета).

Прве две групе изазова (инфраструктура и демографија) подлежу емпиријском праћењу које подразумева израду одговарајућих (конкретних) показатеља (индикатора) помоћу којих се могу мерити ризици, уочавати тенденције и креирати делотворни протокол безбедности, док трећи изазов (национални идентитет) пребива првенствено у флуидној идеолошкој сфери која измиче прецизнијем одређивању степена безбедносног ризика. У датом контексту за процену ризика не постоје довољно јасна мерила за мерење степена угрожености с обзиром на то да се проблеми идентитета, у зависности од идеолошке призме политичких актера, *минимизирају* (неолиберали, социјалдемократе, „зелени“, „глобалисти“ и други) или пак *предимензионирају* (конзервативци, комунисти, „антиглобалисти“, национални либерали итд.). Међутим, управо наведени изазов и/или претња може бити и најчешће *јесте* одлучујући фактор који утиче на тоталитет (не)безбедности државе/друштва.

оперативним „акционим плановима“ или „агендама“. Штавише, њихова имплементација препуштена је случају и импровизацијама који поништавају сврху усвајања докумената. Уместо да буду спискови проблема, стратешки документи би требало да буду практични оријентири, стручни водич и обавезујуће упутство за рад надлежним државним органима, агенцијама и организацијама које о свом (не)чињењу подносе извештаје Влади Републике Србије и формалном извориштy државне суверености – Народној скупштини.

Од идеолошке визуре политичких актера и политичког концепта државе зависи шта ће се препознати као „безбедносни проблем“ (изазов или претња) у сфери идентитета, а шта као могућа „злоупотреба“, „прекорачење овлашћења“, незаконито залажење у домен људских права итд. Због тога је теоријски тешко артикулисати конзистентан појам „идентитетске претње“ и изградити транспарентан и од свих (или бар већине) актера у јавном простору прихваћен систем праћења ризика, односно контроле штете у датој области.

У сфери демографског дефицита и проблема миграција ствари стоје кудикамо другачије. Међутим, оно што је за једне друштвене или политичке актере реална претња њиховом друштвеном положају, развоју или чак постојању – масовне миграције страног становништва и додатно стварање конкуренције на домаћем тржишту рада (обарање цене надница), други тумаче као цивилизацијску благодет („мешање култура“ и „космополитизам“ за либералне идеологе) и као (не)очекивану пословну прилику која обећава ниске цене рада и услуга, већи профит и посредни друштвени просперитет за све, укључујући и тренутне „губитнике“ (за велике предузетнике и корпорације). На овом другом полу рецепције миграције су, такорећи до јуче, почивали бројни панегерици економској и свакој другој врсти глобализације (Хофбауер, 2020).[10]

Како год, у разлици перцепције безбедносног изазова и/или претње не одражава се само различито виђење друштвених добитака од стране друштвених актера унутар исте политичке заједнице већ и оно одлучујуће – разлика у третирању правде или аутономије унутар локалног и глобалног поретка. Да би се речени појмови, процеси и циљеви уравнотежили (хармонизовали), потребно је успоставити одговарајућу институционалну подршку за стабилност, односно безбедност државе.

Заштита критичке инфраструктуре првог реда (енергетски и саобраћајни системи, водоснабдевање и др.) по дефиницији спада у безбедносне приоритете сваке

[10] Тако се већ на датом примеру може видети да не постоји сигурност у рефлексији, а још мање у рецепцији друштвених процеса: када и ако миграције наруше равнотежу понуде и потражње на локалном тржишту рада, што неизоставно доводи до масовног политичког незадовољства, они који су у почетку имали недвосмислену тренутну корист од миграција и јефтиније радне снаге могу постати огорчени противници миграције јер их виде као стратешку претњу својој политичкој позицији. Новостворено незадовољство дојучерашњих „корисника глобализације“ постаће окидач за друштвене немире које ће они предводити заједно са истим оним конзервативним и/или националним „губитницима“ чија се друштвена позиција није мењала. Из тог (не)очекиваног политичког споја економских губитника и политичких конформиста обично настају политички пореци који слабе друштво угрожавајући његову увек крхку правичност, баш као и никад стабилни међународни поредак.

државе.[11] Данас готови сваки грађанин Србије има одређену представу о томе шта значи „избрисати на клик“ (раније се говорило „на дугме“) рад електроенергетског или неког другог јавног система (саобраћај, војска, полиција...), као и то шта значи „крађа идентитета“, проваљивање лозинке банковног рачуна и сл. Исто тако, још од раније постоји општа, магловита и (често неоправдано) подсмешљива представа о томе шта је „специјални рат“, „непријатељска делатност“ и слично, што је данас употпуњено модификованим верзијама као што су „хибридни рат“ или „сајбер ратовање“, чија софистицираност донекле превазилази сировост негдашње црно-беле пропаганде из времена Хладног рата.[12] С друге стране, мало ко – осим, наравно, непосредно заинтересованих – размишља о базама података у здравственим, образовним, еколошким или културним институцијама и сл. Најзад, ретко ко ће се се запитати о манипулацијама у вези са историјским памћењем, лажном обликовању (или поништавању) националног саморазумевања и сл.

*

Најмање отпорна критична инфраструктура – *јавне институције у образовању, здравству, правосуђу* итд., које су изложене сталним сајбер нападима и лажним узбуњивањима преко телефона и електронске поште (дојаве о постављању бомби и сл.), да и не говоримо о крађи личних података (посебно њиховом чувању), још увек немају изграђену системску безбедност, односно заштићеност која би била примерена изазовима времена. Безбедносна рањивост јавних институција односи се колико на информатичку, толико и на физичко-техничку заштиту. Утолико је дигитализацијска израда симулација различитих врста напада на јавне институције и сценарија за њихову одбрану међу примарним, дугорочним задацима Националног симулационог центра за процену безбедносних ризика. У том смислу, између осталог, потребно је израдити дигиталне мапе образовних, здравствених и правосудних установа, заједно са базама података о пријављеним инцидентима који би се класификовали на одговарајући начин (од пријаве бомби, крађа и других врста насиља до различитих инцидената у којима су учествовали запослени). На основу тога могу се анализирати последице таквих аката,

[11] Заштита од земљотреса, пожара, поплава или индустријских акцидената представља засебан безбедносни аспект који овом приликом не улази у домен нашег интересовања. Постојећа правна нормативна по том питању и њена примена чине целовит скуп норми и поступака који се могу истраживати коришћењем софтверских програма који постоје у Националном симулационом центру за процену безбедносних ризика на Факултету безбедности.

[12] Актуелни сукоб „колективног Запада“ са Русијом показује да је црно-бели свет пропаганде и даље делотворан, па чак и милитантнији но што је био онај у коме су се отворено сукобљавале „само идеологије“, не и националне државе.

материјалне и друштвене последице, заједно са иновацијама у системима узбуњивања и контроле штете. Скупа узев, на основу датих анализа и показатеља могуће је разрадити одговарајуће протоколе за процену безбедносних ризика, подједнако корисне за истраживаче, колико и за надлежне безбедносне институције.

Исто важи и за праћење *миграционих токова* у Србији – како оних који се односе на кретање домицилног становништва, тако и оних који су везани за масовни прилив избеглица из иностранства, посебно оних који спадају у организоване илегалне миграције. Према већини релевантних економских, социолошких и геополитичких истраживања у наредним деценијама се очекују нови, велики таласи избеглица из ратовима опустошених зона Африке, Блиског истока, Централне Азије и Украјине, при чему ће многи мигранти не само пролазити већ и остајати у Србији. Висока просечна старост становништва и недостатак радне снаге није проблем само Западне Европе већ и слабо развијених земаља ЕУ које се никада раније у својој историји нису суочавале са сличним проблемима. Процене демографских кретања унутар и око Србије, посебно имајући у виду потенцијале и стратегије њеног насељавања, од приоритетне су важности по њену безбедност (опстанак, сувереност и стабилност), што би по дефиницији морало бити предмет рада Националног симулационог центра за процену безбедносних ризика.

Најзад, посебно деликатан, најмање уочљив, а заправо најважнији по својим карактеристикама и дугорочним последицама, јесте проблем који смо овде провизорно назвали *идентитетска претња*. Проблем нипошто није ексклузивно домаћи, а разумевање је крајње разнолико, чак и унутар истог (Хантингтон, 2008; Фукујама, 2022) или сличног контекста (Бродел, 2008). Србија и српски народ се са тим проблемом суочавају већ читав век и још увек нису сагледали његов друштвени оквир, политичка значења и последице (Цветковић, 1998). Методолошка израда „модела“ српског националног идентитета, попис листе индикатора, начина њиховог праћења и укрштања, сценарија угрожавања и одговора на њих – у Србији и изван ње, све је то захтеван и посебно осетљив предмет истраживања који заслужује своје емпиријско моделовање изван политичких прогласа, идеолошких заклињања и епских приповести. Зато би било корисно израдити профилисане дигиталне мапе Србије и окружења чијом интеракцијом би се могли правити различити сценарији за израду процене ризика од конкретних претњи (рат, тероризам и организовани криминал; индустријске и природне катастрофе; информациони рат итд.).[13]

[13] Примера ради: *Критична инфраструктура I* (привреда); *Критична инфраструктура II* (државне институције); *Критична инфраструктура III* (школе, болнице, цркве);

Контроверзни процеси привредне и политичке глобализације с једне, односно технолошки процеси и иновације у информационој сфери с друге стране, довели су у питање готово све модерне политичке форме оправдавања друштвено-политичког живота, а посебно концепте друштвене правде и државне и/или националне суверености. Од начина на који ће се они институционално (ре)конструисати зависи безбедност, односно опстанак свих политичких заједница у свету.

Библиографија

1. Brodel, F. (2010). Identitet Francuske (Prostor i istorija, ljudi i stvari). Podgorica: CID, Nikšić: Filozofski fakultet.
2. Volkan, V. D. (2018). Imigranti i izbeglice. Beograd: Clio.
3. Стратегија одбране Републике Србије. 2009. Приступљено 28.11.2022. https://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/strategije/Strategija%20odbrane%20Republike%20Srbije.pdf
4. Fukujama, F. (2022). Identitet (Zahtev za dostojanstvom i politika resantimana). Podgorica: CID.
5. Hantington, S. (2008). Američki identitet (Problem dezintegracije Amerike). Podgorica: SoCEN.
6. Hofbauer, H. (2020). Kritika migacija (Ko dobija a ko gubi). Beograd: Albatros plus.
7. Цветковић, В. Н. (2022). Васкрс историје (Идеолошке метаморфозе глобалног поретка). *Социолошки преглед*, 3-2022: 737–742.
8. Цветковић, В. Н. (2019). Државна сувереност и/или национална безбедност (екстерне и интерне функције концепта суверености). У: *Државни поредак (Суверенитет у времену глобализације)* (стр. 87–125). Београд: САНУ.
9. Цветковић, В. Н. (2020). Науке безбедности (Врсте и облици). Београд: Факултет безбедности.
10. Цветковић, В. Н. (2020). Науке безбедности – генеза и смисао. У: *Науке безбедности – Врсте и облици* (стр. 13–39). Београд: Факултет безбедности.Цветковић, В. Н. (2010). Ризик, моћ и заштита – Увођење у науке безбедности. Београд: Службени гласник и Факултет безбедности.
11. Цветковић, В. Н. (1998). Страх и понижење (Југословенски грађански рат и избеглице у Србији). Београд: ИЕС.

Ванредне ситуације I (клизишта, трустна подручја и сл.), *Ванредне ситуације II* (индустријске и саобраћајне хаварије и сл.) итд.

МЕТОДОЛОГИЈА ИЗРАДЕ СТРАТЕГИЈЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ РЕПУБЛИКЕ СРБИЈЕ – ДИЛЕМЕ И ПЕРСПЕКТИВЕ

Ненад Путник[1]

Апстракт

Најзначајнији ризици и изазови по безбедност држава, као и основни субјекти и мере за њихово спречавање, дефинишу се у стратешким безбедносним документима. Ови кровни документи данас су, чешће него у XX веку, подложни ревизијама, имајући у виду динамичност спољних и унутрашњих политичких, социоекономских и безбедносних односа и промена. У раду су анализиране националне безбедносне стратегије појединих земаља, ризици који су у њима представљени и динамика њихових ревизија. Такође, размотрена су и основна стратешка документа из области безбедности у Републици Србији и дате препоруке за њихову евентуалну ревизију или допуну, у односу на актуелне спољне и унутрашње изазове, и по узору на методологију израде безбедносних стратегија земаља чланица ЕУ.

Кључне речи: безбедност, стратегија националне безбедности, ризик, сајбер безбедност, ревизија.

Увод

Стратегија представља кровни документ који дефинише основне и одговорне актере, циљеве и елементе система за који се креира. Стратегије су кључни и основни документи које доносе како државни органи, тако и пословне институције, и оне представљају оквир за даље креирање и операционализацију

[1] Факултет безбедности, Универзитет у Београду, e-mail: nputnik@fb.bg.ac.rs

Рад је настао у оквиру пројекта Фонда за науку Републике Србије „Идеје“ – Пројекат акцелерације иновација и подстицања раста предузетништва у Републици Србији – Management of New Security Risks – Research and Simulation Development – NEWSIMR&D, #7749151.

планова и тактика. Оперативна ефикасност и стратегија су есенцијалне за најбоље перформансе што, у крајњој линији, и јесте основни циљ сваке организације (Porter, 1996, p. 61). Стратегија треба да на систематизован начин дефинише основне елементе система, њихове дужности и одговорности, изазове, потребе и ресурсе. Њихова операционализација доприноси планском, усмереном и ефикасном раду дефинисаних субјеката у односу на задате активности и циљеве. Опште узев, стратегије постављају циљеве и приоритете, дефинишу кључне активности и ресурсе за њихово извршавање и постизање.

Националне стратегије безбедности су кључни државни оквир за дефинисање безбедности и суочавање са основним безбедносним потребама државе и грађана, као и унутрашњим и спољним ризицима. Форма и сложеност националне стратегије безбедности различите су од државе до државе. Оне најкомплексније дефинишу:

- кључне државне органе у погледу остваривања безбедности;
- најважније националне интересе;
- садашње и будуће ризике и изазове;
- ресурсе и потребе;
- временски оквир за остварење циљева и
- начин процене ефикасности остварења.

Стратегије обично представљају документе који су основа за дефинисање и остварење средњорочних и дугорочних планова по питању националне безбедности. Стратегије су обликоване процесима путем којих настају (Cancian et al., 2017, IX). Добро формулисане и уобличене стратегије олакшавају доносиоцима одлука (политичких, економских, безбедносних и других) да сагледају ризике, постојеће ресурсе и предности, као и слабости и циљеве које треба постићи. Сам процес израде стратегије важан је колико и коначан документ – током израде стратегије обухватно се сагледавају све карактеристике и околности од локалног до глобалног нивоа, дефинишу се и рангирају ризици, приоритети, снаге и слабости, као и кључни актери за отклањање ризика и остварење циљева. Одлуке које креатори стратегија доносе одређују друге акте, али и саму операционализацију стратегија, најмање за средњорочни период. Роберт Гејтс (Robert Gates), амерички обавештајни аналитичар, рекао је да израда сваке стратегије траје месецима како би се осигурало да сваки релевантни чинилац владе и министарства одбране може дати свој суд још током нацрта (Gates, 2014, p. 144). Стратешки документи морају децидно навести безбедносне приоритете државе, уз то образлажући зашто су неке активности и потребни ресурси приоритет у односу на друге. Стога не чуди зашто поједини аутори, попут Канциана и сарадника (Cancian et al.), процес израде стратегије описују као сложен и конфликтан (XI). С обзиром на сложеност и значај и израде и стратегије

као крајњег документа, поставља се питање оптималног методолошког приступа овом процесу. Такав приступ би требало да пружи одговор на следећа питања:

- Ко треба да организује и надзире израду?
- Да ли на стратегији треба да ради мања или већа група људи?
- Како ускладити цивилну и војну перспективу? (Canciat et al., 2017, p. 6)
- Колики домет стратегија треба да има, колико далеко „гледати у будућност“?
- Коју методологију процене и приоритизације ризика применити?
- На који начин ће се вршити евалуација примене стратегије?

С обзиром на динамичност геополитичких односа и разноврсност ризика, стратегија мора бити подложна ревизији. Њена обухватност и актуелност биће већа уколико на њеној изради раде стручњаци различитих научних дисциплина и практичног искуства. Јасност и прецизност стратегије олакшава доносиоцима политичких одлука да своје деловање усмеравају на начин који ће обезбедити стабилност земље и сигурност њених грађана.

Изазови са којима се суочавамо, нарочито у последње две деценије, показују нам да је тешко предвидети све ризике, чак и најозбиљније, и да национална безбедност и грађани могу бити изложени потпуно изненадним и непредвидивим изазовима – попут природних катастрофа, појава пандемија, наглих глобалних економских поремећаја, развоја и све веће злоупотребе сајбер простора и слично. Тиме су и стратегије националне безбедности документи који апсолутно морају бити подвргавани анализи и ревизији, у складу са динамичним међународним геополитичким односима, али и опасностима које, чини се, брзо и изнова попримају нове појавне облике или методе деловања, како би „заобишле“ или неутралисале постојеће мере заштите.

Кратак осврт на различите стратегије националне безбедности

Кључне циљеве једне земље, али истовремено и ризике са којима се може суочити, одређују како тренутно дефинисани, тако и геополитички односи из прошлости, политичко уређење, географски положај, број и структура становништва, економија, постојање и квалитет природних ресурса, припадност неком политичком или војно-политичком савезу, али и карактер социјеталне безбедности, разноврсност и стопа криминала, а са друге стране организованост и стабилност кључних институција у држави и друштву. У овом делу рада биће приказане кључне карактеристике националних стратегија безбедности земаља које се сматрају политички, војно и/или економски најмоћнијима у свету.

Свакако да су велики светски догађаји утицали и чак били прекретница у доношењу или измени националних стратегија безбедности. Тридесетих година XX века, па и током већег дела Другог светског рата, доктрина САД заснивала се

на својеврсном изолационизму. Политику суздржавања промовисао је Џорџ Ф. Кенан (George F. Kennan). Његово гледиште било је да се политичким проблемима треба приступити са економског становишта, избегавајући војну силу (Romano, 2011). Велику промену представљала је такозвана Труманова доктрина, која је националну безбедност директно повезала са питањем демократије, када већ постаје јасно да СССР и уопште социјалистички уређене земље постају главни ризик, коме ће се САД супротставити и војно, ако је потребно: „Не подржавамо агресију ниједне земље, али ћемо им помоћи да се бране, ако буду нападнуте“ (Truman Doctrine, 1947). Актом Националне безбедности из 1947. креирано је Министарство одбране које је заменило Министарство рата, а које је обухватило и Морнарицу. Осим тога, створен је и Савет за Националну безбедност који је саветовао председника и Централну обавештајну службу – CIA (Norton et al., 1999, p. 555). Парафразирајући Чомског, може се рећи да је спољна политика САД тада униформисана и да је свака војна интервенција имала политички легитимитет. Нови велики преокрет у безбедносној стратегији САД био је терористички напад 11. септембра 2001. године. Тероризам постаје главна претња, а терористи главни непријатељи, према којима се мора повести тотални рат који ни просторно, ни временски није дефинисан и ограничен (Romano, 2011). Најновије измене, из 2022. године, настале су услед кризе коју је произвео конфликт између Русије и Украјине. Министарство одбране је у Националну стратегију безбедности инкорпорирало Преглед нуклеарног стања (у даљем тексту NPR) и Преглед одбрамбених ракета (у даљем тексту MDR). Као главни изазови безбедности истакнуте су намере Русије према Европи и активности Народне Републике Кине.

Европску стратегију безбедности (у даљем тексту ESS) донео је 2003. године Савет Европе, а њена анализа извршена је 2009. године. У анализи се наводи да су кључне претње по ЕУ и даље остале исте, као и 2003. године, а то су:

- пролиферација оружја за масовно уништење;
- енергетска ефикасност;
- климатске промене;
- тероризам и организовани криминал, којима је у овом документу придодата и претња по сајбер безбедност, са образложењем да напади на приватне или државне ІКТ системе дају нову димензију, као потенцијално ново економско, политичко и војно оружје (ESS, 2009, стр. 13).

У стратегији се наводи да се 20 година након Хладног рата Европа суочава са растућим и комплексним претњама и изазовима, а сарадња свих чланица, као и међународна кооперација, представљају окосницу безбедносне политике и одржања мира. Посматрајући процес интеграција као водећу силу у обезбеђивању мира и просперитета у Европи, ESS је поставила контуре уверења у „стабилност кроз сарадњу“ (Berenskoetter, 2005, p. 77). Европска стратегија безбедности из

2009. године ставља акценат на постојање регионалних конфликата и ирански нуклеарни програм, као нарастајућих ризика. Као кључна, истиче се сарадња са НАТО-ом, а у стратегији се наводи да Европска унија (у даљем тексту ЕУ) мора подржавати Уједињене нације (у даљем тексту УН) у њиховим одговорима на претње по међународни мир и безбедност (ESS, 2009, стр. 40).

Европска стратегија безбедности је 2016. године замењена Глобалном стратегијом спољне и политике безбедности ЕУ, скраћено ЕУ Глобална стратегија (у даљем тексту EUGS). Циљ доношења EUGS било је побољшање ефикасности одбране и заштите ЕУ и њених чланица. На основу ове стратегије, створена је Перманентна структурна кооперација у одбрани (у даљем тексту PESCO), где се 25 земаља чланица сагласило да уједини снаге на заједничким програмима како би се креирале трупе и ресурси за заједничке мисије. Како се наводи, добар пример активности ЕУ јесте милитарна мобилност унутар ЕУ и спровођење PESCO пројеката (EUGS, 2018, стр. 06). У EUGS се наводе исти ризици као и у претходним ESS, уз нагласак да ће ЕУ убрзати рад у области сајбер безбедности.

Уједињено Краљевство (у даљем тексту УК) је 1998. године донело своју прву Националну стратегију безбедности (у даљем тексту NSS), која је доживела многе ревизије, а последњу 2015. године, под називом *National Security Strategy and Strategic Defence and Security Review*. Анализирајући NSS и њене бројне ревизије, аутори Хамерстад и Боаз истичу да се већа пажња поклања изазовима попут климатских промена, пандемија и миграција, уместо ризика попут тероризма и организованог криминала, који се већ остварују и остављају последице (Hammerstad & Boas, 2014, стр. 481). Овакав приступ је у значајнијој мери измењен ревизијом из 2015. године. Још у уводном делу овог документа наводи се да је јака економија кључ безбедности УК. Економска безбедност иде руку под руку са националном безбедношћу (NSS, 2015, стр. 9). Као кључне актере и активности у обезбеђивању одбране, ова стратегија наводи: војне снаге, обавештајне службе, дипломатију, сарадњу са НАТО-ом и јаку владавину права. Као кључни ризици наведени су: тероризам и екстремизам, где је нарочито истакнут тероризам који потиче из Северне Ирске, затим сајбер претње, кршење људских права у свету, регионални конфликти и ризици по економски просперитет.

Последњом Стратегијом националне безбедности, донетом 2021. године, Русија је истакла да себе види као независног актера на међународној сцени и за разлику од претходних стратегија много оштрије упућује на друге државе и савезе као непријатељске. У својој анализи, Мајкл Дуклос (Michel Duclos), искусни дипломата и сада саветник института Монтана, истиче да нова руска стратегија најављује заоштравање на свим пољима и даљу конфронтацију са Западом. Као основни ризици наведене су намере спољних актера да подстицањем тероризма и

екстремизма у Русији изазову њену нестабилност. Климатске промене су наведене као активна претња којој се треба посветити. Енергенти су једна од окосница економске и безбедносне позиције Русије. С обзиром на то да у стратегији Русија наводи своје планове везане за истраживања и експлоатације и на Арктику и на Антарктику, не чуди чињеница да је посебна пажња посвећена климатским променама. Неколико официјелних докумената Русије сведочи о еволуцији у званичном размишљању о климатским променама (Godzimirski, 2022). Још једна посебно истакнута кључна опасност јесу сајбер ризици и главни изазов је очување информационе безбедности. У складу са тим, стратегијом се предвиђа стварање сувереног сегмента интернета, системски развој националних технологија и успостављање снага за информациону конфронтацију.

Кина је 2019. године донела такозвану Белу књигу одбране, коју Ентони Х. Кордесман (Anthony H. Cordesman), емеритус Центра за стратешке и међународне студије (CSiS), види пре свега као одговор на стратегије САД. Кинески стратези опасност виде у предоминантној позицији Сједињених Држава у интернационалном систему (Bolt and Gray, 2007, p. 2). Као претња, у кинеској Белој књизи наводе се и Тајван, Тибет и Туркистан због свог сепаратизма. Своју војску Кина дефинише као одбрамбену, а као основну претњу по стабилност војног система наводи технологије које омогућавају сајбер нападе. Војна стратегија Кине назначује да је оспособљеност у сајбер сфери оно у шта Народноослободилачка армија (PLA) треба да инвестира и да обилато користи (Magnus, 2011, p. 4).

Национална стратегија безбедности Републике Србије

Народна скупштина Републике Србије донела је до сада две националне стратегије безбедности, обе за десетогодишњи период. Прва је донета 2009, а друга 2019. године. Обе стратегије у уводном делу наводе привржености Републике Србије очувању мира демократији, владавини људских права, као и то да је тај документ полазна основа за израду других стратешких и доктринарних докумената и јавних политика.

Разлике у опису стратегијског окружења готово и да нема у обе стратегије. Констатује се да се политички, економски, културни и безбедносни односи у свету одвијају у глобалном мултиполарном и мултилатералном окружењу у коме се све наглашеније испољава уравнотежење моћи и сложена међузависност држава (Стратегија националне безбедности Републике Србије[2]). Наводи се да ризици и претње на глобалном нивоу проистичу из неравномерног економског и културног развоја. Као најважније претње миру на свим нивоима у стратегијама

[2] „Службени гласник РС“ 88/2009/ и 94/2019.

наведени су регионални и локални сукоби, етнички и верски екстремизам, тероризам, организовани криминал, пролиферација оружја за масовно уништавање, илегалне миграције, хибридне претње, сајбер претње, ограничена расположивост природних ресурса (укључујући воду, храну, енергенте и сировине), као и промена климе и деградација природне околине. Ове претње угрожавају стабилност појединих држава и читавих региона, као и глобалну безбедност (Стратегија националне безбедности Републике Србије, 2019).

Национална стратегија безбедности из 2009. године на следећи начин рангира најважније ризике и претње:

- опасност од оружане агресије на Републику Србију;
- сепаратистичке тежње појединих националистичких и верских екстремистичких група;
- противправно једнострано проглашена независност Косова;
- оружана побуна;
- тероризам;
- пролиферација оружја за масовно уништење;
- национални и верски екстремизам;
- обавештајна делатност;
- организовани криминал;
- корупција;
- проблеми економског развоја;
- енергетска међузависност и осетљивост инфраструктуре;
- неравномеран привредни и демографски развој Републике Србије;
- нерешен статус и тежак положај избеглих, прогнаних и интерно расељених лица;
- недовршен процес разграничења између држава некадашње СФРЈ;
- неконтролисано трошење природних ресурса и угрожавање животне средине;
- последице елементарних непогода и техничких и технолошких несрећа;
- опасности повезане са појављивањем и ширењем инфективних болести;
- наркоманија;
- деструктивно деловање појединих верских секти и култова;
- ризик од високотехнолошког криминала;
- промена климе на глобалном нивоу.

У односу на ову, Стратегија националне безбедности из 2019. године доноси незнатне промене у навођењу ризика и прењи – са листе су изостали корупција, нерешен статус избеглих, прогнаних и расељених лица и деструктивно деловање појединих верских секти, а наркоманија је заузела вишу позицију у рангирању:

- оружана агресија на Републику Србију;
- сепаратистичке тежње;

- противправно једнострано проглашена независност територије коју административно обухвата Аутономна Покрајина Косово и Метохија;
- оружана побуна;
- тероризам;
- пролиферација оружја за масовно уништење;
- етнички и верски екстремизам;
- обавештајна делатност иностраних служби;
- организовани криминал;
- наркоманија;
- масовне илегалне миграције;
- проблеми економског развоја;
- проблеми демографског развоја;
- епидемије и пандемије;
- енергетска безбедност;
- недовршен процес разграничења држава бивше СФРЈ;
- елементарне непогоде и техничко-технолошке несреће;
- климатске промене;
- високотехнолошки криминал.

Систем националне безбедности састоји се од управљачког и извршног дела, при чему управљачки део чине Народна скупштина, председник Републике, Влада и Савет за националну безбедност, док извршни део чине систем одбране, систем унутрашње безбедности, безбедносно-обавештајни систем и други субјекти значајни за националну безбедност (Стратегија националне безбедности Републике Србије, 2019).

Национална стратегија безбедности Републике Србије и претходно описане стратегије других земаља имају заједничке поједине ризике, попут тероризма, организованог криминала, климатских промена и непријатељског/обавештајног деловања других земаља. Република Србија оптерећена је нерешеним статусом њене покрајине Косово и Метохија, одакле проистичу значајни ризици који се у стратегији наводе. За разлику од безбедносних стратегија других држава, које истичу сајбер простор и сајбер безбедност као један од кључних стубова одбране и безбедности земље, Република Србија као ризик наводи високотехнолошки криминал, што је изазован, али по опсегу деловања и опису у стратегији, ужи појам.

Сајбер безбедност као савремени изазов

Већина земаља у свету препознала је сајбер опасности као изазов којем се, у безбедносном смислу, мора посебно посветити, а поједине земље (на државном, али чешће на приватном нивоу) већ и спроводе сајбер нападе засебно или као део хибридног ратовања. Сајбер простор је постао нова егзистенцијална димензија за појединце и друштва омогућивши им да приступе свету трансцеденталним путем

који пркоси физичким ограничењима времена и места (Song et al., 2021, p. 62). Сајбер простор је омогућио размену идеја, култура, предлога готово у реалном времену, али и ова, као и све друге иновације, са собом је донела и бројне ризике по појединце, групе, па и саме државе и њихове критичне инфраструктуре. Технологија наставља да игра значајну улогу у панорами глобалних ризика, јер је сфера која утиче на читаво друштво, које је окосница ове проблематике с обзиром на велики број жртава сајбер напада (Coller et al., 2020).

Сајбер простор, његове могућности и корисници учинили су да он постане ново, савремено, готово легитимно бојно поље. Актери претњи у новом амбијенту, сајбер простору, могу бити различити – државни, поддржавни и транснационални субјекти (Миљковић и Путник, 2016, стр. 164). Посебна специфичност лежи у чињеници да се са релативно малим улагањима и једном, једнократном акцијом (хакерски напад) противнику може нанети енормна економска, политичка и/или безбедносна штета. Данас је коришћење информационих и комуникационих технологија инкорпорирано у свакодневни живот нације. Ипак, са тиме долазе и озбиљни ризици и претње који могу погодити сајбер простор због његових рањивости (Santisteban and Andrade-Arenas, 2020, p. 771). Неспорна је чињеница да субјекти безбедности увек воде својеврсну трку са креирањем и иновирањем мера заштите сајбер простора, док нападачи, са друге стране, осмишљавају нове методе напада и њиховог неутралисања. Због свог карактера, последица које изазивају и конспиративности, сајбер напади све су чешћи метод неоружане борбе против непријатеља, било да је он дефинисан као конкурентска компанија, критична инфраструктура друге државе, њен државни орган или оружане снаге. У стратегијама сајбер безбедности појединих земаља, у делу у којем се наводи улога оружаних снага у остваривању способности сајбер одбране, јасно се наводи да оружане снаге морају да развијају капацитете за обавештајни рад, сајбер напад и сајбер одбрану (Миљковић и Путник, 2016, стр. 165). Сајбер напади и сајбер бојно поље постало је неизоставни део хибридних ратова, као најчешћи и један од најефикаснијих неоружаних напада на друштво и државу. Онлајн напади на Естонију и Грузију појачали су страх од сајбер тероризма, а сама чињеница да криминалци и шпијуни могу то исто учинити индиковала је улогу сајбер конфликата у међународним односима, укључујући и потенцијале сајбер дипломатије и сајбер рата (Barnard-Wills and Ashenden, 2012, p. 110). Већ деценију уназад оваква врста рата води се међу најразвијенијим и највећим силама света, пре свега између САД и Кине, а вишегодишњи конфликт између Русије и Украјине обележен је управо вођењем хибридног рата, са нагласком на сајбер нападе. Стога не чуди да је влада Уједињеног Краљевства 2010. године Стратегијом сајбер безбедности успоставила две владине агенције за сајбер безбедност, док су САД 2009. године именовале координатора за сајбер безбедност и навеле да је сајбер безбедност експлицитни део политике

националне безбедности (Barnard-Wills and Ashenden, 2012, p. 111). Данас готово све велике земље имају посебну стратегију сајбер безбедности, која је једнако важан акт као и стратегија националне безбедности. Три значајна догађаја, у последњих десет година, убрзала су процесе креирања стратегија сајбер безбедности (Tatar et al., 2014). Првим догађајем који је „упалио аларм“ сматра се сајбер напад на интернет инфраструктуру Естоније 2007. године. Затим, 2008. године током конфликта између Русије и Грузије у Јужној Осетији, сајбер напади изведени су пре самих оружаних напада (Tatar et al., 2014). Као најзначајнији, сматра се сајбер напад Стакснет црвом 2010. године, који је циљао нуклеарну инфраструктуру Ирана. Осим доношења својих националних стратегија, државе су убрзале и оперативне припреме како за заштиту свог сегмента сајбер простора, тако и за напад на туђе. Стратегијом сајбер безбедности Уједињеног Краљевства дефинисано је постојање Канцеларије за сајбер безбедност, која је задужена за стратешка питања, док Центар за операције у сајбер простору врши мониторинг сајбер простора, координише у случају инцидената и има саветодавну улогу. Бивши премијер Гордон Браун (Gordon Brown) изјавио је: „Како смо у XIX веку морали да осигуравамо мора због националне безбедности и просперитета, у XX веку смо морали да осигуравамо ваздушни простор, у XXI веку морамо осигурати нашу позицију у сајбер простору, како би нашим људима и пословној сфери пружили поузданост да безбедно бораве у том простору“ (Barnard-Wills and Ashenden, 2012, p. 112). Администрација бившег председника САД Барака Обаме (Barack Obama) истакла је да ће дигиталну инфраструктуру третирати као стратешки приоритет националне безбедности. Сајбер безбедност идентификована је као један од најозбиљнијих изазова по економију и националну безбедност са којом се нација суочава (Barnard-Wills and Ashenden, 2012, p. 112). Одбрана сајбер простора постала је главна брига светских лидера (ALDaajeh et al., 2022, p. 2). Анализирајући стратегије сајбер одбране САД, Француске, Холандије, Немачке и Турске, Татар и сарадници (2014) истакли су следеће основне елементе које сваки од ових докумената садржи, а то су: 1) војне сајбер операције, 2) борба против сајбер криминала, 3) обавештајни и контраобавештајни рад, 4) кризни менаџмент сајбер безбедности и критичних инфраструткура и 5) сајбер дипломатија (стр. 211).

Република Србија је 2017. године донела Стратегију развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године.[3] Као један од разлога за доношење овакве стратегије, поред већ поменутог сајбер напада на Естонију, аутори наводе и да, према подацима Министарства унутрашњих послова, број пријављених кривичних дела из области високотехнолошког

[3] „Службени гласник РС“, број 53/2017.

криминала расте 50% годишње, а да су напади на сервере државних органа све учесталији и напреднији. Стратегија је дефинисала пет приоритетних области у циљу унапређења информационе безбедности, а то су:

1) безбедност информационо-комуникационих система, што се односи на ризике нарушавања функционисања органа власти, привреде и организација као последица инцидената у информационо-комуникационим системима;

2) информациона безбедност грађана, што се односи на ризике нарушавања безбедности грађана злоупотребом информационо-комуникационих технологија;

3) борба против високотехнолошког криминала, што се односи на превенцију и санкционисање кривичних дела која се заснивају на злоупотреби информационо-комуникационих технологија;

4) информациона безбедност Републике Србије, што се односи на ризике нарушавања националне безбедности путем информационо-комуникационих система;

5) међународна сарадња, што подразумева сарадњу са страним државним органима, међународним организацијама и другим партнерима у области информационе безбедности[4].

У оквиру ових приоритетних области, неки од стратешких циљева јесу: 1) превенција и заштита путем размене информација, праћења актуелних ризика и подизање свести, 2) безбедност ИКТ система у привредним субјектима и безбедност електронског пословања, 3) безбедност ИКТ система од посебног значаја, 3) безбедност деце на интернету, 4) борба против високотехнолошког криминала, 5) унапређење механизама за откривање високотехнолошког криминала и кривично гоњење учинилаца и 6) изградња војних капацитета система одбране за одбрану од високотехнолошких напада.

Доношењем овакве стратегије, Република Србија је показала да је препознала опасности у сајбер простору, као реалне и могуће остваривe. Стратешки циљеви наведени у овој стратегији умногоме су заједнички са онима које владе других земаља наводе у својим стратегијама. Међутим, велике светске силе су донеле стратегије пре свега са аспекта дефинисања сопствених стратешких позиција у области сајбер ратовања где су, на тај начин, легитимизовале сајбер ратовање као облик могућег савременог конфликта са другом државом. У том смислу, највећи део тих стратегија посебну пажњу поклања војно-одбрамбеним мерама заштите сопственог сајбер простора и методама спровођења офанзивног напада на сајбер бојном пољу у оквиру активности вођења хибридног рата. Република Србија опасности дефинише, пре свега, у области високотехнолошког криминала као

[4] „Службени гласник РС“, број 53/2017.

посебне области криминала, али се истиче и да ће Министарство одбране и Војска Србије развити свеобухватне способности за одбрану у сајбер простору у складу са уставним и законским надлежностима и додељеним мисијама и задацима. Наведене активности обухватају успостављање информационе безбедности и способности за извођење одбране у сајбер простору (Стратегија развоја информационе безбедности у Републици Србији, 2017). Иако су хибридни ратови нешто што званичници Републике Србије наводе као методе које се спроводе над нашом земљом, у Стратегији развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године ова формулација не постоји, као ни у Стратегији националне безбедности. С обзиром на чињеницу да велике светске силе не крију да користе неке методе хибридног ратовања као облике неоружаних напада, или пак као једини облик напада или увертиру у оружани сукоб, Република Србија би требало да уврсти ову претњу у своја стратешка документа током ревизије или приликом доношења нових стратегија из области безбедности.

Закључак

Политичке, економске и безбедносне прилике и догађаји, у прве две деценије XXI века, показују да је ово раздобље великих геополитичких и војних изазова за све земље света. Стабилност и безбедност готово свих земаља данас одређена је не само војном снагом већ и квалитетом животне средине, енергетском стабилношћу, технолошким развојем, нивоом поштовања људских права. У том смислу, и начини израде стратегијских докумената се мењају, заједно са изазовима на које ови документи треба да одговоре. Иако се израда већине националних стратегија безбедности суштински ослања на војне снаге и учешће представника одбрамбених структура у писању документа, савремене невојне претње и изазови показују да својим остваривањем могу изазвати далекосежнију штету и угрозити велики број живота (пандемије, катастрофалне временске непогоде, сајбер напади). Стога је сарадња стручњака различитих области нужна за израду адекватне и ефикасне безбедносне стратегије савременог доба. Аустралијско Министарство одбране је, на пример, нацрт своје Националне стратегије безбедности ставило на јавну расправу, а у саму израду био је укључен и цивилни сектор. За израду Националне стратегије безбедности Француске, за период од 15 година, тадашњи председник Никола Саркози (Nicholas Sarkozy) је 2007. године оформио комисију од 35 чланова за њено писање. Чланови те комисије били су из редова владе, војске, универзитета, правосуђа и индустрије. Радили су организовани у мање радне групе и свака је, у циљу што боље анализе стања и предвиђања будућих изазова, спровела бројне интервјуе, фокус групе и студије случаја (Canciat et al., 2017, p. 36).

Република Србија је и географски и политички увек била на раскршћима великих империја и светских сила. Вођена искуствима из XX века, као и променама, пре свега у Европи, након пада Берлинског зида, Република Србија се одлучила за војну неутралност. Оваква позиција показује усмерење ка мирољубивој политици али, с обзиром на то да не припада ниједном формалном или неформалном војно-политичком савезу, Република Србија мора јачати своје економске, социјалне, одбрамбене и друге стубове, како би у безбедносном смислу остала независна. Неки од кључних ризика који се наводе у Стратегији националне безбедности Србије, донетој 2019. године, присутни су као главне и истакнуте опасности и у безбедносним стратегијама других земаља, попут тероризма, организованог криминала и енергетске стабилности. Реалност показује да се данас Република Србија суочава са истим изазовима као и земље у окружењу, попут илегалних миграција и избијања пандемије. Све наведене опасности врло су комплексне и не могу се везати за једно временско раздобље, већ је извесно да ће претити свету, као и нашој земљи још дуго. Оно што је технолошки напредак донео јесте сасвим нова и специфична врста опасности и сукоба – напади у сајбер простору. Дигитално окружење постало је важно за компаније, владе и појединце – сви они суочавају се са ризицима по сајбер безбедност, а у зависности од своје позиције, деле и извесни степен одговорности за управљање њима (Al-Ghamdi, 2021). Управо због своје геополитичке позиције и војне неутралности, Република Србија би већ сада требало да уложи значајније напоре за осигурање свог сегмента сајбер простора и изградњу капацитета за одбрану од хибридних ратова. Уважавајући иностранa искуства и сложену безбедносну стварност, наши стратешки документи требало би периодично бити евалуирани, па чак и ревидирани, у односу на препознате промене у геополитичким или унутрашњим политичким, социјалним, економским и безбедносним односима и изазовима. Као оптимална, показала се методологија формирања мање групе експерата, не само из војног већ и сектора науке, привреде и референтних невладиних организација, која би, уз примену адекватних методолошких техника прикупљања и анализе података, креирала обухватну стратегију, чији ће основни елементи бити продукт мултидисциплинарног приступа. Министарство одбране координира израду Националне стратегије безбедности, међутим, Радна група за поглавља 30 и 31 Националног конвента о Европској унији (NKEU) изнела је замерку да сам процес израде нацрта ових докумената није био инклузиван, што није у складу с процесима креирања сличних докумената у државама чланицама Европске уније, а сама јавна расправа није организована тако да омогућава и охрабрује суштински дијалог између представника владе и заинтересоване јавности, већ искључиво у форми прикупљања амандмана на нацрте стратегија (https://europeanwesternbalkans.rs/izrada-nacrta-strategija-nacionalne-bezbednosti-odbrane-nije-bila-inkluzivna/). Ове примедбе би требало уважити не

само због тога што се Република Србија декларативно изјашњава за приступање Европској унији већ и из практичних разлога – неки ризици наведени у нашој стратегији и на глобалном нивоу показују карактер изненадности, променљивости и учесталости. Савремена литература о креирању јавних политика указује да све стране на које се акти који се израђују односе треба да учествују у њиховом креирању (Cancial et al., 2017, p. 44). Како су безбедносни концепти прелазили пут и развијали се од стриктно војних до концепта хумане безбедности, ту развојност и разноврсност знања потребних за суочавање са савременим изазовима треба применити и у изради стратешких докумената. Научници из области безбедности слажу се да је концепт безбедности прошао фундаменталну трансформацију – од на претњама оријентисаном концепту одбране до концепта припреме, превентиве и проактивности за будуће ризике, од којих су неки лакше, а неки теже предвидиви (Hammerstad and Boas, 2015, p. 475). Управљање ризицима и кризни менаџмент данас траже знања и ресурсе и изван војне области и ту чињеницу треба применити и при изради и дискусији о стратешким безбедносним документима.

Библиографија

1. ALDaajeh et al. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, 119.
2. Al-Ghamdi. (2021). Guide to developing a National Cyber Security Strategy. *Materials Today: Proceedings.*
3. Barnard-Wills, D. and Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture*, 15(2), 110–123.
4. Berenskoetter, F. B. (2005). Mapping the Mind Gap: A Comparison of US and European Security Strategies. *Security Dialogue* vol. 36, no. 1.
5. Cancian, M. F. et al. (2017). *Formulating National Security Strategy: Past Experience and Future Choices*. Center for Strategic and international Studies.
6. Collier, B., Horgan, S., Jones, R. and Shepherd, L. (2020). The implications of the covid-19 pandemic for cybercrime policing Scotland: A rapid review of the evidence and future considerations.
7. Council of the European Union. ESS. (2007).
8. European External Action Sevice. (2008). The Global strategy for the foreign and security policy of the European Union: implementati0on Report.
9. Gates, R. (2014). *Duty: Memoirs of a Secretary at War*. New York: Alfred A. Knopf.
10. Godzimirski, J. M. (2022). Energy, climate change and security: The Russian strategic conundrum. *Journal of Eurasian Studies*, Vol. 13(1), 16–31.

11. Hammerstad, A. and Boas, I. (2014). National security risks? Uncertainty, austerity and other logics of risk in the UK government's National Security Strategy. *Cooperation and Conflict*, Vol. 50(4), 475–491.
12. https://europeanwesternbalkans.rs/izrada-nacrta-strategija-nacionalne-bezbednosti-odbrane-nije-bila-inkluzivna
13. https://www.csis.org/analysis/chinas-new-2019-defense-white-paper
14. https://www.institutmontaigne.org/en/blog/russias-national-security-strategy-2021-era-information-confrontation
15. Magnus, H. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* 4, no. 2, 1–24.
16. Миљковић, М., Путник, Н. (2016). Активности савремених обавештајних служби у кибер простору. *Војно дело*, 7, стр. 163–180.
17. Norton M, Katzman D, Escott P. et al. (1999). *A People and a Nation: A History of the United States*. Boston, MA: Houghton.
18. Porter, M. (1996). What is strategy? *Harvard Business Review* 74(6): 61–78.
19. Romano, S. M. (2011). Liberal Democracy and National Security: Continuities in the Bush and Obama Administrations. *Critical Sociology*, 38(2): 159–178.
20. Santisteban et al. (2020). Analysis of National Cybersecurity Strategies. *International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 12.
21. Song, M. et al. (2021). Comparative Analysis of National Cyber Security Strategies using Topic Modelling. *International Journal of Advanced Computer Science and Applications*, Vol. 12, No. 12.
22. Стратегија националне безбедности Републике Србије, „Службени гласник РС“ 88/2009.
23. Стратегија националне безбедности Републике Србије, „Службени гласник РС“ 94/2019.
24. Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године, „Службени гласник РС“, број 53/2017.
25. Tatar, Ü., Çalik, O., Çelik, M. & Karabacak, B. (2014). A comparative analysis of the national cyber security strategies of leading nations. In: *international Conference on Cyber Warfare and Security* (p. 211). Academic Conferences international Limited.
26. Truman Doctrine. (1957).
27. „Службени гласник РС“, број 53/2017.

METHODOLOGY FOR DEVELOPING THE NATIONAL SECURITY STRATEGY OF THE REPUBLIC OF SERBIA - DILEMMA AND PERSPECTIVES

Abstract

The most significant risks and challenges to the security of states, as well as the main subjects and measures for their prevention, are defined in strategic security documents. Today, more often than in the 20th century, these umbrella documents are subject to revisions, bearing in mind the dynamism of external and internal political, socio-economic and security relations and changes. The paper analyzes the national security strategies of individual countries, the risks presented in them and the dynamics of their revisions. Also, the basic strategic documents in the field of security in the Republic of Serbia were discussed and recommendations were made for their possible revision or addition, in relation to current external and internal challenges, and based on the methodology of developing security strategies of EU member states.

Keywords: security national security strategy, risk, cyber security, revision.

.

УНАПРЕЂЕЊЕ СТРАТЕШКОГ ОКВИРА РЕПУБЛИКЕ СРБИЈЕ ЗА СПРЕЧАВАЊЕ И СУЗБИЈАЊЕ ОРГАНИЗОВАНОГ КРИМИНАЛА, ТЕРОРИЗМА И ЕКСТРЕМИЗМА: ПОУКЕ ВЕЛИКИХ СИЛА

Божидар Бановић[1], Ненад Стекић[2]

Апстракт

Академска проучавања социолошких појава попут организованог криминала, тероризма и екстремиз(а)ма у новије време попримају већи значај због повећаног броја изазова са којима се савремене државе суочавају. Повећано интересовање се огледа доминантно у сфери националне безбедности узимајући у обзир да све државе теже да задовоље минимум потребног нивоа сигурности грађана, али и других објеката заштите попут критичне инфраструктуре, државних граница, те традиционалне војне безбедности. Циљ овог рада је да прикаже могуће модалитете унапређења стратешког и легислативног оквира Републике Србије у односу на идентификоване безбедносне ризике са којима се суочава током треће деценије 21. века. Анализа је усредсређена на приказ недостатака правног регулисања ове материје и могућности унапређења постојећег стања. Аутори најпре анализирају позитивноправне норме у овој области, а потом нуде приказ могућег модела организације стратешког и нормативног корпуса аката Републике Србије по узору на решења из Народне Републике Кине, као могућег модела једне од светских суперсила у систему међународних односа. Осим систематичног приказа нормативних аката кроз Регистар правних прописа и осталих аката које регулишу борбу против наведених безбедносних појава, аутори кроз дискусију

[1] Редовни професор, Факултет безбедности Универзитета у Београду, e-mail: banovicb@fb.bg.ac.rs

[2] Научни сарадник, Институт за међународну политику и привреду, e-mail: nenad.stekic@diplomacy.bg.ac.rs

Рад је настао у оквиру пројекта који финансира Фонд за науку Републике Србије у оквиру Програма „Идеје“ – Management of New Security Risks – Research and Simulation Development, NEWSIMR&D, #7749151.

нуде сет препорука које могу послужити као улазни параметри за софтверску симулацију безбедносних ризика у будућим истраживачким напорима.

Кључне речи: организовани криминал, екстремизам, тероризам, национална безбедност, систем националне безбедности, Србија, НР Кина.

Ка систематичном креирању стратешког оквира

Академска проучавања социолошких појава попут организованог криминала, тероризма и екстремиз(а)ма у новије време попримају већи значај због увећања изазова по националну безбедност са којима се савремене државе суочавају. Повећано интересовање се огледа доминантно у сфери националне безбедности, узимајући у обзир да све државе теже да задовоље минимум потребног нивоа сигурности грађана, али и других објеката заштите попут критичне инфраструктуре, државних граница, те традиционалне војне безбедности. Зарад остваривања тог циља предузимају се комплексне процене ризика како би се утврдио приоритет заштите, али и могући интензитет последица у случају наступања ризика. Када је уврштена као аналитички алат у теоријски систем студија безбедности, процена ризика је, доминантно, била окренута ка сајбер простору и тада „новим безбедносним парадигмама“ (Biringer et al., 2007). Након терористичких напада на САД 2001. године, институционалне, али и академске процене ризика прелиле су се и на сферу ових безбедносних појава. Студије које третирају процену ризика против тероризма[3] усмерене су на појединачну процену ризика о томе да ли је „безбедносно интересантан“ појединац у стању да учини ово кривично дело (Hart, Michie & Cooke, 2007; Monahan, 2016; Monahan & Skeem, 2016), као и на процену испољавања тероризма и сродних кривичних дела у оквиру опште стопе криминалитета на одређеном простору (Woo, 2002).

Циљ овог рада је да прикаже могуће модалитете унапређења стратешког и легислативног оквира Републике Србије у односу на идентификоване безбедносне ризике са којима се суочава током треће деценије 21. века. Анализа је усредсређена на приказ недостатака правног регулисања ове материје и могућности унапређења постојећег стања. Поред тога, овај чланак има неколико додатних циљева. Најпре, анализа случаја правних прописа Републике Србије која ће бити приказана у наставку текста треба да послужи као основ за идентификацију недостатака у нормативном и стратешком оквиру Републике

[3] Додатно, уочљива је дистинкција на ауторе који фаворизују квантитативне у односу на квалитативне процене ризика испољавања тероризма. О томе више видети у: Biringer, Betty E., Rudolph V. Matalucci, and Sharon L. O'Connor. *Security Risk Assessment and Management: A professional practice guide for protecting buildings and infrastructures*. John Wiley & Sons, 2007; Woo, Gordon. "Quantitative terrorism risk assessment." *The Journal of Risk Finance* (2002).

Србије за супротстављање безбедносним појавама у областима тероризма, екстремизма и нарушавања територијалне целовитости. У литератури се често идентификује нормативна проблематика регулисања ове области у зависности од нивоа имплементације права – национални или мултинационални какав је Европска унија (Føllesdal et al., 2008), али и смештања тероризма и организованог криминала у контекст међудржавних односа. Антонио Касезе (*Antonio Cassese*) наводи да кључни изазов у нормирању тероризма лежи у потреби за његовим укључивањем у оквире међународног јавног права, поредећи овај феномен са политички релевантним дешавањима у систему међународних односа (Cassese, 2006). Даље, остваривање увида у искуства великих сила, на пример Народне Републике Кине (у даљем тексту НР Кине или само Кине), послужиће као основ за уочавање могућих нормативних решења за супротстављање безбедносним ризицима и уочавање нише која омогућава идентификовање ризика који могу настати као последица одсуства системског решавања ових проблема. Коначно дискусија о наведеној тематици послужиће као основ за састављање улазних параметара за софтверску симулацију која ће бити реализована као једна од многобројних активности Националног симулационог центра за истраживање, обуку и образовање у области безбедности који ће бити успостављен у оквиру пројекта *NEWSIMR&D*.[4]

Овај чланак је организован на следећи начин. Најпре ће бити приказан стратешки и нормативни оквир Републике Србије у анализираним областима. Аутори идентификују потенцијалне правне и стратешке празнине позитивног права и нуде препоруке за побољшавање тренутног стања упућене доносиоцима одлука. У раду се приказују нормативна решења из Националне стратегије за спречавање и борбу против тероризма (2017), затим Закона о националној бази података за спречавање и борбу против тероризма (2021), као и нормативним решењима из Стратегије за борбу против прања новца и финансирања тероризма за период 2020–2024. Аутори потом усредсређују пажњу на приказ истоветног правног регулисања борбе против тероризма, али и осталих аката којима се гарантује територијална целовитост, на примеру НР Кине као суперсиле у систему међународних односа, и уочавају могуће поуке које би биле примењиве на локални контекст и правну традицију домаћег права. На крају, аутори нуде сет препорука и исхода за могуће софтверско симулирање ризика који могу настати као последица нерегулисања важне нормативне материје. Додатно, аутори у

[4] Пројекат уводи иновативан приступ у управљању новим безбедносним ризицима. Главна новина пројекта је интердисциплинарни приступ анализама нових безбедносних феномена, попут сајбер безбедности, миграција, личних података, социопатолошких феномена и енергетске безбедности. Видети више на: https://newsimrdproject.fb.bg.ac.rs/indexrs.html (14.10.2022).

прилогу рада (Прилог 1) нуде крађи попис постојећих (2022) аката који регулишу анализиране области у Републици Србији.

Стратешки оквир Републике Србије

Стратешко регулисање безбедносних појава у савременом друштвеном контексту Републике Србије учињено је, као последица реформе сектора безбедности, усвајањем Стратегије националне безбедности и Стратегије одбране 2009. године, а потом и њиховом поновном израдом и усвајањем оба поменута документа 2019. године. Тероризам, према одредбама најновије Стратегије националне безбедности, представља „велики ризик и озбиљну претњу безбедности Републике Србије“, а „њени грађани, у земљи и иностранству, могу бити објекти терористичког деловања“ (Народна скупштина, 2019, стр. 2). Стратегија третира и деловање екстремистичких група које се јављају „у променљивом интензитету у појединим деловима Републике Србије и могу дестабилизовати политичко-безбедносну ситуацију“ (2019, стр. 2). Екстремизам, према одредбама стратегије, „може бити и генератор сепаратистичких тежњи, нарочито уколико за то постоји подршка из иностранства“ (2019, стр. 2). Када је реч о тероризму, у домену *стратешког*, Република Србија је остварила значајне кораке усвајањем Националне стратегије за спречавање и борбу против тероризма за период 2017–2021. године.[5] У делу који се односи на планирање, документ наводи да је процена ризика и процена претњи, заснована на „бројним индикаторима и анализи кључних фактора и елемената који утичу на степен претње“ (Влада Србије, 2017), показала да су „терористичке претње Републици Србији реалне, што се манифестује у спознаји да унутар земље, као и у окружењу, постоје лица и групе способни и вољни да припреме, организују и спроведу терористичке нападе на мете у Републици Србији“ (Влада Србије, 2017). Стратегија је предвиђала четири приоритетне области – превенцију, заштиту (отклањањем претњи), кривично гоњење терориста уз поштовање људских права и, као последњу област, одговор система у случају терористичког напада (Влада Србије, 2017).

Паралелно са овом, Србија је остварила правни континуитет у области борбе против прања новца и финансирања тероризма, у оквиру које је до сада усвојено три стратегије – за период 2008–2013. године, затим друга за период 2014–2019. и тренутно важећу, трећу Националну стратегију за борбу против прања новца и финансирања тероризма са роком примене 2020–2024. године.[6] Циљ стратегије

[5] Међутим, узимајући у обзир да је Стратегија орочена на период од 5 година са трајањем до 2021. и да није усвојена нова стратегија која би на кохерентан начин третирала борбу против тероризма, Република Србија је остала без значајног акта у овој области.

[6] Стратегија је заменила претходну која је била орочена на период 2014–2019.

јесте „у потпуности заштитити привреду и финансијски систем државе од опасности које узрокују прање новца и финансирање тероризма и ширења оружја за масовно уништење“ (Влада Србије, 2020, стр. 20). Полазишна основа на којој се базира документ јесте позивање на активнију сарадњу јавног и приватног сектора, те увођење приступа заснованог на анализи и процени ризика (2020, стр. 21), што последично треба да доведе до јачања система и интегритета институција финансијског и нефинансијског сектора и допринесе безбедности, сигурности и владавини права (2020, стр. 21).

Радно тело за израду ове стратегије спровело је крађу анализу ризика и утврдило да постоје три стуба који осигуравају стабилан рад институција: постојање политичке стабилности и континуиране посвећености и опредељења на високом политичком нивоу и на нивоу државних органа и институција појединачно; додатно разрађивање механизма координације и интерресорне сарадње; очување и додатно јачање ресурса, људских и материјално-техничких у складу са анализом и проценом ризика (2020, стр. 22). Стратегија препознаје смањивање ризика од прања новца, финансирања тероризма и ширења оружја за масовно уништење кроз континуирано унапређење стратешког, законодавног и институционалног оквира, затим спречавање уношење у финансијски и нефинансијски систем имовине за коју се сумња да је стечена кривичним делом, која је намењена финансирању тероризма или ширењу оружја за масовно уништење, односно унапредити откривање такве имовине уколико је већ у систему, као најзначајније посебне циљеве (2020, стр. 21). Поред тога, стратегија идентификује кажњавање извршиоца кривичног дела прање новца и уочавање и отклањање претњи од финансирања тероризма и кажњавање извршилаца кривичног дела финансирања тероризма као додатна два циља (2020, стр. 21). Осим поменутог, Акционим планом за спровођење поменуте стратегије, као активност под бројем 1.1.1, предвиђено је „утврђивање методологије и ажурирање националне процене ризика од прања новца и финансирања тероризма“.

Током 2021. године, Народна скупштина Републике Србије је усвојила Закон о националној бази података за спречавање и борбу против тероризма који установљава јединствену националну базу података као „платформу која садржи скуп података као део већ ускладиштених података у постојећим базама надлежних органа,[7] и која омогућава приступ тим подацима и контролисану и

[7] Закон идентификује министарство надлежно за унутрашње послове, министарство надлежно за спољне послове, Безбедносно-информативну агенцију, Војнобезбедносну агенцију и Војнообавештајну агенцију, министарство надлежно за послове одбране, Управу за спречавање прања новца министарства надлежног за послове финансија, Републичко јавно тужилаштво и Тужилаштво за организовани криминал као надлежне органе у овој области (2021, чл. 2, ст. 3).

безбедну размену података“ (Народна скупштина, 2021, чл. 2а) о индексираним лицима. Решења садржана у овом закону имају за циљ да на јасан и прецизан начин уреде поступак похрањивања података у базу, њену садржину, приступ подацима, њихово коришћење и заштиту, са посебним нагласком на поштовању међународних стандарда заштите људских права и слобода. Са друге стране, циљ одредаба овог закона јесте обезбеђивање ефикасне размене података између државних органа надлежних за превенцију и борбу против тероризма и подизање способности система безбедности за благовремени и ефикасни одговор на претњу коју представља тероризам. Закон предвиђа да су предмет индексирања сва физичка и правна лица, као и групе или организације „које су означене и стављене на међународну или националну листу терориста, терористичких организација или финансијера тероризма“ (Народна скупштина, 2021, чл. 2, ст. 4). Тако ограничен предмет индексирања, према одредбама закона, не искључује иностранa лица или организације које су већ регистроване од стране Уједињених нација и/или међународних организација, као ни са „консолидоване листе успостављене на основу закона који уређује међународне мере ограничавања“ (Народна скупштина, 2021). Закон предвиђа и коришћење већ постојећих база података других државних органа које укључују лица која су осумњичена, оптужена или осуђена за кривично дело тероризам и са њим повезана кривична дела (2021, чл. 5).[8]

Закон о националној бази података је добро законско решење које има и неколико својих мана. Разлози заштите података и приступа подацима јесу недвосмислено јасни и закон предвиђа да „надлежни орган који је проследио упит може од надлежног органа који је индексирао лице (прим. аут. БИА) захтевати достављање проширених података, ако је то неопходно за обављање конкретног посла из његове надлежности“ (2021, чл. 8). Како акт прецизира органе које имају надлежност делимичног приступа подацима, било би адекватно овај списак допунити и научноистраживачким институцијама које у својим акредитованим студијским програмима имају научне области студије безбедности. Тиме би се пружила могућност академској заједници да, у оквирима контролисане употребе појединих сетова података, оствари значајне увиде у обрасце испољавања терористичких активности у земљи и иностранству.

Оно што је добра страна приказаних аката јесте инсистирање на проценама ризика као алату који уједначено приказује хазарде који су улазни параметри за све анализе нарушавања (националне) безбедности. Међутим, ниједан од три приказана документа не прецизира ниво систематизације ризика као ни

[8] Закон је Безбедносно-информативној агенцији поверио администрирање базом података.

методологију за израду процене ризика у креирању стратешких аката и њиховом ажурирању.

Као позитиван пример у правцу уважавања и примене међународно признате методологије у процени ризика требало би истаћи неколико докумената: Национална процена ризика од прања новца и национална процена ризика од финансирања тероризма, Процена ризика од прања новца и финансирања тероризма у сектору дигиталне имовине и Процена ризика од финансирања ширења оружја за масовно уништење (Закључак Владе РС, 2021).[9] Поменуте процене ризика резултат су усклађивања стратешко-нормативног оквира Републике Србије са Препорукама Радне група за финансијску акцију (*Financial Action Task Force* – FATF 2012; 2022).[10] Препоруком бр. 1, под насловом „Процена ризика и примена приступа заснованог на процени ризика“ (*risk-based approach*), сугерише се државама да идентификују, процене и схвате ризике с којима се суочавају на плану прања новца и финансирања тероризма и да предузму кораке, укључујући и одређивање органа или механизма који ће координисати мере за процену ризика, те да определе ресурсе у циљу делотворног смањења тих ризика. Циљ процене ризика јесте да се дође до закључака о томе који сектори и какво поступање носе потенцијално виши ризик од прања новца и финансирања тероризма, а које нижи, како би држава могла адекватно да одговори на утврђене ризике кроз мере и активности које предузима, као и да у складу са процењеним ризицима донесе адекватне одлуке о расподели ресурса, чиме би се обезбедило да мере за спречавање или ублажавање прања новца и финансирања тероризма буду сразмерне идентификованим ризицима.

---

[9] Ови документи усвојени су Закључком Владе Републике Србије, на седници одржаној 30. 09. 2021. године. Поменуте процене ризика обухватају период од три године, од 1. 1. 2018. године до 31. 12. 2020. године. **Прве националне процене ризика од прања новца и финансирања тероризма спроведене су 2012, односно 2014. године, а затим 2018. године.**

[10] Радна група за финансијску акцију (*Financial Action Task Force* – FATF) јесте међувладино тело које су 1989. године основали министри држава-чланица. Задатак овог тела је успостављање стандарда и промовисање делотворне примене законских, регулаторних и оперативних мера за борбу против прања новца, финансирања тероризма и ширења оружја за масовно уништење, као и других сродних претњи по интегритет међународног финансијског система. Препоруке FATF постављају свеобухватан и конзистентан оквир мера које државе треба да примене како би се бориле против прања новца и финансирања тероризма и ширења оружја за масовно уништење. С обзиром на то да су Препоруке још 2003. године прихваћене од 180 држава, може се закључити да су стекле универзално признање као међународни стандард за борбу против прања новца и финансирања тероризма.

Законом о спречавању прања новца и финансирања тероризма прописује се да се „процена ризика од прања новца и финансирања тероризма на националном нивоу израђује у писменој форми и ажурира најмање једном у три године, а сажетак процене ризика ставља се на располагање јавности и не сме садржати поверљиве информације“ (2017, члан 70), чиме је процена ризика успостављена и као нормативна обавеза.[11]

Поменуте националне процене ризика, осим што успостављају основу за доношење стратешко-политичких докумената у овој области, представљају и значајно унапређење посматрано и са методолошког аспекта, што смо идентификовали као слабост претходно анализираних стратешких докумената у овом раду. Према наводима у самом тексту националних процена ризика, као основа, коришћена је методологија Светске банке (*National Money Laundering and Terrorist Financing Risk Assessment Toolkit*), при чему је она у одређеним областима допуњавана. Развијени су домаћи критеријуми за процену ризичних форми привредних друштава, те допуњени критеријуми за процену ризика који се односе на прекограничне претње.[12]

Користећи поменуту методологију, Национална процена ризика од прања новца заснована је на анализи података о: кривичним делима чијим се извршењем стиче противправна имовинска корист (потенцијална предикатна кривична дела), предикатним кривичним делима поводом којих је покренут поступак и за кривично дело прање новца, учесталости извршења предикатних кривичних дела, висини скривене – одузете – процењене противправне имовинске користи из предикатног кривичног дела и укључености организованих криминалних група у извршењу кривичних дела. Методологија је укључивала и увид у предмете јавних

[11]Приступ заснован на процени ризика у области спречавања прања новца и финансирања тероризма у Србији први пут је уведен Законом о спречавању прања новца и финансирања тероризма из 2009. године.

[12] Новина у овом циклусу националне процене ризика јесте и то да је Република Србија по први пут спровела и процену ризика од прања новца и финансирања тероризма у сектору дигиталне имовине и процену ризика од финансирања ширења оружја за масовно уништење. За процену ризика од прања новца и финансирања тероризма у сектору дигиталне имовине коришћена је методологија Савета Европе, а за процену ризика од финансирања ширења оружја за масовно уништење коришћена је методологија RUSI Института за одбрамбене и безбедносне студије (RUSI), односно Водич за спровођење националне процене ризика од финансирања пролиферације, уз учешће и консултације експерата из САД и ЕУ.

тужилаштава и судова,[13] те професионално искуство чланова радне групе за израду процене ризика.

Претња од тероризма темељи се на: информацијама и статистичким подацима прикупљеним од стране јавног тужилаштва, служби безбедности и других надлежних државних органа. Не улазећи дубље у анализу текста поменутих националних процена ризика, можемо констатовати да је методолошки поступак коришћен у њиховој изради путоказ за будуће стратешко политичке документе у овој области.

Стратешко регулисање криминалитета – случај НР Кине

НР Кина представља академски релевантан случај велике силе у међународном систему, чији би пример правног регулисања тероризма, екстремизма и унутрашњих претњи националној безбедности могао да послужи као релевантан извор за систематичније уређивање правних решења у случају других земаља. У наставку ће бити приказани важни проблеми који су третирани правним актима на стратешком нивоу – супротстављање тероризму и етнорелигијском екстремизму, прецизније ситуација у кинеској западној провинцији Синђанг, али и изазови са проблемима унутрашње безбедности који се односе на ситуацију у Хонгконгу, као и проблеми са оспореном сувереношћу на делу кинеске територије коју званични Пекинг третира делом Кине – Тајваном.

Провинцију Синђанг насељавају претежно Ујгури, туркофона национална мањина сунитских муслимана којих у Кини има око 10 милиона (Britannica, 2022). Међуетничке тензије које су настајале током претходне три деценије у овој провинцији између Кинеза (Хан) и Ујгура кулминирале су серијом инцидената током 2009. године у којима је живот изгубило око 200 Хан Кинеза, што је условило систематичну борбу централних власти против екстремизма и, како су их тада оцениле, „тероризма у овој области“. Једно од првих нормативних одговора централних власти на изазове у поменутој провинцији био је кинески

[13] На самом почетку су анализиране одредбе Кривичног законика и посебних закона којима су прописана кривична дела. На овај начин сачињена је листа од укупно 115 кривичних дела. До података о предикатним кривичним делима поводом којих је покренут и поступак за прање новца дошло се увидом у списе предмета јавних тужилаштава и судова, као и анализом годишњих извештаја о раду Републичког јавног тужилаштва, статистичких извештаја надлежних јавних тужилаштава и судова. Њиховом анализом дошло се до закључака о учесталости извршења појединих предикатних кривичних дела, висине имовинске користи повезане са извршењем кривичног дела, секторима преко којих је вршено прање новца, учешћу организованих криминалних група у прању, откривеној готовини која се доводи у везу са прањем, као и бројним другим подацима.

Закон о супротстављању тероризму из 2015. године. Он третира тероризам као сваки „предлог или радњу која ствара друштвену панику, угрожава јавну безбедност, нарушава личност и имовину или врши принуду над националним властима или међународним организацијама, методама као што су насиље, уништавање, застрашивање, како би постигле њихове политичке, идеолошке или друге циљеве“ (China Counter-terrorism Law, 2015, art. 3). Занимљиво је да закон укључује Кинеску народноослободилачку армију, кинеске народне оружане полицијске снаге и организације народне милиције у спречавање и руковођење терористичким активностима уз ангажовање институција на националном, али и на нивоу провинција, за борбу против тероризма.[14] Посебно поглавље закона посвећено је анализи безбедносне проблематике и превенције терористичких активности на територији Кине. Закон предвиђа да сви телекомуникациони и интернет оператори морају да, када открију информације које указују на могуће планирање терористичких или екстремистичких аката, одмах обуставе њихов пренос и избришу релевантне информације или затворе релевантне веб странице и укину релевантне услуге, а такве кориснике пријаве надлежним органима (China Counter-terrorism Law, 2015, art. 19).

Закон додатно регулише услове под којима се суди за специфична кривична дела тероризма и осталих екстремистичких активности – попут распиривања међуетничке, верске или идеолошке мржње, као и битнија нарушавања јавне безбедности. Међутим, оно што је особеност овог закона, а што је један од коренитих узрока због којих званични Пекинг трпи критике међународне заједнице и оптужбе западних држава предвођених САД, односи се на третирање затвореника након одслужења затворске казне. Према одредбама овог акта, за осуђенике који су одслужили казну затвора, пре пуштања на слободу по одслужењу казне, „надлежне инстанце врше процену њихове опасности по друштво на основу природе, околности и штете по друштво њиховог злочина, њиховог понашања током издржавања казне и утицаја њиховог пуштања на слободу на њихову заједницу“ (China Counter-terrorism Law, 2015, art. 30). Када процене укажу да осуђеници представљају опасност по друштво, затворски службеници имају задатак да доставе суду препоруку за упућивање у „едукативне кампове“ у месту издржавања казне, а копију писмене препоруке шаљу и тужилаштву за исти степен (2015, art. 30).[15]

Следећа важна одлика овог закона јесте и сарадња између државних институција и органа у пословима супротстављања тероризму и то између министарстава

[14] Међутим, Закон оставља могућност да поједини органи попут Државног савета НР Кине (владе) и Централне војне комисије имају право вета на такво учешће других органа.

[15] Видети више у: (Seymour and Anderson, 2015).

(ориг. „одељења Државног савета“) који у својим портфељима имају различите ресоре. Тако закон предвиђа да министарства НР Кине за спољне послове, јавну безбедност, националну безбедност, развој и реформу, индустрију и информатичко друштво, трговину и туризам треба да успоставе системе за процену ризика који би повећали степен безбедносне заштите кинеских држављана у земљи и иностранству и осигурали кинеске компаније, објекте инвестирања или средства са седиштем ван територије копна, ради спречавања и реаговања на терористичке нападе (2015, art. 41). Закон још регулише питања прикупљања обавештајних података, одговора на кризе, затим врсте и начине истражних поступака, те облике међународне сарадње.

У мају 2021. године Кина је усвојила посебан акт са снагом закона који се односи на улогу јавних органа безбедности у супротстављању организованом криминалу. Закон регулише превенцију и управљање процесом борбе против организованог криминала које имплементирају државни органи Кине, као и верификацију за прикупљање података. Према одредбама акта, органи јавне безбедности дужни су да користе савремену информациону технологију у складу са законом за успостављање механизма за прикупљање, истраживање и процену трагова организованог криминала и руковање њима путем оцењивања и класификације. Органи јавне безбедности благовремено спроводе „статистичке, аналитичке, истраживачке и судске послове о траговима организованог криминала и организују инспекцијски надзор у складу са законом; за питања која не спадају у делокруг органа јавне безбедности, предају се надлежним надлежним органима на решавање у складу са законом“ (China Law, 2021).

Паралелно са нормативно-правном регулацијом проблема са којима се суочава Кина у погледу националне безбедности, теку активности званичног Пекина на мултилатералном нивоу које се огледају у активностима испољеним нарочито према међународним организацијама, а доминантно у систему Уједињених нација. Крајем августа 2022. године, Кина је предала извештај под називом „Борба против тероризма и екстремизма у Синђангу: истина и чињенице“ канцеларији високог комесара Уједињених нација за људска права (енг. *The Office of High Commissioner for Human Rights* – OHCHR). У документу на преко 100 страница, Кина настоји да оправда постојање „кампова за едукацију“ као борбу против тероризма и екстремизма која је потребна и оправдана (OHCHR, 2022). Коначно, наводи се да због последица терористичких активности у западној провинцији испаштају бројне етничке групе и да је борба централних власти против екстремизма у овом делу државе управо подржана од стране свих народа који настањују Кину (2022, стр. 12). Према тврдњама из извештаја, „кампови за едукацију“ су места за дерадикализацију који су успостављени у складу са законом“ (2022, стр. 47).

Исходи за могуће софтверске симулације

Проблеми националне безбедности које идентификује Стратегија националне безбедности Републике Србије из 2019. године представљају плодотворну основу за спровођење софтверских симулација и анализу ризика од њиховог могућег испољавања, као и сагледавање последица по стабилност државе и региона. У наставку ће бити приказано неколико препорука/идеја које ће послужити као улазни параметри за софтверске симулације у спровођењу *NEWSIMR&D* пројекта.

1. *Спровести процену ризика по безбедност критичне енергетске инфраструктуре, а нарочито оне која је подложна саботажама и терористичким активностима.*

Диверсификација снабдевања енергентима је нарочито постала актуелна током кризе у Украјини, што је додатно учинило сложеним међународнополитички положај у ком се Република Србија тренутно налази. Нова безбедносна архитектура у Европи условила је различите модалитете допремања нафте и гаса који укључују употребу знатно ширег опсега инфраструктурних објеката и инсталација које су подложне намерно изазваним кваровима – саботажама. Због тога је потребно индексирати јавно доступне податке ресорних министарстава и других надлежних органа о критичној (енергетској) инфраструктури и спровести систематичну анализу ризика по њену безбедност и последице које би настале услед кварова.

2. *Спровести процену безбедносних ризика и заштиту дипломатских и конзуларних објеката Републике Србије у иностранству од екстремистичких и терористичких активности.*

Заштита држављана Републике Србије и њихова ванредна репатријација у случају инцидентних ситуација у иностранству одговара једној од одредби Стратегије националне безбедности из 2019. године. Међутим, стратегија не препознаје дипломатско-конзуларна представништва као објекте заштите, који нарочито могу бити изложени екстремистичком деловању, нарочито због осетљивих спољнополитичких одлука које званични Београд доноси у погледу тренутних дешавања у међународним односима. Због тога би требало спровести систематичну процену ризика по објекте дипломатског представљања Србије у иностранству уз коришћење бројних варијабли помоћу којих би се идентификовао ниво ризика.

3. *Учинити део варијабли Националне базе података за спречавање и борбу против тероризма доступним за академска проучавања.*

Национална база је тренутно (2022) у процесу оснивања, пошто је закон који је предвиђа усвојен 2021. године. Узимајући у обзир да се индексирање и унос веће

количине података може очекивати током ове и наредних година, одређене варијабле могу представљати плодотворну основу за спровођење статистичких и других анализа које ће бити од значаја за даље побољшање општег нивоа безбедности Републике Србије. Могућу препреку таквом напору представља члан 11 закона који предвиђа да се подаци садржани у Националној бази чувају „у електронској форми и штите у складу са одредбама закона који уређује заштиту тајних података, закона који уређује заштиту података о личности и закона који уређује информациону безбедност“ (Народна скупштина, 2021, чл. 11), а приступ подацима, осим БИА која администрира базом, имају само надлежни државни органи на основу посебног захтева који мора бити оправдан. Из тог разлога, било би пожељно да се део варијабли попут броја индексираних (потенцијалних) учинилаца кривичних дела у вези с тероризмом, или других статистичких података који би представљали значајан улазни параметар за софтверску симулацију, учини доступним академским институцијама зарад прецизнијег објашњења и предикције трендова у будућности. Такво решење видљиво је и у кинеском закону о учешћу органа јавне безбедности у супротстављању тероризму.[16]

4. *Укључивање представника академске заједнице и повећање сарадње ресорних министарстава у погледу креирања нове стратегије за борбу против тероризма.*

Слично као и у случају НР Кине, Национална стратегија Србије (која је од 2021. године застарела) предвиђала је структурисана буџетска средства и сарадњу у њеном спровођењу између Министарства правде, Министарства културе и информисања, Министарства трговине, туризма и телекомуникација, МУП-а, Безбедносно-информативне агенције, Министарства спољних послова и Тужилаштва за организовани криминал. Поред јаче међуресорне сарадње, потребно је основати радну групу за израду нове стратегије за период 2023–2027. године, коју би чинили и представници академске заједнице.

Закључак

Проблематика која се тиче сузбијања екстремизма, организованог криминала, као и других облика нарушавања националне безбедности у научној публицистици представља готово бескрајну инспирацију за бројна истраживања, као и за прегледне студије. Међутим, таква академска проучавања неретко остају на нивоу прегледних радова, без јасних препорука или даљих предлога за побољшање

[16] Тренутно законско решење предвиђа да се подаци из поменуте базе могу користити само у сврху спречавања претње од тероризма, благовременог откривања и документовања терористичке активности и кривичног гоњења (2021, чл. 12).

система процене ризика. Сложеност система међународних односа и процеси који се, чини се, све брже и интензивније испољавају и остављају коренште промене на начине на које модерна друштва функционишу, утиче и на нешто радикалније одговоре које државне власти креирају у жељи да умање њихове негативне последице. Због тога је управо овај чланак представљао израз настојања да се на сажет начин изврши краће поређење правног оквира у области организованог криминала, тероризма и осталих безбедносних претњи за две, наизглед различите државе – Републике Србије и НР Кине. Додата вредност ове анализе јесу исходи за могуће софтверске симулације који су засновани на постојећим законским решењима у нашој држави. Аутори су идентификовали четири кључне препоруке које уједно представљају улазне параметре за систематичније доприносе софтверским симулацијама чији ће налази потенцијално послужити студентима, академској заједници, али и државним доносиоцима одлука у овој области.

Библиографија

1. Biringer, B. E., Matalucci, R. V. and O'Connor, L. S. (2007). Security Risk Assessment and Management: A professional practice guide for protecting buildings and infrastructures. John Wiley & Sons.
2. Britannica. (2022). Uyghur people, Приступљено 29.9.2022. https://www.britannica.com/topic/Uyghur
3. Cassese, A. (2006). The multifaceted criminal notion of terrorism in international law. Journal of International Criminal Justice 4.5. p. 933–958.
4. China Law. (2021). Public Security Organ Provisions on Efforts to Counter Organized Crime Приступљено 8.10.2022.: https://www.chinalawtranslate.com/en/police-organized-crime-rules
5. Føllesdal, A., Wessel, A. R. and Wouters, J. Eds. (2008). Multilevel regulation and the EU: the interplay between global, European, and national normative processes. BRILL
6. Greitens, S. C., Lee, M. and Yazici, E. (2019). Counterterrorism and preventive repression: China's changing strategy in Xinjiang. International Security 44.3 p. 9–47.
7. Hart, S. D., Michie, C. and Cooke, J. D. (2007). Precision of actuarial risk assessment instruments: Evaluating the ‘margins of error’of group v. individual predictions of violence. The British Journal of Psychiatry 190.S49 s60-s65.
8. Monahan, J. (2016). The individual risk assessment of terrorism: Recent developments. The handbook of the criminology of terrorism. p. 520–534.
9. OHCHR. (2022). Fight agaiinst Terrorism and Extremism in Xinjiang: Truth and Facts. Приступљено 14.09.2022.:

https://www.ohchr.org/sites/default/files/documents/countries/20220831/ANNEX_A.pdf

10. Seymour, J. D. and Anderson, R. M. (2015). New Ghosts, Old Ghosts: Prisons and Labor Reform Camps in China: Prisons and Labor Reform Camps in China. Routledge.
11. Woo, G. (2002). Quantitative terrorism risk assessment. The Journal of Risk Finance.
12. Влада Србије. (2017). Национална стратегија за спречавање и борбу против тероризма за период 2017–2021. године, „Службени гласник РС“, бр. 94 од 19. октобра 2017, Београд.
13. Влада Србије. (2020). Стратегија за борбу против прања новца и финансирања тероризма за период 2020–2024. године, „Службени гласник РС“, бр. 14/2020 Београд.
14. Народна скупштина. (2019). Стратегија националне безбедности Републике Србије, „Службени гласник РС“, бр. 94/2019-13, Београд.
15. National Money Laundering and Terrorist Financing Risk Assessment Toolkit. World bank. Приступљено 25.10.2022.

https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use

Appendix I:

Закони и други прописи Републике Србије у области организованог криминала, тероризма и екстремизма

01 Кривични законик
02 Законик о кривичном поступку
03 Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције
03-01 Уредба о евидентирању имовног стања лица која врше функцију, односно обављају послове и задатке у посебним организационим јединицама из Закона о организацији и надлежности државних органа у сузбијању организованог криминала
03-02 Правилник о организацији, раду и поступању са притвореницима у Посебној притворској јединици
04 Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала

05 Закон о организацији и надлежности државних органа у поступку за ратне злочине
06 Закон о Безбедносно-информативној агенцији
06-01 Уредба о начину евидентирања, обраде, чувања, коришћења, заштите и достављања другим надлежним државним органима информација и докумената о пословима из надлежности Безбедносно-информативне агенције
07 Закон о Војнобезбедносној и Војнообавештајној агенцији
07-01 Уредба о посебним критеријумима и поступку за пријем у радни однос и престанак радног односа у Војнобезбедносној агенцији и Војнообавештајној агенцији
08 Закон о полицији
08-01 Уредба о специјалној и посебним јединицама полиције
08-02 Правилник о полицијским овлашћењима
08-03 Правилник о начину обављања појединачних полицијских послова
08-04 Правилник о начину и условима примене полицијских овлашћења према малолетним лицима
08-05 Правилник о криминалистичко-форензичкој регистрацији, узимању других узорака и криминалистичко-форензичким вештачењима и анализама
08-06 Правилник о начину спровођења и методологији примене полиграфског испитивања
08-07 Правилник о начину вршења унутрашње контроле
08-08 Правилник о начину спровођења теста интегритета
09 Закон о спречавању прања новца и финансирања тероризма
10 Закон о ограничавању располагања имовином у циљу спречавања тероризма и ширења оружја за масовно уништење
11 Закон о националној бази података за спречавање и борбу против тероризма
12 Закон о спречавању корупције
12-01 Правилник о Регистру јавних функционера и Регистру имовине и прихода јавних функционера
13 Закон о одговорности правних лица за кривична дела
14 Закон о програму заштите учесника у кривичном поступку
14-01 Правилник о начину спровођења Програма заштите учесника у кривичном поступку у заводима за извршење заводских санкција
15 Закон о одузимању имовине проистекле из кривичног дела
16 Закон о информационој безбедности

16-01 Уредба о безбедности и заштити деце при коришћењу информационо-комуникационих технологија
16-02 Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја
16-03 Правилник о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја
17 Закон о заштити података о личности
18 Закон о тајности података
19 Закон о међународној правној помоћи у кривичним стварима

IMPROVEMENT OF THE STRATEGIC FRAMEWORK OF THE REPUBLIC OF SERBIA FOR PREVENTING AND COMBATING ORGANIZED CRIME, TERRORISM AND EXTREMISM: LESSONS FROM THE GREAT POWERS

Abstract

Due to the growing number of issues that contemporary states must overcome, academic research on societal phenomena including organized crime, terrorism, and extremism has recently gained more significance. The rising attention is mostly seen in the area of national security, given that all nations work to provide the bare minimum of security for their populations as well as for other protection targets including vital infrastructure, state boundaries, and conventional military security. In light of the security vulnerabilities that have been recognized for the Republic of Serbia in the third decade of the twenty-first century, this paper seeks to propose potential avenues for upgrading the strategic and legal framework of the country. The analysis is concentrated on the presentation of the flaws in the legal regulation of this topic and the potential for change. The authors first outline the pertinent positive legal standards before outlining a potential structure for the Republic of Serbia's strategic and normative corpus of acts based on lessons learned from the People's Republic of China, one of the potential role models for a superpower in the system of international relations. The authors provide a set of recommendations through the discussion that can be used as input parameters for software simulation of security risks in future research projects. These recommendations are made in addition to the systematic display of normative acts through the Register of Legal Regulations and other acts that regulate the struggle against the aforementioned security phenomena.

Keywords: organized crime, extremism, terrorism, national security, national security system, Serbia, People's Republic of China.

ПОЈЕДИНИ ЕЛЕМЕНТИ СТРАТЕШКО-НОРМАТИВНОГ ОДГОВОРА РЕПУБЛИКЕ СРБИЈЕ У СФЕРИ СУЗБИЈАЊА ТЕРОРИЗМА

Александра Илић [1]

Апстракт

Поједини облици криминалитета, попут тероризма, представљају феномене у вези са којима постоји висок степен сагласности како на глобалном тако и на националном нивоу о неопходности другачијег приступа у њиховом сузбијању. Специфичност реаговања подразумева с једне стране доношење одговарајућег нормативног оквира, уз претходно јасно постављене стратегијске циљеве, а с друге стране реализацију специјализације свих актера који учествују у различитим фазама кривичноправног реаговања на тероризам. У раду се анализирају поједини аспекти стратешко-нормативног одговора Републике Србије, пре свега у контексту могућег унапређења постојећих решења. Полази се од стратешког оквира постављеног у Националној стратегији за спречавање и борбу против тероризма за период 2017–2021. године, у контексту кривичноправног реаговања на тероризам, и указује на могуће правце унапређења стратегијских циљева у тој области посебно имајући у виду неопходност усвајања нове стратегије. Комплексност сузбијања тероризма подразумева разнолику активност државе на нормативном плану. С тим у вези, аутор анализира поједине аспекте те проблематике. С једне стране се бави питањем организације и надлежности државних органа у сузбијању тероризма и указује на пропусте у законском регулисању те области, као и начине побољшања постојећих решења.

---

[1] Факултет безбедности, Универзитет у Београду, e-mail: alex.mag.ilic@gmail.com

Рад је настао у оквиру пројекта Фонда за науку Републике Србије „Идеје“ – Пројекат акцелерације иновација и подстицања раста предузетништва у Републици Србији – Management of New Security Risks – Research and Simulation Development – NEWSIMR&D, #7749151.

С друге стране, специфичност кривичноправног реаговања огледа се и у контексту извршења казне затвора, па се тако лица осуђена на казну затвора за дела тероризма подвргавају специјалном режиму. Ту се поставља питање граница у другачијем третирању таквих осуђеника и важности поштовања људских права тих лица, што истовремено представља и стратегијски циљ Републике Србије.

Кључне речи: стратешко-нормативни одговор, тероризам, сузбијање, полиција, тужилаштво, судови, извршење казне затвора.

Увод

Нема сумње да се борба против појединих облика криминалитета, међу којима се налази и тероризам, у појединим аспектима разликује у односу на реаговање државних органа у погледу дела конвенционалног криминалитета. Специфичност и озбиљност кривичних дела која се налазе у надлежности посебних државних органа јесте основ и за другачије регулисање питања организације и надлежности тих органа.

Како би се та проблематика уредила свеобухватно, неопходно је предвидети посебну надлежност државних органа и организација у оквиру читавог система формалне социјалне контроле: полиције, тужилаштва, судова и затворског система. У том смислу, стратешко-нормативни оквир регулисања проблематике организације и надлежности државних органа у сузбијању тероризма подразумева с једне стране анализу стратешких докумената у области борбе против тероризма, док се с друге стране налазе сви закони и подзаконска акта која би требало на нормативном плану да разрађују основне смернице постављене у тим стратешким документима.

У области борбе против тероризма на стратешко-нормативном плану у Републици Србији имамо несрећену ситуацију. Последња усвојена стратегија у вези са тероризмом већ скоро годину дана није актуелна, па је неопходно донети нову која ће садржати адекватан пресек тренутне ситуације и нагласити важне кораке које би требало предузети у наредним годинама. Такође, и на нормативном плану се могу уочити одређена проблематична места која би било добро другачије уредити или попунити поједине празнине како би се унапредила борба против тероризма.

С тим у вези, у раду ће се анализирати још увек актуелна, иако застарела, стратегија за спречавање и борбу против тероризма, односно део стратегије који се дотиче питања организације и надлежности државних органа у сузбијању тероризма. Нормативна анализа ће обухватити на првом месту основни законски оквир који обрађује проблематику организације и надлежности полиције, тужилаштва, судова и затворског система у области борбе против тероризма уз

истовремено прављење паралеле, на одређеним местима, са општим организационим режимом поменутих органа формалне социјалне контроле.

Стратешки одговор Републике Србије у области кривичног гоњења и суђења за дела тероризма

Још увек важећи стратешки документ у области сузбијања тероризма у Републици Србији јесте Национална стратегија за спречавање и борбу против тероризма за период 2017–2021. година[2] (у даљем тексту: Национална стратегија). Имајући у виду да се ближи крај 2022. године, неопходно је доношење новог стратешког документа који би обухватио актуелни моменат и наредни период.

Национална стратегија разрађује стратегијске циљеве у четири приоритетне области. Прва приоритетна област се тиче превенције тероризма, насилног екстремизма и радикализације која води у тероризам. Друга приоритетна област се бави заштитом, уочавањем и отклањањем претњи од тероризма, као и слабостима у систему заштите. Трећа приоритетна област се односи на кривично гоњење за тероризам, уз поштовање људских права, владавине права и демократије. Последња приоритетна област представља одговор система у случају терористичког напада. За потребе овог рада биће анализирани одређени сегменти треће приоритетне области која обухвата три стратегијска циља: усклађеност националних прописа са одговарајућим резолуцијама Савета безбедности Уједињених нација, правним тековинама Европске уније и другим међународним стандардима, затим унапређен систем откривања, идентификације и кривичног гоњења извршилаца кривичног дела тероризам и кривичних дела повезаних са тероризмом, уз поштовање људских права и, на крају, ефикасно суђење за кривично дело тероризам и друга кривична дела повезана са тероризмом. С обзиром на то да је у раду акценат на питању организације и надлежности државних органа у сузбијању тероризма, тако ће се на овом месту направити осврт на други и трећи стратегијски циљ (стратегијски циљеви 3.2 и 3.3): унапређење система откривања, идентификације, кривичног гоњења извршилаца кривичних дела тероризма и ефикасно суђење за кривична дела тероризма.

Национална стратегија одређује кривично гоњење терориста као изграђен систем вођења истрага о актима тероризма и оптужења одговорних за извршење кривичног дела тероризам, односно кривичних дела повезаних са терористичким организацијама и терористичким активностима, која одликује правичност и ефикасност. Стратегијски циљ унапређења система откривања, идентификације и

[2] Национална стратегија за спречавање и борбу против тероризма за период 2017–2021. година („Службени гласник РС“, бр. 94/2017).

кривичног гоњења извршилаца кривичних дела тероризма остварује се кроз ефикасно кривично гоњење извршилаца кривичног дела тероризам и кривичних дела повезаних са овим кривичним делом, уз пуно поштовање људских права гарантованих Уставом, законима Републике Србије и међународним правом. Због природе кривичног дела, кривично гоњење захтева свеобухватност и мултидисциплинарни приступ, уз учешће различитих државних органа и организација које поседују специфична знања и вештине, како би се обезбедило квалитетно вођење кривичног поступка. Како би се остварио поменути стратегијски циљ, неопходно је да се развију кадровски, материјално-технички и стручни капацитети јавног тужилаштва и полиције, ојача међусобна сарадња, оствари пуна координација, те интензивира међународна сарадња, укључујући и сарадњу са Интерполом, Европолом и другим, као и међународно-правна помоћ у кривичним стварима, што представља услов успешног гоњења терориста и лица која чине мрежу подршке.

Стратегијски циљ који се односи на ефикасна суђења за кривична дела тероризма подразумева суђење лицима оптуженим за кривично дело тероризам и кривична дела повезаних са тероризмом, уз поштовање принципа правичног суђења, како би се омогућило да сви одговорни за тероризам буду процесуирани пред надлежним правосудним органима и да им у ефикасном судском поступку буде суђено уз поштовање људских права. Поменути стратегијски циљ треба да се оствари кроз настојања да се унапреде кадровски и стручни капацитети судова и ојача поверење јавности у њихову способност да се суоче са извршиоцима кривичног дела тероризам и других кривичних дела повезаних са тероризмом.

Када се упореде ова два истакнута стратегијска циља, може се уочити да им је заједничко стављање акцента на унапређење кадровских и стручних капацитета надлежних државних органа и организација, затим императив поштовања људских права окривљених лица, као и пуно поштовање правног оквира који одређује поступање у случајевима гоњења и суђења за дела тероризма. Ипак, поред многих заједничких карактеристика оба циља, може се уочити и једна битна разлика која осликава начелан однос државе према појединим актерима кривичноправне борбе против тероризма. Наиме, у оквиру стратегијског циља усмереног ка остварењу ефикаснијег суђења за дела тероризма помиње се, између осталог, јачање поверења јавности у способност судова да се суоче са извршиоцима кривичних дела тероризма у ширем смислу. Такве напомене нема у оквиру стратегијског циља који се бави положајем и улогом полиције и тужилаштва, чиме се јасно ставља до знања да се сва одговорност за евентуални (не)успех у вођењу поступака и суђењу за дела тероризма, без изузетка, сваљује на судове и на тај начин искључује се било каква одговорност осталих органа формалне социјалне контроле. Оваквом формулацијом о „јачању поверења јавности у способност судова да се суоче са извршиоцима кривичних дела

тероризма“ иде се линијом мањег отпора и уместо да се на истом месту истакне важност остваривања принципа судијске самосталности и независности, што су најважнији инструменти за суочавање судова са разним изазовима криминалитета у савремено доба, па и када је реч о кривичним делима тероризма, на овај начин се као важнији задатак поставља утицај на став јавног мњења, као да ће јавност да води поступак и пресуђује, а не органи поступка (тужилаштво и судови). Ако се погледа историја кажњавања, јасно је да је јавност представљена у народу одувек имала важну улогу у церемонијама јавних мучења, посебно током средњег века. Стварно и непосредно присуство народа у тим моментима неопходно је за њихово извршење јер мучење за које би се знало, али које би се одвијало у тајности, не би баш имало смисла (Foucault, 1995, p. 57, 58). Овако – бити сведок казне је као да се у кажњавању учествује, односно у контексту у којем се овде говори то се односи на учествовање у поступку одлучивања. Услед притиска јавности, независност и самосталност судова и судија, који поступају у конкретним предметима, у оваквим околностима могу бити озбиљно доведени у питање (Илић, 2017, стр. 221). С тим у вези, у новој националној стратегији за сузбијање тероризма неопходно је на другачији начин одредити механизме за остваривање поменутих стратегијских циљева, односно истаћи на подједнак начин одговорност свих државних органа и организација које учествују у кривичном гоњењу и суђењу за дела тероризма. Нарочито је важно истаћи улогу тужилаштва које према актуелној концепцији кривичног поступка има значајну улогу јer, између осталог, руководи и истрагом. Ново законско решење полази од претпоставке да највише оправдања има решење сагласно којем прикупљање доказа о учињеном кривичном делу и учиниоцу треба поверити органу који је за ово и иначе задужен и који ће у даљој фази поступка бити одговоран за оптужење, заступање оптужнице и њен успех на суду (Илић et al., 2022, стр. 834). Коначно, јачање принципа независности и самосталности свих државних органа који су део било ког кривичноправног процеса мора бити најважнији задатак државе, поменут како на стратешком тако и на нормативном плану. Свакако, без практичне реализације тог основног циља и најбољи стратешки и нормативни документи губе на значају.

Стратешки циљеви који се тичу унапређења система откривања, идентификације, кривичног гоњења извршилаца кривичних дела тероризма и ефикасног суђења за кривична дела тероризма разрађени су у одговарајућим законским решењима, о чему ће бити речи у наставку.

Организација и надлежност државних органа Републике Србије у сузбијању тероризма – опште одредбе

Основни законски оквир у контексту кривичноправног реаговања на тероризам чине закони који се примењују у пракси деловања свих органа формалне социјалне контроле. На том списку се налазе следећи закони: Кривични законик[3] (у даљем тексту: КЗ), Законик о кривичном поступку[4] (у даљем тексту: ЗКП), Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције[5] (у даљем тексту: ЗОНДОСОК), Закон о извршењу казне затвора за кривична дела организованог криминала[6] (у даљем тексту: ЗИКЗОК) и Закон о спречавању прања новца и финансирању тероризма[7] (у даљем тексту: ЗОСПНОФИТ).

Организација и надлежност државних органа у сузбијању тероризма регулисани су у ЗОНДОСОК који се примењује од 01. марта 2018. године. Пре тога је важио сличан Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела[8]. ЗОНДОСОК уређује образовање, организацију, надлежност и овлашћења државних органа и посебних организационих јединица државних органа, ради откривања, кривичног гоњења и суђења за кривична дела одређена овим законом. Поред низа других кривичних дела, предвиђених у члану 3 ЗОНДОСОК, изричито се помињу и кривична дела која се могу подвести под појам тероризма у ширем смислу, а која су прописана у КЗ. То су, поред основног кривичног дела тероризам (члан 391 КЗ), следећа кривична дела: кривично дело јавно подстицање на извршење терористичких дела (члан 391а КЗ), кривично дело врбовање и

---

[3] Кривични законик („Службени гласник“ РС, бр. 85/05, 88/05 – испр., 107/05 – испр., 72/09, 111/09, 121/12, 104/13, 108/14 и 94/16 и 35/19).

[4] Законик о кривичном поступку („Службени гласник РС“, бр. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 – одлука УС и 62/21 – одлука УС).

[5] Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције („Службени гласник РС“, бр. 94/2016 и 87/2018 – др. закон).

[6] Закон о извршењу казне затвора за кривична дела организованог криминала („Службени гласник РС“, бр. 72/09 и 101/10).

[7] Закон о спречавању прања новца и финансирања тероризма („Службени гласник РС“, бр. 113/2017 и 91/2019 и 153/20).

[8] Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела („Службени гласник РС“, бр. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004 – др. закон, 45/2005, 61/2005, 72/2009, 72/2011 – др. законик, 101/2011 – др. закон и 32/2013).

обучавање за вршење терористичких дела (члан 391б КЗ), кривично дело употреба смртоносне направе (члан 391в КЗ), кривично дело уништење и оштећење нуклеарног објекта (члан 391г КЗ), кривично дело финансирање тероризма (члан 393 КЗ) и кривично дело терористичко удруживање (члан 393а КЗ) (члан 2, став 1, тачка 5 ЗОНДОСОК). Треба истаћи и надлежност посебних државних органа и организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривично дело прање новца (члан 245 КЗ) у случају да имовина која је предмет прања новца потиче, између осталог, од поменутих кривичних дела тероризма у ширем смислу (члан 3, став 1, тачка 5 ЗОНДОСОК).

Према члану 4 ЗОНДОСОК, државни органи надлежни за поступање у предметима кривичних дела организованог криминала и тероризма јесу: Тужилаштво за организовани криминал, Министарство унутрашњих послова – организациона јединица надлежна за сузбијање организованог криминала, Посебно одељење Вишег суда у Београду за организовани криминал, Посебно одељење Апелационог суда у Београду за организовани криминал и Посебна притворска јединица Окружног затвора у Београду.

Организација и надлежност тужилаштва у сузбијању тероризма

Без обзира на назив појединих органа, односно организационих јединица, који искључиво садрже синтагму организовани криминал, неспорно је да се надлежност органа из члана 4 ЗОНДОСОК тиче откривања, кривичног гоњења и суђења за дела тероризма. Наиме, у члану 5, став 1 ЗОНДОСОК прописује се да је Тужилаштво за организовани криминал (у даљем тексту: Тужилаштво) надлежно за поступање у предметима кривичних дела из члана 3 ЗОНДОСОК за територију Републике Србије, што неспорно обухвата и дела тероризма. Такође, у члану 5, став 2 ЗОНДОСОК прописује да радом Тужилаштва руководи Тужилац за организовани криминал (у даљем тексту: Тужилац).

Ипак, приликом регулисања начина избора Тужиоца, односно избора заменика Тужиоца, ЗОНДСОК (у члану 5, став 3) истиче да предност имају кандидати који поседују потребна стручна знања и искуство из области борбе против организованог криминала и корупције. У вези са таквом одредбом морају се поставити два питања. Прво се тиче нејасноће због чега је, приликом прописивања потребних стручних знања и искуства која би кандидат за Тужиоца односно заменика Тужиоца требало да има, изостављена област борбе против тероризма. Да ли је то учињено случајно или је законодавац свесно то учинио, сматрајући да није потребно тражити од кандидата поседовање и тих додатних стручних знања и искустава? У прилог случајности такве одредбе говори раније решење из Закона о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела,

које је на идентичан начин регулисало исто питање, с том разликом што пређашњи закон нигде, па ни у свом називу, није истицао тероризам, осим приликом набрајања дела у ставу 2, у вези са којима је постојао посебан режим. Чињеница је да ни тада није било спорно да су посебни органи и организационе јединице државних органа надлежни за сузбијање и кривичних дела тероризма, али је проблем „игнорисања" стручних знања и искустава из области борбе против тероризма постојао и тада. Уместо да се у новом законском тексту који регулише организацију и надлежност државних органа у сузбијању посебно тешких кривичних дела, односно ЗОНДСОК, то питање уреди на адекватан начин, то је опет пропуштено да се учини. С друге стране, проблематику „непомињања" стручних знања и искустава из области борбе против тероризма треба посматрати и из другачијег угла. Питање је да ли би се, увођењем тог додатног критеријума, појавили кандидати за Тужиоца и заменика Тужиоца који би испуњавали све потребне услове у вези са стручним знањем и искуством. Ако се сагледа статистика откривања, кривичног гоњења и суђења за дела тероризма[9], онда се лако може доћи до закључка да прилика за стицање искуства у области тероризма у Републици Србији и није било много. Ипак, законодавац је могао једноставно да обухвати организовани криминал и тероризам заједно у оквиру одредбе која прописује услове за Тужиоца и заменика Тужиоца. Таквим обухватањем би се добила чиста норма која се садржински поклапа са њеним домашајем.

Може се поставити питање због чега законодавац помиње корупцију у оквиру одредбе која регулише услове за Тужиоца и заменика Тужиоца када се ради о поступању у предметима организованог криминала и тероризма, а нарочито имајући у виду да ЗОНДОСОК посебно уређује организацију и надлежност државних органа у сузбијању корупције (члан 13). Одговор се може наћи у проширеној надлежности државних органа који поступају у предметима организованог криминала и тероризма с обзиром на то да се према члану 3, став 1, тачка 2 ЗОНДОСОК предвиђа поступање поменутих органа и у предметима кривичних дела против службене дужности (чл. 359, 366, 367 и 368 КЗ), када је окривљени, односно лице коме се даје мито, службено или одговорно лице које врши јавну функцију на основу избора, именовања или постављења од стране Народне скупштине, председника Републике, Владе, опште седнице Врховног касационог суда, Високог савета судства или Државног већа тужилаца. Такође, у надлежности државних органа који поступају у предметима организованог криминала и тероризма налазе се и предмети кривичних дела против привреде (чл. 223, 223а, 224, 224а, 227, 228, 228а, 229, 230, 231, 232, 232а, 233, чл. 235, став

[9] Подаци за 2021. годину показују да нема ниједна пријава, оптужење, као ни осуда за неко дело тероризма, приступљено 01. новембра 2022. године: https://publikacije.stat.gov.rs/G2022/Pdf/G20221189.pdf

4, чл. 236 и 245 КЗ) ако вредност имовинске користи прелази 200.000.000 динара, односно ако вредност јавне набавке прелази 800.000.000 динара (члан 3, став 1, тачка 3 ЗОНДОСОК). С обзиром на то да се у последњем случају ради о кривичним делима против привреде, нејасно је такође зашто законодавац није истакао да је пожељно да кандидати за Тужиоца и заменика Тужиоца поседују потребна стручна знања и искуство из области борбе против привредног криминала, као што је то учинио приликом прописивања критеријума за постављење руководиоца одељења, односно распоређивање или упућивање заменика јавних тужилаца у посебно одељење вишег јавног тужилаштва за сузбијање корупције, у чијој се надлежности налазе поменута кривична дела против привреде када имовинска корист не прелази 200.000.000 динара, односно када вредност јавне набавке не прелази 800.000.000 динара. Наиме, законодавац је у члану 15, став 3 ЗОНДОСОК посебно истакао поседовање потребних стручних знања и искустава из области борбе против привредног криминала, а посебно из области сузбијања кривичних дела против службене дужности и корупције. У случају кривичних дела против привреде која се налазе у надлежности државних органа који поступају у предметима организованог криминала и тероризма то истицање би имало и већи значај јер се ради о тежим облицима тих кривичних дела с обзиром на вредност имовинске користи, односно вредност јавне набавке.

Организација и надлежност полиције у сузбијању тероризма

Полицијске послове у вези са кривичним делима из члана 3 ЗОНДОСОК обавља Министарство унутрашњих послова – организациона јединица надлежна за сузбијање организованог криминала. Организациона јединица надлежна за сузбијање организованог криминала поступа по захтевима Тужиоца, у складу са законом. Министар надлежан за унутрашње послове (министар полиције), уз прибављено мишљење Тужиоца, поставља и разрешава старешину организационе јединице надлежне за сузбијање организованог криминала и доноси акт којим ближе уређује организацију и рад организационе јединице надлежне за сузбијање организованог криминала, у складу са законом. Иако се и овде помиње само организовани криминал, јасно је да се надлежност посебне организационе јединице полиције односи и на сузбијање дела тероризма.

С тим у вези, у оквиру Управе криминалистичке полиције формирана је Служба за борбу против тероризма и екстремизма (у даљем тексту: Служба) која је надлежна за спречавање, откривање и расветљавање кривичних дела повезаних са тероризмом и екстремизмом, као и откривање и хватање извршилаца ових кривичних дела. Служба је основана у децембру 2013. године, проширењем Одељења за праћење и истраживање појава тероризма основаног 2007. године.

Служба за борбу против тероризма и екстремизма континуирано прати све безбедносно интересантне појаве и догађаје на територији Републике Србије и прикупља оперативна сазнања у вези са лицима, групом, организацијама и покретима чије је деловање повезано или се може довести у везу са тероризмом и/или екстремизмом, а у циљу спречавања извођења кривичних дела повезаних са тероризмом и екстремизмом у Републици Србији или коришћења територије Републике Србије за припрему или извођење оваквих акција у другим државама, као и спречавања активности пропагирања тероризма и екстремизма, врбовања и регрутовања, те обезбеђивања или прикупљања средстава намењених за финансирање ових активности. У својим активностима Служба блиско сарађује са другим организационим јединицама Министарства унутрашњих послова Републике Србије, надлежним органима Републике Србије (превасходно правосудним и безбедносно-обавештајним), као и надлежним институцијама партнерских држава, регионалним и глобалним организацијама и иницијативама. Служба континуирано прати нова достигнућа у циљу едукације у свим областима рада у борби против тероризма и екстремизма, кроз посете органима за спровођење закона других земаља, учешће на домаћим и међународним специјалистичким семинарима, научним и стручним скуповима. Служба се састоји од Одељења за борбу против тероризма и Одељења за борбу против екстремизма, као и четири теренска одсека, у Београду, Новом Саду, Нишу и Новом Пазару (МУП Републике Србије, 2022).

Специјална антитерористичка јединица (у даљем тексту: САЈ) јесте организациона јединица у саставу Дирекције полиције, Министарства унутрашњих послова (МУП Републике Србије, 2022). У складу са Уредбом о специјалним и посебним јединицама полиције[10], САЈ представља специјалну јединицу полиције (члан 2, став 2). САЈ је савремена, високопрофесионална антитерористичка јединица полиције, уско специјализована и опремљена најсавременијом специјалистичком опремом, намењена за извршавање сложених и високоризичних задатака безбедности и заштите Републике Србије и њених грађана. То се, између осталог, односи и на борбу против тероризма на тактичком нивоу. Намењена је за извршавање следећих високоризичних задатака, у складу са законским прописима и овлашћењима, попут: планирање и извршавање најсложенијих безбедносних задатака у борби против тероризма, интервенције у случају талачких ситуација, интервенције у случају отмице ваздухоплова и других кризних ситуација у ваздухопловима, интервенције у случајевима барикадирања и пружања отпора ватреним оружјем, и други задаци. Систем обуке

[10] Уредба о специјалним и посебним јединицама полиције („Службени гласник РС“, бр. 47/18, 59/18, 91/18, 29/19, 69/19, 66/20, 78/20, 102/20, 113/20, 133/20, 146/20, 149/20, 60/21, 83/21, 125/21, 67/22 и 83/22).

за припаднике САЈ-а чине: селективна обука, основна антитерористичка обука, виша антитерористичка обука и редовна обука готових снага. Поред обуке која се реализује у САЈ-у, део припадника се усавршава и обучава у наставним центрима и програмима у оквиру Министарства унутрашњих послова, наставним центрима Војске Србије, као и у програмима и активностима међународне сарадње у иностранству (МУП Републике Србије, 2022).

Организација и надлежност судова у сузбијању тероризма

За поступање у предметима кривичних дела тероризма надлежан је Виши суд у Београду, као првостепени, за територију Републике Србије (члан 7, став 1 ЗОНДОСОК). Надлежност врши Посебно одељење Вишег суда у Београду за организовани криминал (у даљем тексту: Посебно одељење Вишег суда) чијим радом руководи председник овог одељења (члан 7, став 2 и 3 ЗОНДОСОК). С тим у вези, председника Посебног одељења Вишег суда поставља председник Вишег суда у Београду из реда судија распоређених на рад у то одељење, на време од четири године (члан 7, став 4 ЗОНДОСОК). У оквиру исте одредбе регулишу се и услови који се траже за председника Посебног одељења Вишег суда, при чему ЗОНДОСОК истиче само обавезно поседовање професионалног искуства у одређеном трајању и одређеној области – десет година у области кривичног права без даљег прецизирања унутар те области.

Кад су у питању судије Посебног одељења Вишег суда, њих распоређује председник Вишег суда у Београду на време од шест година, уз њихову писмену сагласност (члан 7, став 5 ЗОНДОСОК). У погледу потребних услова, ЗОНДОСОК истиче да судија Посебног одељења Вишег суда мора имати најмање осам година професионалног искуства у области кривичног права (члан 7, став 5 ЗОНДОСОК). Основно правило је да се попуњавање посебних одељења неког суда чини из реда судија тог истог суда, што је у складу са Законом о судијама[11] (у даљем тексту: ЗОС), односно начелом непремештивости судија по којем судија има право да врши функцију у суду за који је изабран, осим у случајевима прописаним у ЗОС (члан 18, став 1). То даље значи да судија само уз своју сагласност може бити упућен из једног у други суд, при чему сагласност мора бити писмена и дата пре доношења решења о упућивању (члан 18, став 2 и 3 ЗОС). ЗОС регулише и стандардну процедуру упућивања судија у члану 20. С тим у вези, судија може бити упућен на рад само у други суд исте врсте и истог или непосредно нижег степена, најдуже годину дана, или, изузетно, судија може бити

[11] Закон о судијама („Службени гласник РС“, бр. 116/08, 58/09 – одлука УС, 104/09, 101/10, 8/12 – одлука УС, 121/12, 124/12 – одлука УС, 101/13, 111/14 – одлука УС, 117/14, 40/15, 63/15 – одлука УС, 106/15, 63/16 – одлука УС, 47/17 и 76/21).

упућен у суд непосредно вишег степена, ако испуњава законом прописане услове за избор за судију суда у који се упућује (члан 20, став 1 и 2 ЗОС). Судија се упућује у суд у коме недостатак, спреченост, изузеће судија или други разлози отежавају или успоравају рад суда доношењем решења о упућивању судије, уз његову сагласност, што чини Високи савет судства (члан 20, став 3 и 4 ЗОС). Према истим основним правилима, пре доношења решења о упућивању судије, Високи савет судства ће прибавити мишљење седнице свих судија суда у који је судија изабран и суда у који се упућује (члан 20, став 5 ЗОС).

Ипак, изузетно од одредаба Закона о судијама, Високи савет судства може упутити судију из другог суда на рад у Посебно одељење Вишег суда, на време од шест година, уз његову писмену сагласност (члан 7, став 6 ЗОНДОСОК). Судија који се упућује мора испуњавати услове из члана 7, став 5 ЗОНДОСОК (најмање осам година професионалног искуства у области кривичног права). Одступање у односу на општи режим огледа се у времену на које се судија из другог суда упућује на рад у Посебно одељење Вишег суда. У општем режиму је то најдуже годину дана, док је у случају упућивања у Посебно одељење Вишег суда то знатно дуже – шест година. Оправдање специјалног решења треба тражити у потреби да се обезбеди стабилност састава Посебног одељења Вишег суда у дужем временском периоду, у складу са правилом о распоређивању судија у Посебно одељење Вишег суда које чини председник Вишег суда – у оба случаја је то шест година.

Приликом распоређивања, односно упућивања у Посебно одељење Вишег суда, предност имају судије које поседују потребна стручна знања и искуство из области борбе против организованог криминала и корупције (члан 7, став 7 ЗОНДОСОК). Као и у случају прописивања критеријума за избор Тужиоца односно заменика Тужиоца, и за потенцијалне судије Посебног одељења Вишег суда важи исто. У том смислу, могу се истаћи исте примедбе које се тичу пропуста законодавца да предвиди борбу против тероризма, односно стручна знања и искуство у тој области као пожељну околност приликом селекције могућих кандидата за распоређивање, односно упућивање у Посебно одељење Вишег суда. Такође, ЗОНДОСОК ни овде не помиње стручна знања и искуство у области привредног криминала иако из члана 3, став 1, тачка 2 ЗОНДОСОК произилази надлежност Посебног одељења Вишег суда и у том случају.

За одлучивање у другом степену у предметима кривичних дела из члана 3 ЗОНДОСОК надлежан је Апелациони суд у Београду за територију Републике Србије, односно Посебно одељење Апелационог суда у Београду за организовани криминал (у даљем тексту: Посебно одељење Апелационог суда) (члан 8, став 1 и 2 ЗОНДОСОК). Радом Посебног одељења Апелационог суда руководи председник тог одељења кога поставља председник Апелационог суда у Београду из реда судија распоређених на рад у то одељење, на време од четири године, при

чему мора имати најмање 12 година професионалног искуства у области кривичног права (члан 8, став 3 и 4 ЗОНДОСОК). Судије у Посебно одељење Апелационог суда распоређује председник Апелационог суда у Београду, на време од шест година, уз њихову писмену сагласност. У погледу услова, ЗОНДОСОК прописује обавезно најмање десет година професионалног искуства судија у области кривичног права (члан 8, став 5). Као и у случају упућивања судија у Посебно одељење Вишег суда, тако и кад је у питању упућивање у Посебно одељење Апелационог суда, постоји одступање од временског ограничења трајања тог упућивања које је прописано у ЗОС. С тим у вези, ЗОНДОСОК предвиђа да Високи савет судства може упутити судију из другог суда на рад у Посебно одељење Апелационог суда, на време од шест година, уз његову писмену сагласност и обавезну испуњеност услова који се тиче година професионалног искуства у области кривичног права (члан 8, став 6 ЗОНДОСОК). Приликом распоређивања, односно упућивања у Посебно одељење Апелационог суда, предност имају судије које поседују потребна стручна знања и искуство из области борбе против организованог криминала и корупције. С обзиром на то да је и у овом случају на идентичан начин регулисано питање поседовања стручних знања и искуства као и у вези са распоређивањем, односно упућивањем судија у Посебно одељење Вишег суда, могу се истаћи исте примедбе и указати на важност бољег регулисања тог питања *de lege ferenda*.

Улога затворског система у сузбијању тероризма

Улога затворског система у области сузбијања тероризма долази до изражаја у две ситуације: издржавање притвора као мере за обезбеђење присуства окривљеног у кривичном поступку за дела тероризма и издржавање казне затвора изречене учиниоцима кривичних дела тероризма.

Притвор одређен у кривичном поступку за кривична дела из члана 3 ЗОНДОСОК, па самим тим и дела тероризма, издржава се у Посебној притворској јединици Окружног затвора у Београду (у даљем тексту: Посебна притворска јединица) (члан 10, став 1 ЗОНДОСОК). Посебна притворска јединица се налази на две локације – у оквиру централног објекта Окружног затвора у Београду који се налази у Бачванској улици и у оквиру зграде Специјалног суда у Устаничкој улици. Обе локације се формално воде као притворске јединице Окружног затвора у Београду. Министар надлежан за правосуђе ближе уређује организацију, рад и поступање са притвореницима у Посебној притворској јединици (члан 10, став 2 ЗОНДОСОК). У том смислу, постоји Правилник о организацији, раду и

поступању са притвореницима у Посебној притворској јединици[12] (у даљем тексту: Правилник о ОРП). Правилник је донет давно, 2005. године, пре доношења актуелног ЗКП, па је на одређеним местима неусклађен са актуелним процесним решењима (нпр. помињање истражног судије). Посебна притворска јединица је затвореног типа у којој се обављају послови физичко-техничког обезбеђења простора и лица, спровођење притвореника, вођење прописаних евиденција, послови здравствене заштите и административно-правни послови (члан 2, став 2 Правилника о ОРП). У Посебној притворској јединици образује се Одељење за обезбеђивање притвореника против којих се води кривични поступак за организовани криминал (члан 3, став 1 Правилника о ОРП). Сходно тумачењу употребљених израза у ЗОНДОСОК, требало би и овде сматрати да се у Посебној притворској јединици смештају и лица којима је изречен притвор због сумње да су извршили дело тероризма. У члану 6, став 1 Правилника о ОРП прецизира се ко може да буде смештен у Посебну притворску јединицу. У том смислу, наводи се да се прима лице против кога је одређен притвор решењем надлежног суда, као и лице у односу на које је донето решење о задржавању органа унутрашњих послова, због основане сумње да је извршило кривично дело из области организованог криминала или ратних злочина. Посебном притворском јединицом руководи начелник кога одређује министар надлежан за правосуђе на предлог директора Управе (члан 4, став 1 Правилника о ОРП).

С друге стране, посебна организација и надлежност у систему извршења кривичних санкција установљена је у погледу извршења казне затвора изречене за дела тероризма (и других посебно тешких кривичних дела). Основни проблем и дилема у вези са применом овог посебног режима извршења казне затвора, и самим тим разграничењем у односу на општи режим извршења казне затвора, уочава се у неусаглашеним законским решењима у погледу инкриминација у вези са тероризмом које се наводе у ЗИКЗОК, односно у КЗ. Наиме, кривично дело међународни тероризам које помиње ЗИКЗОК више не постоји у КЗ; сада је у оквиру члана 391 регулисано кривично дело тероризам које на јединствен и свеобухватан начин покрива оно што је раније било садржано у оквиру кривичних дела тероризам и међународни тероризам. Проблем је то што је у међувремену, изменама и допунама КЗ, као резултат реализације међународних обавеза Републике Србије насталих потписивањем одговарајућих конвенција, унет одређен број кривичних дела која такође потпадају под феномен тероризма, али која се не налазе на списку дела у односу на која се примењује посебан режим извршења из ЗИКЗОК, о чему је било речи на почетку рада. С тим у вези, логичким тумачењем одредаба о примени посебног режима извршења казне

[12] Правилник о организацији, раду и поступању са притвореницима у Посебној притворској јединици („Службени гласник РС“, бр. 81/05).

затвора долази се до закључка да се тај посебан режим не може успоставити у односу на учиниоце тих других дела тероризма уколико нису учињени од стране организоване криминалне групе када ће се третирати као дела организованог криминала. Јасно је да намера законодавца није била да изостави ова дела, с обзиром на то да у моменту доношења ЗИКЗОК она нису ни била предвиђена у КЗ, па је зато било неопходно ускладити одредбе ЗИКЗОК са актуелним одредбама КЗ. То још увек није учињено, па имамо ситуацију која не би смела да постоји. *De lege ferenda* би требало ускладити одредбе ЗИКЗОК са КЗ у погледу круга дела која се подводе под тероризам у ширем смислу и на која се примењује посебан режим извршења казне затвора (Илић, 2022, стр. 36, 37).

За извршење изречене казне затвора за кривична дела тероризма (као и других посебно тешких кривичних дела) образује се Посебно одељење за издржавање казне затвора за кривична дела организованог криминала у казнено-поправном заводу затвореног типа са посебним обезбеђењем (у даљем тексту: Посебно одељење) (члан 2, став 1 ЗИКЗОК). Уколико је пунолетним лицима, уз поменуту казну затвора, изречена мера безбедности обавезног психијатријског лечења и чувања у здравственој установи, обавезног лечења алкохоличара и обавезног лечења наркомана, као и лечења у току извршења казне затвора, у Специјалној затворској болници обезбеђују се посебне просторије под надзором (члан 2, став 2 ЗИКЗОК).

Посебно одељење се налази у казнено-поправном заводу затвореног типа са посебним обезбеђењем и организује се као посебна унутрашња организациона јединица изван састава служби у казнено-поправном заводу затвореног типа са посебним обезбеђењем (члан 2, став 1 Правилника о организацији и раду Посебног одељења за издржавање казне затвора за кривична дела организованог криминала[13] (у даљем тексту: Правилник о ОРПОЗАЗИКС)). Казнено-поправни заводи затвореног типа са посебним обезбеђењем јесу: Казнено-поправни завод у Београду – Падинска скела, Казнено-поправни завод у Пожаревцу – Забела и Казнено-поправни завод у Истоку (члан 3 Уредбе о оснивању завода за извршење кривичних санкција у Републици Србији[14]). Посебним одељењем руководи начелник Посебног одељења, који за свој рад и рад Посебног одељења одговара управнику завода, и кога распоређује директор Управе, на образложени предлог управника завода (члан 8, став 1 и 2 ЗИКЗОК). У Посебном одељењу организује се рад запослених на пословима одржавања реда и безбедности и пословима

[13] Правилник о организацији и раду Посебног одељења за издржавање казне затвора за кривична дела организованог криминала („Службени гласник РС“, бр. 37/10).

[14] Уредба о оснивању завода за извршење кривичних санкција у Републици Србији („Службени гласник РС“, бр. 20/06, 89/09, 32/10, 53/11 и 11/17).

здравствене заштите у сменама (члан 4, став 2 Правилника о ОРПОЗАЗИКС). Послове одржавања реда и безбедности у Посебном одељењу обављају запослени у заводима из службе за обезбеђење, који су посебно обучени и упућени на рад у Посебно одељење (члан 3 ЗИКЗОК). Само упућивање на рад у Посебно одељење може се реализовати уз сагласност службеног лица или без његове сагласности, ако за тим постоји потреба службе, што чини директор Управе за извршење кривичних санкција на предлог управника завода у коме се налази Посебно одељење, на време од шест месеци (члан 6, став 1 ЗИКЗОК).

Закључак

Анализа како стратешког тако и нормативног оквира проблематике организације и надлежности државних органа у сузбијању тероризма указује на неопходност одговарајућих измена у тој области. Постоје два основна проблема која се уочавају након спроведене анализе. Прва се тиче (не)актуелности појединих решења, односно читавих докумената, као у случају Националне стратегије. С тим у вези, неопходно је да се правовремено реагује и да се усклађују прописи са практичним захтевима борбе против тероризма који представља веома динамичну појаву како би се избегло да носиоци терористичких активности буду корак испред оних који треба да спрече ту активност. Савремене форме криминалитета иначе одликује способност брзог и лаког прилагођавања различитим околностима чега доносиоци одлука, у свим сегментима борбе против тероризма, треба да буду свесни.

Други основни проблем је недовољна разрађеност појединих законских одредаба које регулишу организацију и надлежност државних органа у сузбијању тероризма. Међу свим посебним формама криминалитета, у вези са којима постоји сагласност да је неопходно предвидети другачије реаговање органа формалне социјалне контроле у односу на форме конвенционалног криминалитета, тероризам је најслабије разрађен. Невидљив је у контексту прописивања захтева који се односи на поседовање стручних знања и искустава приликом селекције кандидата за Тужиоца, заменика Тужиоца и судије Посебних одељења Вишег и Апелационог суда. С обзиром на то да је у питању специфичан облик криминалитета, другачији од организованог криминалитета и корупције, законодавац би требало више да обрати пажњу на значај селекције носилаца правосудних функција којима је, између осталог, задатак процесуирање кривичних дела тероризма. Слична невидљивост постоји и у сегменту извршења казне затвора. Наиме, тешко је наћи објашњење за нереаговање законодавца и усклађивање извршних одредаба са материјалним у области тероризма иако је

прошла читава једна деценија од када су унете значајне, и још увек актуелне, измене у погледу прописивања кривичних дела тероризма у КЗ.

Имајући у виду све наведено, како би се унапредио одговор државе у области борбе против тероризма, неопходно је да се пажљиво размотре постојећа анализирана решења и унесу одговарајуће измене и допуне. Поменути стратешко-нормативни оквир није свакако једини сегмент те борбе, његово побољшање има смисла само ако је праћено одговарајућим решењима и у другим сегментима.

Библиографија

1. Закон о извршењу казне затвора за кривична дела организованог криминала („Службени гласник РС“, бр. 72/09 и 101/10).
2. Законик о кривичном поступку („Службени гласник РС“, бр. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 – одлука УС и 62/21 – одлука УС).
3. Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела („Службени гласник РС“, бр. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004 – др. закон, 45/2005, 61/2005, 72/2009, 72/2011 – др. законик, 101/2011 – др. закон и 32/2013).
4. Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције („Службени гласник РС“, бр. 94/2016 и 87/2018 – др. закон).
5. Закон о спречавању прања новца и финансирања тероризма („Службени гласник РС“, бр. 113/2017 и 91/2019 и 153/20).
6. Закон о судијама („Службени гласник РС“, бр. 116/08, 58/09 – одлука УС, 104/09, 101/10, 8/12 – одлука УС, 121/12, 124/12 – одлука УС, 101/13, 111/14 – одлука УС, 117/14, 40/15, 63/15 – одлука УС, 106/15, 63/16 – одлука УС, 47/17 и 76/21).
7. Илић, А. (2017). *Медији и криминалитет – криминолошки аспекти*. Докторска дисертација. Београд: Правни факултет.
8. Илић, А. (2022). *Коментар Закона о извршењу кривичних санкција*. Београд: Службени гласник.
9. Илић, П. Г., Бељански, С., Мајић, М. и Трешњев, А. (2022). *Коментар Законика о кривичном поступку*. Београд: Службени гласник.
10. Кривични законик („Службени гласник РС“, бр. 85/05, 88/05 – испр., 107/05 – испр., 72/09, 111/09, 121/12, 104/13, 108/14 и 94/16 и 35/19).
11. Национална стратегија за спречавање и борбу против тероризма за период 2017–2021. година („Службени гласник РС“, бр. 94/2017).
12. Правилник о организацији и раду Посебног одељења за издржавање казне затвора за кривична дела организованог криминала („Службени гласник РС“, бр. 37/10).

13. Правилник о организацији, раду и поступању са притвореницима у Посебној притворској јединици („Службени гласник РС“, бр. 81/05).
14. Републички завод за статистику. (2022). *Пунолетни учиниоци кривичних дела у Републици Србији, 2021*. Приступљено 01. новембра 2022. године: https://publikacije.stat.gov.rs/G2022/Pdf/G20221189.pdf
15. Специјална антитерористичка јединица (МУП), приступљено 15. октобра 2022. године: http://www.mup.gov.rs/wps/portal/sr/direkcijapolicije/ojdpp/specijalna+antiteroristicka+jedinica/saj
16. Служба за борбу против тероризма (МУП), приступљено 20. октобра 2022. године: http://www.mup.gov.rs/wps/portal/sr/direkcija-policije/
17. Уредба о оснивању завода за извршење кривичних санкција у Републици Србији („Службени гласник РС“, бр. 20/06, 89/09, 32/10, 53/11 и 11/17).
18. Уредба о специјалним и посебним јединицама полиције („Службени гласник РС“, бр. 47/18, 59/18, 91/18, 29/19, 69/19, 66/20, 78/20, 102/20, 113/20, 133/20, 146/20, 149/20, 60/21, 83/21, 125/21, 67/22 и 83/22).
19. Foucalt, M. (1995). *Dicipline & Punish: The Birth of the Prison*. Vintage books. New York: A division of random house, INC.

SOME ELEMENTS OF THE STRATEGIC AND NORMATIVE RESPONSE OF THE REPUBLIC OF SERBIA IN THE SPHERE OF COMBATING TERRORISM

Abstract

Certain forms of crime, such as terrorism, represent phenomena in connection with exist high degree of agreement both at global and national level on necessity of a different approach in their suppression. The specificity of the reaction means, on the one hand, the adoption of an adequate legal framework, with previously clearly defined strategic goals, and on the other hand, the realization of the specialization of all subjects which participate in different phases of the criminal law response to terrorism. In work it is analized some aspects of the strategic-normative responseer of Republic of Serbia, above all in the context of the possible improvement of existing solutions. It starts from the strategic framework set in the National Strategy for the Prevention and Combating of Terrorism for the period 2017-2021, in the context of the criminal law response to terrorism, and indicates possible directions for the improvement of strategic goals in that area, especially bearing in mind the necessity of adopting a new strategy. The complexity of combating terrorism implies diverse activity of the state on the normative

level. In this connection, the author analyzes certain aspects of that problem. On the one hand, it deals with the issue of the organization and competence of state authorities in the fight against terrorism, and points to shortcomings in the legal regulation of that area, as well as ways to improve existing solutions. On the other hand, the specificity of the criminal law response is also reflected in the context of serving a prison sentence, so persons sentenced to prison for acts of terrorism are subjected to a special regime. This raises the question of boundaries in the different treatment of such convicts and the importance of respecting the human rights of those persons, which at the same time represents a strategic goal of the Republic of Serbia.

Keywords: *strategic-normative response, terrorism, suppression, police, prosecution, courts, execution of prison sentence.*

СТРАТЕГИЈА НАЦИОНАЛНЕ БЕЗБЕДНОСТИ И УНУТРАШЊА БЕЗБЕДНОСТ – АНАЛИЗА ЗА РЕПУБЛИКУ СРБИЈУ

Јана Марковић [1]

Апстракт

Рад је настао у оквиру истраживања које је имало за циљ утврђивање начина на који је концепт приватне безбедности имплементиран у највишим правним и уједно стратешким документима држава из окружења и Европе. За Републику Србију, анализиране су стратегије националне безбедности од 2006. године, када је као таква постала независна држава. Како изучавање концепта приватне безбедности изискује разумевање унутрашње безбедности и националне безбедности, као виших инстанци, истраживањем је фокус стављен и на њих, превасходно на концепт унутрашње безбедности, којем је овај рад посвећен.

Аутор ће применити анализу садржаја релевантне домаће научне литературе и водећих – стратешких докумената у области националне безбедности како би читаоцу приближио концепт стратегије националне безбедности и концепт унутрашње безбедности, а потом и начин на који је концепт унутрашње безбедности интегрисан у домаћим стратешким документима у области безбедности.

У овом раду представљена је анализа Стратегија националне безбедности Републике Србије усвојених 2009. и 2019. године, и то са аспекта унутрашње безбедности. Унутрашња безбедност је узета као полазна основа и перспектива анализе с обзиром на то да је њено разумевање предуслов разумевања целине којој припада, али и елемената који је чине, како се остварује кроз делатност надлежних органа државне управе и рад правних лица, предузетника и физичких лица који врше послове приватног обезбеђења.

---

[1] Студент докторских студија, Факултет безбедности Универзитета у Београду, Београд; e-mail: 1996janamarkovic@gmail.com . Стипендиста Министарства просвете, науке и технолошког развоја.

Рад је настао у оквиру пројекта који финансира Фонд за науку Републике Србије у оквиру Програма „Идеје“ – Management of New Security Risks – Research and Simulation Development, NEWSIMR&D, #7749151.

Кључне речи: стратегија, национална безбедност, унутрашња безбедност, Република Србија.

Увод

Безбедност једне државе и њених конститутивних елемената, територије, становништва и суверенитета, постиже се у првом реду системом националне безбедности, који је управо и замишљен као апарат за достизање и одржавање жељеног нивоа безбедности у држави. Могуће га је дефинисати као „скуп функционално повезаних државних органа, органа локалне самоуправе и других организација, који, делујући у складу са правним поретком државе, теже да заштите унутрашњу и спољну безбедност државе, друштва и грађана“ (Драгишић, 2011, стр. 17).

Реч је о апарату који је са протоком времена, умножавањем и усложњавањем безбедносних изазова, ризика и претњи, континуирано и сам постајао већи и сложенији, са далеко већим могућностима, али и потенцијалним опасностима које их прате, а које саме и произилазе из тих могућности. Услед увећања и усложњавања задатака постављених у сфери националне безбедности, а нарочито послова унутрашње безбедности, део послова који је до тада био у искључивој надлежности државе и њених органа и служби почео је да се „пребацује“ на приватне субјекте – субјекте приватне безбедности. Тек са настанком приватних субјеката чије су активности директно или посредно увезане са безбедносном функцијом државе, односно њеним системом националне безбедности, могло се говорити о приватној безбедности.

Да би један овакав апарат, који обезбеђује опстанак и функционисање државе и друштва, био применљив и ефикасан, неопходна је адекватна нормативна основа која ће послужити за даљи развој нормативног оквира, институционални и организацијски развој, за утврђивање политике и смерница у области националне безбедности. Такву нормативну основу обезбедила би стратегија националне безбедности, као засебан документ, раздвојен, али не и изолован, од стратегије државе као вишег стратешког документа, стратегије одбране или стратегије унутрашње безбедности као нижих стратешких докумената.

Циљ рада јесте да читаоцу приближи концепте стратегије националне безбедности и унутрашње безбедности ради бољег разумевања предмета рада, односно, анализе начина на који је концепт унутрашње безбедности обухваћен највишим стратешким актом уједно у Републици Србији, за област националне безбедности и област унутрашње безбедности. Очекивани налази заснивају се на претпоставци да концепту унутрашње безбедности није посвећена пажња коју завређује услед недостатка њој кровне стратегије, као и недостатка дефинисања

кључних елемената потребних за свеобухватно одређење и потпуно разумевање овог елемента националне безбедности.

Поред уводних и закључних разматрања, рад је структуриран тако да обухвата три целине од којих је свака посвећена одређеном сегменту истраживања. Прва целина обухвата теоријско одређење стратегије националне безбедности јасно је разграничавајући са стратегијом државе и даје осврт на њену, не тако смислену, класификацију спроведену од стране државних органа. Друга целина разматра концепт унутрашње безбедности и њен однос са другим видовима безбедности, док је трећа целина садржински најнепосреднија предмету истраживања и бави се самом анализом концепта унутрашње безбедности у стратегијама националне безбедности Републике Србије. Поред наведених стратегија, у раду се прави осврт на још нека нормативна акта, попут стратегија из подручја деловања Министарства унутрашњих послова и Закона о полицији, како би се поткрепили изнети ставови, али је фокус задржан на самим стратегијама националне безбедности. То би значило да се проучавање концепта унутрашње безбедности са аспекта нормативних докумената не исцрпљује на овом месту, што оставља простор за нова истраживања овог концепта са аспекта других, нижих нормативних докумената. Исто тако, како је за теоријско одређење концепта унутрашње безбедности коришћена само домаћа литература, јер је фокус рада стављен на систем Републике Србије, даља истраживања би могла проширити листу референци са иностраним ауторима.

Основе стратегије националне безбедности

Стратегија би се могла дефинисати као најопштији плански документ креиран са идејом да се његовом имплементацијом остваре дефинисани свеобухватни и дугорочни циљеви. Из наведеног се може закључити да стратегије државе представљају планске документе донете на највишем нивоу општости у сврху остваривања дефинисаних свеобухватних и дугорочних циљева државе. Сходно томе, за остваривање таквих циљева државе у области (националне) безбедности доносе се стратегије (националне) безбедности. Овоме бисмо могли додати да је реч о стратешком документу политичког карактера, којим се одређују политике или правци политичког деловања у области (националне) безбедности.

Имајући у виду предмет овог рада, за појмовно одређење стратегије националне безбедности преузеће се схватање по којем она (стратегија националне безбедности) представља „услов, основ, усмеравајући и корективни документ једне државе (друштва) настао као израз уважавања општеприхваћених стандарда безбедносног организовања савремених држава... Друкчије речено, у стратегију националне безбедности је уткана црвена линија испод које држава неће и не може ићи у одбрани својих интереса“ (Стајић, 2015, стр. 320).

Република Србија је своју прву кодификовану Стратегију националне безбедности добила 2009. године чије је спровођење постало предуслов остваривања „потпуног и интегрисаног функционисања система националне безбедности, кроз координирано ангажовање свих државних органа и других субјеката који се баве пословима безбедности“, као и израде стратегијских докумената нижег нивоа општости, и уопште, нормативном уређењу делатности у оквиру система националне безбедности (Kovač, 2010, стр. 227). У актуелној Стратегији националне безбедности из 2019. године, а за разлику од њене претходнице, изричито се наводи да она (Стратегија националне безбедности) „представља полазну основу за израду других стратешких и доктринарних докумената, докумената јавних политика и нормативно-правних аката у свим областима друштвеног живота и функционисања државних органа и институција, ради очувања и заштите безбедности грађана, друштва и државе” (Стратегија националне безбедности Републике Србије, 2019).

Стратегија националне безбедности Републике Србије дефинише се као највиши стратешки документ „чијом реализацијом се штите национални интереси Републике Србије од изазова, ризика и претњи безбедности у различитим областима друштвеног живота“ (Закон о одбрани, 2007, члан 4), односно, „чијим спровођењем се штите националне вредности и интереси Републике Србије од изазова, ризика и претњи безбедности у свим областима друштвеног живота“ (Стратегија националне безбедности Републике Србије, 2019). Из наведеног се уочава одређена сличност у дефинисању, односно одређивању елемената дефиниције стратегије националне безбедности. Узимајући у обзир начин на који је она дефинисана у ранијој стратегији, као „најважнији стратешки документ којим се утврђују основе политике безбедности у заштити националних интереса Републике Србије“ (Стратегија националне безбедности Републике Србије, 2009), може се рећи да су претходно две наведене дефиниције садржајније и исправније. Наиме, стратегија је препозната као највиши, а не најважнији документ, чиме је начињен корак напред, обухваћени су објекат заштите – националне вредности и интереси, извор угрожавања безбедности – изазови, ризици и претње, и на крају, обухваћене су *све*, а не *различите* области друштвеног живота, чиме је такође начињен корак напред.

Иако се дефинише као највиши стратешки документ, треба имати у виду да се стратегија националне безбедности може појмити као највиши стратешки документ у области националне безбедности, али никако као највиши и најопштији такав документ који држава доноси. Самим тим, стратегија националне безбедности као „систем комплементарних норми, из домена државних стратегија које се непосредно односе на систем безбедности и на реализовање специфичних одбрамбених функција државе у политичкој, економској, правној, технолошкој, едукативној, информационој, војној, верској и

другим областима функционисања државе“ јесте „целовит и релативно трајан програм, чијом реализацијом треба да се остваре спољна и унутрашња безбедност државе, у миру и рату, кроз ефикасно решавање безбедносних ризика, изазова и претњи, ради заштите слобода, имовинске сигурности, права грађана и демократских тековина“ и разликује се од стратегије државе као „општег и интегралног програмског становишта за очување и достизање највиших националних (државних) вредности и интереса, уз ангажовање целокупних умних, духовних и материјалних потенцијала државе ради њене заштите и успешног развоја, кроз остваривање дефинисаних циљева у миру и рату“ (Kovač, 2003, стр. 26, 82). На основу изнетог теоријског одређења стратегије државе, могуће је извући закључак да Република Србија нема стратегију државе као општу стратегију која би представљала полазну основу за израду првобитно других стратешких и доктринарних докумената. Такође, упркос ставу да се стратегија националне безбедности налази на „хијерархијском врху полистратегијског система“, како су њоме операционализовани и формулисани национални интереси и циљеви од општих до појединачних и како се њоме операционализују посебне и појединачне стратегије (Đorđević i Katančević, 2016, стр. 129), узимајући у обзир један од критеријума класификације стратешких докумената[2], стратегија националне безбедности јесте општа када је у питању област националне безбедности и посебна у односу на стратегију државе.

На сајту Генералног секретаријата Владе Републике Србије[3] Стратегија националне безбедности из 2009. године сврстана је међу стратешке документе у области *Одбрана и спољна политика,* док се област унутрашњих послова уопште не препознаје као засебна. Оваквим чињењем, Стратегија националне безбедности је стављена у исту раван са другим стратегијама у односу на које би начелно требало да буде општа. Такође, додатно збуњује и то што на званичном сајту постоји извршена класификација само оних стратегија које су усвојене у периоду од 2001. до 2012. године.

Са друге стране, у истраживању које је спровео Републички секретаријат за јавне политике Владе Републике Србије рађена је анализа званичних стратешких докумената који су класификовани у 13 сектора, међу којима је и сектор унутрашњих послова. За сектор унутрашњих послова је издвојено 16 стратегија и, иако се оне појединачно не наводе, у извештају се закључује да се „Стратегија развоја Министарства унутрашњих послова (2011–2016) намеће као кровни

[2] Аутори дају три критеријума класификације стратешких докумената. За рад је као критеријум узет степен општости стратешких докумената, према којем се стратешка документа могу разврстати у три групе: општи, посебни и појединачни (Стајић, Радивојевић и Мираковић, 2017, стр. 1331).

[3] Приступљено 6.10.2022. преко https://www.gs.gov.rs/strategije-vs.html

документ“ (Републички секретаријат за јавне политике, 2014). У време када је истраживање рађено, наведена стратегија је била важећа, међутим, оно што ствара нејасноће јесте то да је и Стратегија националне безбедности једна од поменутих 16 стратегија, чиме се аутоматски она (Стратегија националне безбедности) поставила као нижи акт од Стратегије развоја Министарства унутрашњих послова. Сходно наведеном, оправдано је поставити питања (Стајић, Радивојевић и Мираковић, 2017, стр. 1332).

Појмовно одређење унутрашње безбедности

У домаћој регулативи, унутрашња безбедност се дефинише као систем са одређеном наменом и субјектима, који улази у састав извршног дела система националне безбедности. Тако, „систем унутрашње безбедности намењен је 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“ (Стратегија националне безбедности Републике Србије, 2019, стр. 5). Из наведене дефиниције јасно је ко/шта се штити, од чега се штити и ко штити. Међутим, одређење би било потпуније уколико би обухватило и начин на који се штити или којим активностима.

Стајић истиче да је унутрашња безбедност неизоставна компонента сваког система безбедности која се јавља као одговор на унутрашње појаве угрожавања (Стајић, 2015, стр. 44). Правећи разлику између унутрашње и спољне безбедности, Мијалковић дефинише прву као „заштићеност виталних друштвених вредности и интереса унутар граница земље, од угрожавајућих појава које првенствено настају изнутра или су комбиноване (потпомогнуте) са угрожавајућим факторима који долазе споља“ (Мијалковић, 2015, стр. 85). Под виталним друштвеним вредностима подразумева пре свега уставно уређење, политички, социјални и економски систем, људске слободе и права и животну средину.

Наведене вредности које се штите унутрашњом безбедношћу могу се одредити и као референтни објекти. Слично, Ивановић као референтне објекте унутрашње безбедности наводи политички и друштвено-економски поредак, уставно-правни поредак и јавни ред и мир, или шире – саму државу, а систем националне безбедности државе препознаје као референтни субјекат унутрашње безбедности (Ivanović, 2017, стр. 202). Иако би можда прецизније било рећи да је референтни

субјекат систем унутрашње безбедности, с обзиром на његову уску повезаност са осталим сегментима система националне безбедности, оправдано је задржати првобитно тумачење.

Сходно референтним објектима, односно „према непосредном објекту заштите“ (Милошевић, 2001, стр. 3) могла би се направити дистинкција између државне и јавне безбедности као компоненти унутрашње безбедности. Према томе, државна безбедност обухвата заштиту политичког, друштвено-економског и уставно-правног поретка, док јавна безбедност обухвата заштиту јавног реда и мира (Ivanović 2017, стр. 201), а оба правца безбедности заједно са „законом одређеним пословима управе“ чине област унутрашњих послова (Милетић и Талијан, 2011, стр. 9). Поред државне и јавне безбедности, аутори са једне стране одређују и војну безбедност (Милошевић, 2001, стр. 3; Милетић и Талијан, 2011, стр. 9), односно, са друге стране, додају заштиту и спасавање у ванредним ситуацијама и, у најширем смислу, заштиту животне средине (Форца, 2019, стр. 62) као део шире (унутрашње) безбедности. Овакво тумачење указује на корелацију између унутрашње и јавне безбедности као корелацију вишег и нижег појма. Узимајући у обзир одређивање јавне безбедности према два мерила – органском и функционалном, могуће је јавну и унутрашњу безбедност поставити у исту раван. Према органском мерилу, сва питања из надлежности полиције јесу питања која се сврставају у област јавне безбедности. Са друге стране, према функционалном мерилу, сва питања која омогућавају остваривање јавне безбедности без обзира у чијој надлежности се налазе сврставају се у област јавне безбедности (Милетић и Талијан, 2011, стр. 10). Могуће је уочити да, схваћена у функционалном смислу, јавна безбедност обухвата доста шири спектар послова, не везујући се стриктно за полицију. Полиција се сматра традиционалним субјектом јавне безбедности и све до приватизације јавне безбедности она је сматрана и главним субјектом. Данас, она је субјекат који „најчешће“ (Милетић и Талијан, 2011, стр. 9) спроводи послове јавне безбедности. Наиме, основна функција полиције као државног органа везује се за јавни поредак и, у првом реду, превенцију његовог нарушавања, репресију против оних који га нарушавају и стварање и одржавање услова стабилизације јавног поретка (Марковић, 2010, стр. 355). Међутим, иако главни, полиција није и једини субјекат јавне безбедности. Уколико се јавна безбедност класификује на традиционални јавни сектор и приватни сектор (Савић, 2007, стр. 72), онда су поред полиције у остваривању јавне безбедности задужени и приватни субјекти. Узимајући на овом месту претходна одређења унутрашње безбедности, као што је већ назначено, могуће је ставити знак једнакости између јавне и унутрашње безбедности. Ипак, док се у стратегијама националне безбедности термин „јавна безбедност“ не користи, у Закону о полицији се користи у контекстима поступања полиције у стању повећаног ризика по стање јавне безбедности и израде процене јавне безбедности (Закон о

полицији, 2016, чланови 24, 25 и 29). Из наведеног, уочава се терминолошка неусклађеност како између аутора који су се бавили овом тематиком, тако и у оквиру нормативних докумената, што представља озбиљну препреку разумевању ових концепта и њихових корелација.

У литератури се, међутим, може наћи другачији став који прави разлику између унутрашње и националне безбедности. Уважавајући научни приступ, аутори безбедност рашчлањују на унутрашњу (индивидуална, социјетална и национална) и међународну (регионална, глобална, заједничка, колективна и кооперативна) безбедност (Стајић и Гаћиновић, 2007, стр. 35), па се унутрашња безбедност, која се „често поистовећује са заштитом економске, политичке, правне и социјалне сигурности грађана“ (Ђукић, 2019, стр. 71), састоји од индивидуалне, социјеталне и националне безбедности и, сходно томе, национална безбедност је нижи појам од унутрашње безбедности, што се не подудара са одредбама позитивног законодавства којима се регулише ова област.

Дистинкција између унутрашње и међународне безбедности представљена је како би се обухватио и овај приступ у одређењу унутрашње безбедности и, иако има своје упориште и свакако није занемарљив (приступ), а како је већ наведено, с обзиром на то да не одговара тумачењу које је прописано регулативом, неће се узимати у даље разматрање. Да закључимо, реч је о концепту којим се обезбеђује заштита и континуирано функционисање унутрашњег уставног поретка, друштвеног, политичког, правног, економског, еколошког и сваког другог система на којем почивају вредности једног друштва и државе. Наведени циљеви остварују су интегрисаним деловањем субјеката унутрашње безбедности, који су подељени у две групе – надлежне органе државне управе и правна лица, предузетнике и физичка лица која врше послове приватног обезбеђења.

Прва група субјеката остављена је непотпуно прецизирана, па није до краја разјашњено ко овој групи припада. Сасвим сигурно да је то Министарство унутрашњих послова. Став да је реч о субјектима из сектора унутрашњих послова, правосуђа, безбедносно-обавештајног система, из инспекција и царине (Стајић и Гаћиновић, 2007, стр. 99) није потпуно прихватљив уколико се узме у обзир да је регулативом предвиђен безбедносно-обавештајни систем као засебан сегмент извршног дела система националне безбедности, а правосуђе сврстано у „друге субјекте значајне за националну безбедност“ (Стратегија националне безбедности Републике Србије, 2019, стр. 5). Уз то, области инспекција и царине припадају различитим министарствима, односно, у другом случају, Министарству финансија.

Друга група субјеката је делимично јасна, узимајући у обзир Закон о приватном обезбеђењу[4] који регулише ову област. Међутим, недостатак је што се оваквом регулативом не препознају субјекти који обављају детективску делатност као субјекти унутрашње безбедности, те се поставља питање да ли је то учињено намерно или је реч о пропусту. Става сам да је потребно поред одређивања правних лица, предузетника и физичких лица која врше послове приватног обезбеђења одредити и правна лица, предузетнике и физичка лица која врше послове из области делатности пружања детективских услуга као субјекте унутрашње безбедности. Услед наведеног, употреба појма приватног обезбеђења би могла бити ограничавајућа и унети нејасноће, алудирајући само на субјекте који врше за себе или друге субјекте послове заштите лица, имовине и пословања, послове транспорта новца, вредносних и других пошиљки или послове одржавања реда на јавним скуповима, спортским приредбама и другим местима окупљања грађана (редарска служба).

Наиме, потребно је најпре решити недоумицу по питању појмова „приватна безбедност“ и „приватно обезбеђење“, потом одредити субјекте приватне безбедности и субјекте приватног обезбеђења, а затим сагледавајући могућност тих субјеката да задовоље пред њих постављене задатке унутрашње безбедности одредити који је појам исправније користити. Уколико правна лица, предузетници и физичка лица која врше послове из области делатности пружања детективских услуга доприносе унутрашњој безбедности, онда би сасвим оправдано било заменити појам „приватно обезбеђење“ појмом „приватна безбедност“ или говорити о субјектима приватне безбедности, који су своју улогу у остваривању унутрашње безбедности добили оног тренутка када је полиција почела постепено да део својих овлашћења преноси на њих (субјекте приватног обезбеђења) услед увећања и усложњавања задатака постављених у сфери унутрашње безбедности.

Унутрашња безбедност у Стратегијама националне безбедности Републике Србије из 2009. и 2019. године

Уколико се посматра количина пажње која је посвећена унутрашњој безбедности у претходној и актуелној стратегији националне безбедности, уочљиво је да Стратегија националне безбедности из 2009. године садржи и те како више одредаба које се односе на предметну област.

Наиме, у Стратегији националне безбедности из 2019. године, унутрашња безбедност помиње се у оквиру одељка *5.1.2. Извршни део система националне безбедности,* на три места, и то као систем који улази у састав извршног дела

[4] Закон о приватном обезбеђењу („Службени гласник РС“, бр. 104/2013-8, 42/2015-3, 87/2018-312).

система националне безбедности и у виду послова унутрашње безбедности које поред надлежних органа државне управе обављају и правна лица, предузетници и физичка лица која врше послове приватног обезбеђења. Поред наведеног, у актуелној стратегији као један од националних интереса наводи се „очување унутрашње стабилности и безбедности (Републике Србије и њених грађана)“ (Стратегија националне безбедности Републике Србије, 2019, стр. 3, 4.2). Са друге стране, Стратегија националне безбедности из 2009. године препознаје концепт унутрашње безбедности као политику која заједно са политикама у другим областима друштвеног живота чини елемент политике националне безбедности. Целокупан одељак *4.4. Политика унутрашње безбедности* бави се наменом, субјектима, циљевима и предусловима ефикасног спровођења политике унутрашње безбедности.

Намена унутрашње безбедности обухваћена је обема стратегијама, с тим да се у претходној стратегији обухвата намена *политике* унутрашње безбедности као „заштита демократског политичког система, људских права и слобода, јавног реда и мира и имовинске сигурности грађана и других друштвених вредности“ (Стратегија националне безбедности Републике Србије, 2009, 4.4), док се у актуелној обухвата намена *система* унутрашње безбедности као „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“ (Стратегија националне безбедности Републике Србије, 2019, 5). Такође, узимајући у обзир саме одредбе које се односе на намену, њено одређење је свеобухватније у актуелној стратегији.

Као субјекти остваривања политике унутрашње безбедности препознати су законодавни, извршни и судски органи, као и „субјекти из области приватног обезбеђења чија делатност обухвата заштиту безбедности појединаца, објеката и других материјалних добара која није обухваћена заштитом надлежних државних органа“ (Стратегија националне безбедности Републике Србије, 2009, 4.4), што је и те како непрецизно одређење и различито од оног датог у актуелној стратегији.

Вредно помена јесте и навођење основних циљева политике националне безбедности и то „заштита уставног поретка, живота и имовине грађана, спречавање и сузбијање свих облика тероризма, организованог, финансијског, економског и високотехнолошког криминала, корупције, прања новца, трговине људима, наркоманије, пролиферације конвенционалног наоружања и оружја за масовно уништење, обавештајних и субверзивних делатности, као и других изазова, ризика и претњи безбедности“ (Стратегија националне безбедности Републике Србије, 2009, 4.4). Овакво набрајање циљева пропуштено је у актуелној стратегији, а као „замена“ за ову одредбу могло би се узети у обзир

истицање горенаведене намене система унутрашње безбедности. Међутим, навођење циљева како је то учињено у претходној стратегији употпуњује концепт унутрашње безбедности дат у највишем стратешком документу ове области.

Значајно у вези са циљевима јесте навођење њиховог усмерења „на поштовање и заштиту људских права и достојанства, као и на професионално, непристрасно и транспарентно извршавање послова уз уважавање обичајних, верских, културних и других особености етничких и других друштвених група и специфичности локалних заједница“ (Стратегија националне безбедности Републике Србије, 2009, 4.4), за шта се може рећи да доприноси гарантовању начела функционисања система националне безбедности попут професионалности и непристрасности.

Предуслови ефикасног спровођења политике унутрашње безбедности и остваривања циљева, а самим тим остваривања унутрашње безбедности попут „нормативне доградње делатности (...) одговарајућих стратегија, благовремено прикупљање и размена података и информација, координисање рада служби безбедности и јачање њихових организационих, људских и материјалних капацитета“ потпуно су изостављени у актуелној стратегији.

Значајни недостатак актуелне стратегије јесте непостојање одредаба о сарадњи субјеката унутрашње безбедности, а нарочито надлежних органа државне управе и субјеката који врше послове приватног обезбеђења. Ова питања су делимично обухваћена претходном стратегијом препознавши сарадњу државних органа са субјектима из области приватног обезбеђења и другим субјектима као „важну претпоставку остваривања и унапређења заштите живота и имовине грађана, људских и мањинских права“ (Стратегија националне безбедности Републике Србије, 2009, 4.4). Иако мање или више обухваћена другима правним документима[5], сматрам да је новом стратегијом начињен пропуст у погледу питања сарадње државних органа са субјектима из области приватног обезбеђења из разлога што би стратегија као највиши документ, који поставља основе за усмеравање активности државних органа и других субјеката у вршењу послова унутрашње безбедности, требало бар да помене питање сарадње.

У претходној стратегији препознат је значај јединственог система заштите и спасавања за остваривање унутрашње безбедности, као и деловање у ванредним ситуацијама проузрокованим елементарним непогодама и техничко-технолошким несрећама, ради заштите живота и имовине грађана, као једног од циљева предметне политике. Ове одредбе су такође изостављене у актуелној стратегији. Наведено, међутим, не видим као пропуст с обзиром на доношење регулативе у области ванредних ситуација, а потом и у области смањења ризика од катастрофа и управљања ванредним ситуацијама.

---

[5] Закон о полицији („Службени гласник РС“, бр. 6/2016, 24/2018) и

На крају овог дела, значајно је поменути и то да, иако Стратегија националне безбедности из 2009. године у *Закључку* предвиђа израду Стратегије унутрашње безбедности за шта би послужила као полазна основа, а којом би се област унутрашњих послова нормативно уредила посебним кровним документом специјализованим за њу, такав документ није израђен. Такође, у актуелној стратегији националне безбедности овакав документ се не наводи.

Како је унутрашња безбедност део националне безбедности, она доприноси деловању целокупног система националне безбедности и самим тим безбедности државе. Заједно са системом одбране, безбедносно-обавештајним системом и другим субјектима значајним за националну безбедност, са једне стране, и управљачким делом система националне безбедности, са друге стране, спроводи политику националне безбедности и остварује националне интересе којима се штите основне националне вредности. На тај начин, деловањем система унутрашње безбедности стварају се претпоставке за политички, економски, социјални, културни и укупни друштвени развој Републике Србије, а у односу на изазове, ризике и претње безбедности у окружењу. У актуелној стратегији националне безбедности говори се о „стратегијском“ окружењу. Слажем се са ставом да овакво дефинисање окружења повлачи извесне нејасноће (Станковић, 2021, стр. 84) и сматрам да је дефинисање окружења као „безбедносног“, што је и био случај у претходној стратегији националне безбедности, оправданије/исправније.

У светлу савремених безбедносних изазова, ризика и претњи, актуелна стратегија националне безбедности мање-више, а на сличан начин, обухватила је све изазове, ризике и претње са којима се Република Србија суочава, а који су обухваћени и претходном стратегијом. Не улазећи у детаљну анализу овог питања, потребно је пак указати на неколико ставки. Актуелна стратегија националне безбедности препознала је *масовне илегалне миграције* као значајни безбедносни изазов, чиме је начињен значајан корак напред у изради овог стратешког документа и постављања основа за даље деловање као одговор на њих. Актуелна стратегија националне безбедности је и нешто свеобухватније препознала *Епидемије и пандемије* као изазов чије се последице осећају од 2020. године, него што је то учињено претходном. *Климатске промене* идентификоване су у актуелној стратегији такође као посебан изазов, с тим да није јасно зашто је из актуелне стратегије избачен претходно утврђен изазов – *неконтролисано трошење природних ресурса и угрожавање животне средине.* Такође, није јасно зашто је исто учињено у вези са изазовима – *деструктивно деловање појединих верских секти и култова* и *нерешен статус и тежак положај избеглих, прогнаних и интерно расељених лица.* Посебно, са аспекта унутрашње безбедности, пажњу привлачи нејасноћа у вези са *корупцијом* као посебним изазовом. Наиме, корупција је у Стратегији националне безбедности из 2009. године била

препозната као посебан изазов, уврштена на значајном месту, одмах до организованог криминала, док је у актуелној стратегији изостављена као посебан изазов. Конкретније, она се у актуелној стратегији наводи као један од облика организованог криминала и као један од других изазова, ризика и претњи безбедности, који *може* испољити значајан утицај. Даље, истиче се да она (корупција) „често не испољава отворен утицај на безбедност Републике Србије, па ју је тешко открити и препознати обрасце њеног деловања“ (Стратегија националне безбедности Републике Србије, 2019, стр. 4). Збуњује то што се у стратегији користи реч „може“, што имплицира само на постојање могућности проузроковања (негативног) утицаја, негирајући тиме извесност штетних последица коруптивног деловања. Уз то, намеће се питање да ли то што је дела корупције теже открити, те препознати обрасце њеног испољавања узето као критеријум за њено уврштавање у *друге изазове, ризике и претње.* Можда је овакво категорисање корупције повезано са одлуком да се не дефинише и усвоји нова стратегија која би се бавила овим безбедносним проблемом.[6] Оправдано је и питање које поставља Станковић, а које указује на нејасноћу навођења корупције као једног од облика организованог криминала, док се илегалне миграције наводе такође као један од облика организованог криминала, али и као засебан изазов (Станковић, 2021, стр. 91).

Како у области унутрашње безбедности стратегија националне безбедности као кровни документ није једини документ ове врсте, радом је обухваћена анализа других стратегија које спадају у подручје деловања Министарства унутрашњих послова. Треба имати на уму да стратешки документ не мора нужно да садржи термин „унутрашња безбедност“ да би се закључило да он доприноси остваривању овог вида безбедности. Међутим, како је анализа извршена управо користећи овај термин, резултати анализе не пружају превише и указују само на један документ – *Стратегију интегрисаног управљања границом у Републици Србији за период 2022–2027. године.* Концепт унутрашње безбедности у овом стратешком документу обухваћен је у контексту смањења ризика и подизања свеукупне унутрашње безбедности (мисија и визија), подржано вршењем граничне провере, анализом ризика и успостављањем међународне сарадње у овој области.

87/2018; МУП Дирекција полиције. 2017. *Стратешки план полиције за период 2018–2021. године – јавна верзија*. МУП; Закон о приватном обезбеђењу. 2013. „Службени гласник РС“, бр. 104/2013-8, 42/2015-3, 87/2018-312.

[6] Република Србија имала је од 2005. године стратегију за борбу против корупције, а последња је била Национална стратегија за борбу против корупције у Републици Србији за период од 2013. до 2018. године.

Закључак

Када је реч о концепту унутрашње безбедности и његовој разради у Стратегијама националне безбедности Републике Србије из 2009. и 2019. године, може се рећи да је учињено назадовање. У претходној стратегији (из 2009. године) политика унутрашње безбедности препозната је као посебан елемент у оквиру политике националне безбедности, док то није случај са тренутно важећом стратегијом, у којој се обрађује свеобухватна политика националне безбедности као таква. Самим тим, овом концепту је у ранијој стратегији била посвећена доста већа пажња, него што је то учињено новом стратегијом. Иако су одређене одредбе претходне стратегије, попут оне која се односи на систем заштите и спасавања и деловања у ванредним ситуацијама, изостављене и то сасвим оправдано јер су постале засебно регулисана материја у оквирима материје унутрашње безбедности, постоје одредбе које је требало задржати новом стратегијом.

На крају, значајно би било утврдити зашто не постоји Стратегија унутрашње безбедности која ће бити *највиши стратешки документ у области унутрашње безбедности*. Наведеном иде у прилог то да је, са једне стране, доношење ове стратегије било предвиђено Стратегијом националне безбедности из 2009. године, док, са друге стране, Република Србија има Стратегију одбране која представља нижи стратешки документ у односу на Стратегију националне безбедности.

Такође, уколико се осврнемо на регулативу унутрашњих послова и Закон о полицији[7], интересантно је да је до 2005. године постојао закон који је у свом називу садржао термин „унутрашњи послови“, који је замењен Законом о полицији. Са друге стране пак нацрт закона који би заменио тренутно важећи Закон о полицији, који је ушао у јавну расправу, а који је потом и повучен из ње, у свом називу садржао је термин „унутрашњи послови“. У тренутно важећем Закону о полицији на само једном месту се помиње *унутрашња безбедност,* и то у контексту образовања помоћне полиције када је потребно надокнадити ангажовање великог броја полицијских службеника ради извршења задатака „када је угрожена унутрашња безбедност“ (Закон о полицији, 2016, члан 249).

Стратегија унутрашње безбедности, по угледу на Стратегију одбране, могла би да обухвати безбедносно окружење са аспекта унутрашње безбедности Републике Србије, идентификовање изазова, ризика и претњи безбедности од значаја за унутрашњу безбедност, формулисање интереса и циљева у области унутрашње безбедности, утврђивање политике унутрашње безбедности, структуру, управљање и начела функционисања система унутрашње безбедности Републике Србије. На тај начин, Стратегија националне безбедности остала би „окрњена“ за ближе регулисање унутрашње безбедности (као што је већ „окрњена“ за ближе

[7] Закон о полицији („Службени гласник РС“, бр. 6/2016, 24/2018 и 87/2018).

регулисање одбране), али би се предметној области посветила подједнака пажња као и области одбране.

Да би измена постојећих и/или писање нових нормативних докумената било оправдано, а сами документи адекватно написани, теоријски усклађени и практично применљиви, неопходно је првенствено извршити анализу појмовног апарата који се користи у овим документима, дефинисати нове и редефинисати постојеће појмове и тиме обезбедити њихову усаглашеност. Добар почетак могао би бити дефинисање појмова као што је унутрашња безбедност и њеног односа са, рецимо, јавном или спољном безбедношћу. Додајући наведеном, посвећивањем веће пажње стилу и језику писања, искључиле би се појмовна неусклађеност и могуће нејасноће и несугласице као последица те неусклађености. Укључивање организација цивилног друштва, академске и стручне јавности у писање ових докумената од нарочитог је значаја.

Комплетној области унутрашње безбедности потребно је приступити обухватније и систематичније него што је то чињено до сада. Да ли ће се то учинити редефинисањем постојећег стратешког документа или усвајањем новог који ће бити уједно и прави кровни стратешки документ области унутрашње безбедности, остаје отворено питање. Тако ће бити све док се међу одговорнима не покрене иницијатива и створи свест о потреби да се области унутрашње безбедности посвети већа пажња у нормативном и практичном смислу.

Библиографија

1. Влада Републике Србије Генерални Секретаријат. Приступљено 6.10.2022. преко https://www.gs.gov.rs/strategije-vs.html
2. Драгишић, З. (2011). *Систем националне безбедности Републике Србије*. Београд: Универзитет у Београду, Факултет безбедности.
3. Đorđević, D. R. i Katančević, V. (2016). Komparativna analiza strategijsko-doktrinarnih dokumenata u sferi bezbednosti i odbrane. *Vojno delo* 68 (3): 122–40. doi:10.5937/vojdelo1603122D.
4. Ђукић, С. (2019). Нарушавање јавног реда и мира као облик угрожавања унутрашње безбедности. *Војно дело* 71 (1): 70–84. doi:10.5937/vojdelo1902131D.
5. Закон о одбрани. (2007). *Службени гласник РС*, бр. 116/2007, 88/2009, 88/2009 – др. Закон, 104/2009 – др. Закон, 10/2015 и 36/2018.
6. Закон о полицији. (2016). *Службени гласник РС*, бр. 6/2016, 24/2018 и 87/2018.
7. Закон о приватном обезбеђењу. (2013). *Службени гласник РС*, бр. 104/2013-8, 42/2015-3, 87/2018-312.
8. Ivanović, A. R. (2017). Pojam i elementi nacionalne bezbednosti. *Pravne teme* 5(9): 186–211.

9. Kovač, M. (2003). *Strategijska i doktrinarna dokumenta nacionalne bezbednosti – teorijske osnove*. Beograd: Svet knjige.
10. Kovač, M. (2010). Strategija nacionalne bezbednosti Republike Srbije. U: *Srbija u savremenom geostrateškom okruženju*, priredili Slavica Đerić Magazinović i Nevenka Jeftić Šarčević, 215–229. Beograd: Medija centar „Odbrana"; Institut za međunarodnu politiku i privredu; Ministarstvo odbrane Republike Srbije, Sektor za politiku odbrane, Institut za strategijska istraživanja.
11. Марковић, Р. (2010). *Уставно право*. Београд: Правни факултет Универзитета у Београду и Службени гласник.
12. Мијалковић, С. (2015). *Национална безбедност.* Београд: Криминалистичко-полицијска академија.
13. Милетић, С. и Талијан, М. (2011). *Јавна безбедност – послови и начини рада, организација и руковођење*. Нови Сад: Факултет за правне и пословне студије др Лазар Вркатић.
14. Милошевић, М. (2001). *Систем државне безбедности*. Београд: Полицијска академија.
15. МУП Дирекција полиције. (2017). *Стратешки план полиције за период 2018–2021. године – јавна верзија. МУП*. Преузето са: http://www.mup.rs/wps/wcm/connect/c206983b503f4ebfbf5b8d5bc65ca8e3/Strateski+plan+policije+-+Javna+verzija-WEB.pdf?MOD=AJPERES&CVID=m3r4AMv
16. Републички секретаријат за јавне политике. (2014). *Анализа стратешких докумената*. Републички секретаријат за јавне политике. Преузето са http://vs3836.cloudhosting.rs/malodrvo/analiza-strategija.pdf
17. Савић, А. (2007). *Национална безбедност*. Београд: Криминалистичко-полицијска академија
18. Стајић, Љ. и Гаћиновић, Р. (2007). *Увод у студије безбедности*. Београд: Драслар партнер.
19. Стајић, Љ., Радивојевић, П. Н. и Мирковић, М. В. (2017). Неки аспекти политике унутрашње безбедности као елемента Стратегије националне безбедности Републике Србије. *Зборник радова Правног факултета у Новом Саду* 51(4): 1325–1342. doi:10.5937/zrpfns51-16569.
20. Стајић, Љ. (2015). *Основи система безбедности – са основама истраживања безбедносних појава.* Нови Сад: Правни факултет у Новом Саду.
21. Станковић, Н. (2021). Концепт људске безбедности у стратегији националне безбедности из 2019. године – корак уназад. *Политика националне безбедности* 20(1): 75-109. doi:10.22182/pnb.2012021.5.
22. Стратегија интегрисаног управљања границом у Републици Србији за период 2022–2027. године. (2022). *Службени гласник РС*, бр. 89/2022.
23. Стратегија националне безбедности Републике Србије. (2009). *Службени гласник РС*, бр. 88/2009.

24. Стратегија националне безбедности Републике Србије. (2019). *Службени гласник РС*, бр. 94/2019.
25. Форца, Б. (2019). Теоријско одређење функција система националне безбедности. *Безбедност* 61(1): 40–69. doi:10.5937/bezbednost1901040F.

STRATEGY OF NATIONAL SECURITY AND INTERNAL SECURITY – ANALYSIS FOR THE REPUBLIC OF SERBIA

Abstract

The work is the result of research that aimed to determine the way in which the concept of private security was implemented in the highest legal and at the same time strategic documents of countries from the surrounding area and Europe. For the Republic of Serbia, national security strategies have been analyzed since 2006, when it became an independent state as such. As the study of the concept of private security requires an understanding of internal security and national security, as higher instances, the research focused on them as well, and primarily on the concept of internal security.

The author will use the analysis of the content of relevant scientific literature and leading strategic documents in the field of national security in order to bring the concept of national security strategy and the concept of internal security closer to the reader, and then the way in which the concept of internal security is integrated in domestic strategic documents in the field of security.

This paper presents an analysis of the national security strategies of the Republic of Serbia adopted in 2009 and 2019 from the aspect of internal security. Internal security is taken as the starting point and perspective of the analysis, given that it is realized through the activities of competent state administration bodies and the work of legal entities, entrepreneurs and individuals who perform private security services.

Keywords: *strategy, national security, internal security, Republic of Serbia.*

СТРАТЕГИЈА НАЦИОНАЛНЕ БЕЗБЕДНОСТИ РЕПУБЛИКЕ СРБИЈЕ И ПРИВАТНО ОБЕЗБЕЂЕЊЕ

Горан Ј. Мандић[1]

Апстракт

Иако је матични закон који уређује област приватног обезбеђења, Закон о приватном обезбеђењу, донет тек 2013. године, та чињеница не оспорава раније регулисање ове области неким другим документима. Наиме, значај и улога приватног обезбеђења у спровођењу политике унутрашње безбедности препознати су Стратегијом националне безбедности Републике Србије из 2009. године. Њоме се такође указивало на потребу и неопходност сарадње приватног обезбеђења са другим субјектима националне безбедности, пре свега органима државне управе, као и на већем степену уређености ове области како нормативно, тако и доктринарно, чиме се недвосмислено указује на значај коју приватно обезбеђење има у заштити националних вредности и интереса. Са друге стране, у Стратегији националне безбедности Републике Србије из 2019. године може се приметити значајно другачији приступ према приватном обезбеђењу с обзиром на мањак доследности у дефинисању одређених елемената ове области. Услед недостатка одредби које би регулисале питање сарадње, као и уређености приватног обезбеђења, а све у циљу очувања и унапређења националне безбедности, одаје се утисак да је начињен пропуст који би потенцијално могао носити са собом дугорочне последице. Иако је питање сарадње детаљно обрађено, може се довести у питање легитимитет одредби нижег правног акта који адекватну потпору за своје одредбе не налази у највишим стратешким документима једне државе каква је Стратегија националне безбедности. Но, оправдање за нижи степен општости/свеобухватности стратегије из 2019. године у односу на поменуту из 2009. године, може се пронаћи управо у доношењу

[1] Ванредни професор; Факултет безбедности Универзитета у Београду, Београд; e-mail: goran.mandic@fb.bg.ac.rs.

Рад је настао у оквиру пројекта који финансира Фонд за науку Републике Србије у оквиру Програма „Идеје“ – Management of New Security Risks – Research and Simulation Development, NEWSIMR&D, #7749151.

закона коме је, условно речено, „делегирала“ послове дефинисања и регулисања неких питања у поменутој области, док, из објективних разлога, иста могућност није постојала 2009. године.

Кључне речи: стратегија националне безбедности, приватно обезбеђење, Закон о приватном обезбеђењу.

Увод

Стратегија националне безбедности Републике Србије јесте највиши стратешки документ чијим се спровођењем штите националне вредности и интереси Републике Србије од изазова, ризика и претњи безбедности у свим областима друштвеног живота (Стратегија националне безбедности, 2019, стр. 1).

Приватно обезбеђење обухвата пружање услуга, односно вршење послова заштите лица, имовине и пословања физичком и техничком заштитом када ти послови нису у искључивој надлежности државних органа, као и послове транспорта новца, вредносних и других пошиљки, одржавања реда на јавним скуповима, спортским приредбама и другим местима окупљања грађана (редарска служба), које врше правна лица и предузетници регистрована за ту делатност, као и правна лица и предузетници који су образовали унутрашњи облик организовања обезбеђења за сопствене потребе. Притом, услуге приватног обезбеђења не спадају у полицијске или друге послове безбедности које врше органи државне управе (Закон о приватном обезбеђењу, 2013, члан 2).

Институционализација приватног обезбеђења остварена је 2013. године доношењем закона који је правно уредио ову област. У међувремену, до данас су спроведене две измене и допуне закона, а донесени су и одређени подзаконски акти којим је требало ближе уредити поменуту област.

Приватно обезбеђење у склопу свог делокруга послова и са својим материјалним и људским ресурсима може представљати значајан део система националне безбедности Републике Србије. Међутим, да би оно (приватно обезбеђење) постало део система националне безбедности, неопходно је да буде стварно, а не само формално, прихваћено као партнер Министарства унутрашњих послова у остваривању појединих сегмената безбедности у Републици Србији.

Први и основни корак у остварењу поменутог јесте адекватно укључивање и презентовање употребе приватног обезбеђења кроз основни стратешки документ – кроз Стратегију националне безбедности Републике Србије којом се утврђују основе политике безбедности у заштити националних интереса.

Анализа стратегија из 2019. и 2009. године требало би да укаже на трендове (не)прихватања приватног обезбеђења као равноправног партнера у остваривању неких сегмената безбедности на теритирији Републике Србије.

Анализа стратегија националне безбедности Републике Србије

Анализа Стратегије националне безбедности из 2019. године

У Стратегији националне безбедности РС из 2019. године (у даљем тексту Стратегија из 2019. године), Службени гласник РС, број 94/2019, приватно обезбеђење се помиње у поглављу 5.1.2. „Извршни део система националне безбедности“, и то на следећи начин:

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.

Прво, Стратегија националне безбедности је највиши стратешки документ Републике Србије у области заштите националних вредности и интереса.

Друго, у овом документу, ово је једина одредба која изричито дозвољава да послове унутрашње безбедности обављају субјекти који нису надлежни органи државне управе.

Треће, може се уочити неусаглашеност у погледу одређења ових субјеката.

Ако упоредимо горенаведену одредбу и одредбу на почетку овог поглавља стратегије:

Извршни део система националне безбедности извршава задатке у зависности од врсте и начина испољавања изазова, ризика и претњи безбедности, ангажовањем: војних и полицијских снага, служби безбедности, ватрогасно-спасилачких јединица, јединица цивилне заштите, комуналне милиције, царине, службе за обезбеђење у заводима за извршавање кривичних санкција, правосудне страже, ***служби и агенција за обезбеђење личности и објеката****, великих техничко-технолошких система, привредних друштава, других правних лица, удружења, предузетника и грађана.*

можемо рећи да је нејасно шта се подразумева под појмовима *служби и агенција за обезбеђење личности и објеката.*

Четврто, ова одредба сужава поље деловања ових субјеката само на послове унутрашње безбедности.

На основу изнетог, могуће је закључити да Стратегија из 2019. год. допушта да као једна од компоненти система националне безбедности буде **приватна безбедност**.

Међутим, да ли је овакав закључак исправан?! У стратегији се нигде не користи термин приватна безбедност већ термин приватно обезбеђење. Како је приватно обезбеђење ужи појам од приватне безбедности, следи да стратегија допушта да као једна од компоненти система националне безбедности буде **приватно обезбеђење**.

Уколико се имплицира на постојање јавне и приватне компоненте безбедности, те се за јавну компоненту безбедности везује јавна безбедност, зашто се за приватну компоненту безбедности везује приватно обезбеђење?! Остаје неразјашњено.

Анализа Стратегије националне безбедности из 2009. године

Анализирајући Стратегију националне безбедности РС из 2009. године[2], уочава се следеће:

Прво, препозната је све већа одговорност у спровођењу политике унутрашње безбедности субјеката из области приватног обезбеђења.

Друго, јасно је дефинисана њихова делатност која обухвата заштиту безбедности појединаца, објеката и других материјалних добара која није обухваћена заштитом надлежних државних органа.

Треће, јасно је препозната потреба за уређењем ове делатности, и то у целости нормативно и доктринарно.

Четврто, јасно је препозната потреба за сарадњом државних органа са субјектима из области приватног обезбеђења.

На крају, послове из области националне безбедности обављају и субјекти из области приватног обезбеђења.

Стратегија из 2009. године	**Стратегија из 2019. године**
Субјекти из области приватног обезбеђења	Службе и агенције за обезбеђење личности и објеката (штуро одређење које треба занемарити) / правна лица, предузетници и физичка лица која врше послове приватног обезбеђења
Спровођење политике унутрашње безбедности	Вршење послова унутрашње безбедности
Делатност – заштита безбедности појединаца, објеката и других материјалних добара која није обухваћена заштитом надлежних државних органа	Делатност – обезбеђење личности и објеката (штуро одређење које треба занемарити) / вршење послова приватног обезбеђења (извучено из контекста)
Препозната потреба за уређеношћу	-
Препозната потреба за сарадњом	-

Табела 1: Упоредни приказ одредби о приватном обезбеђењу у Стратегијама националне безбедности Републике Србије из 2009. и 2019. године (извор: аутор)

[2] „Службени гласник РС“, број 88/09.

Стратегија из 2019. године очекивано изоставља одредбе о потреби за **уређеношћу** и **сарадњом** у овој области сходно томе да је 2013. године донесен матични закон који уређује ова питања.

О приватном обезбеђењу

Област приватног обезбеђења регулисана је Законом о приватном обезбеђењу.[3] Као неке од значајних одредаба издвајају се:

Овим законом уређују се обавезно обезбеђење и заштита одређених објеката, послови и рад правних и физичких лица у области приватног обезбеђења, услови за њихово лиценцирање, начин вршења послова и остваривање надзора над њиховим радом.

Из приложеног одређења приватног обезбеђења следи да су субјекти из области приватног обезбеђења:

1) правна лица и предузетници регистрована за ту делатност и
2) правна лица и предузетници који су образовали унутрашњи облик организовања обезбеђења за сопствене потребе*;*

   док су послови приватног обезбеђења:

1) заштите лица, имовине и пословања физичком и техничком заштитом када ти послови нису у искључивој надлежности државних органа,
2) транспорт новца, вредносних и других пошиљки и
3) одржавања реда на јавним скуповима, спортским приредбама и другим местима окупљања грађана.

Није јасно зашто на овом месту закон обухвата само неке послове приватног обезбеђења, док у наредном делу изричито као послове наводи следеће:

1) процене ризика у заштити лица, имовине и пословања;
2) заштите лица и имовине физичким и техничким средствима, као и послове одржавања реда на јавним скуповима, спортским приредбама и другим местима окупљања грађана у делу који није у надлежности Министарства унутрашњих послова;
3) планирања, пројектовања и надзора над извођењем система техничке заштите, монтаже, пуштања у рад, одржавања система техничке заштите и обуке корисника;
4) обезбеђења транспорта и преноса новца и вредносних пошиљки у делу који није у надлежности министарства.

[3] „Службени гласник РС“, бр. 104/2013, 42/2015, 87/2018.

Уређеност

Питање уређености постигнуто је Законом о приватном обезбеђењу, који је усвојен и ступио на снагу 2013. године као матични закон који уређује област приватног обезбеђења. Данас је на снази верзија акта из 2018. године. Како је паралелно са доношењем и применом закона текло доношење и примена прописа донетих на основу њега, следи да је уређеност постигнута, бар привидно (формално).

Подзаконска акта, која ближе одређују област приватног обезбеђења, јесу:

- Правилник о начину примене овлашћења службеника обезбеђења (2019);
- Правилник о начину вршења послова техничке заштите и коришћења техничких средстава (2019);
- Правилник о ближим условима које морају да испуне правна и физичка лица за спровођење стручне обуке за вршење послова приватног обезбеђења (2014);
- Правилник о стручном испиту за вршење послова приватног обезбеђења и редарске службе (2019);
- Правилник о боји и саставним деловима униформе службеника обезбеђења (2019);
- Правилник о програмима и начину обављања стручне обуке за вршење послова приватног обезбеђења и редарске службе (2019);
- Правилник о ближим условима за издавање овлашћења за спровођење обуке за вршење послова приватног обезбеђења и редарске службе (2019);
- Уредба о ближим критеријумима за одређивање обавезно обезбеђених објеката и начину вршења послова њихове заштите (2016);
- Правилник о садржини, изгледу и начину употребе легитимације службеника приватног обезбеђења (2016) и
- Правилник о начину употребе средстава принуде у вршењу послова приватног обезбеђења (2015).

Доношењем закона, област приватног обезбеђења је формално уређена, с тим да сам закон има бројне нејасноће и пропусте.

Сарадња у складу са Законом о приватном обезбеђењу

Законом о приватном обезбеђењу уређује се питање сарадње између Министарства унутрашњих послова и субјеката из области приватног обезбеђења кроз следеће активности:

- Министарство унутрашњих послова (у даљем тексту: Министарство) врши безбедносну проверу (лица која треба да раде на пословима приватног обезбеђења) којом се утврђује постојање или непостојање безбедносне сметње.

- Министарство спроводи обуку физичких лица за вршење послова приватног обезбеђења и обуку физичких лица за вршење послова редарске службе.
- Министарство даје овлашћење за обављање обуке привредном друштву, предузетнику и школској установи.
- Министарство спроводи стручни испит за службеника обезбеђења и редара.
- Министарство утврђује начин провере обучености физичких лица, односно начин полагања стручног испита за вршење послова приватног обезбеђења и висину трошкова организовања и спровођења стручних испита, као и садржину и начин вођења евиденција о лицима која су полагала и положила стручни испит.
- Министарство прима захтеве за издавање лиценци и издаје лиценце за вршење послова приватног обезбеђења правном лицу, предузетнику и физичком лицу.
- Министарство поступа по жалби на решење о захтеву за издавање лиценце и решење о одузимању лиценце.
- Министарство даје одобрење за набавку оружја.
- Министарство врши надзор приватног обезбеђења – испуњености услова и начина обављања делатности, примену овлашћења и вођење евиденција и спровођење прописа о држању и ношењу оружја приватног обезбеђења.
- Месно надлежна полицијска управа прима обавештење о закључењу, анексу или раскиду уговора за физичку заштиту лица која се врши оружјем и за пружање услуга видео-надзора са архивирањем снимка.
- Месно надлежна полицијска управа прима план обезбеђења од организатора скупа, заједно са пријавом о одржавању јавног скупа, односно обавештењем.
- Надлежна полицијска управа прима обавештење о датуму и времену почетка циклуса обуке, са распоредом обуке по темама и терминима, предавачима и списком полазника од привредних друштава, предузетника и школских установа који спроводе обуку.
- Надлежна полицијска управа прима обавештење о престанку рада или гашењу правног лица и предузетника од одговорног лица у правном лицу и код предузетника.
- Надлежна полицијска управа прима обавештење о употреби средстава принуде од службеника обезбеђења.
- Надлежна полицијска управа прима извештај о употреби средстава принуде са мишљењем одговорног лица у правном лицу и код предузетника.
- Надлежна полицијска управа прима захтев за издавање легитимације службенику обезбеђења.
- Министар надлежан за унутрашње послове (у даљем тексту: министар) прописује ближе услове, у погледу потребних објеката, односно просторија, материјално-техничких средстава и опреме, стручне

оспособљености и броја лица која спроводе обуку лица за вршење послова приватног обезбеђења и редарске службе, као и програме стручне обуке и начин њиховог спровођења.
- Министар утврђује ближи начин вршења послова техничке заштите и коришћења техничких средстава.
- Министар прописује ближи начин примене овлашћења утврђених овим законом.
- Министар прописује боју и саставне делове униформе коју носе службеници обезбеђења.
- Министар прописује висину таксе за издавање лиценце.
- Министар прописује ближу садржину, изглед и начин употребе легитимације службеника приватног обезбеђења.
- Министар решењем оснива посебну радну групу – Стручни савет за унапређење приватног обезбеђења и јавно приватног партнерства у сектору безбедности.
- Овлашћени полицијски службеник проверава услове и начин обављања делатности, примену овлашћења, вођење евиденција, начин чувања и ношења ватреног оружја, и, по потреби, спроводи и друге радње којима се остварује непосредан и ненајављен увид у вршење послова приватног обезбеђења.
- Овлашћени полицијски службеник разматра примедбе на записник о обављеном надзору и, према потреби, понавља радње на које се примедбе односе, односно мења или одустаје од предложене мере.
- Овлашћени полицијски службеник може да у току надзора, уз потврду, привремено одузме пословне књиге, евиденције, другу документацију, видео-снимке или друге исправе, до окончања поступка надзора.
- Овлашћени полицијски службеници Министарства могу лице које поседује лиценцу, која се за обављање послова приватног обезбеђења издаје физичком лицу, да упути на лекарски преглед, ако се оправдано посумња да више не испуњава психофизичке услове за вршење послова.
- Овлашћени полицијски службеник може да захтева стављање архивираних снимака на увид.
- Полицијски службеник може да изда наређење службенику обезбеђења.
- Полицијски службеник прима привремено одузете предмете уз потврду о привременом одузимању предмета.
- Полиција прима обавештење о вршењу кривичних дела или прекршаја са елементима насиља у штићеном објекту, штићеном простору или простору који је видљив из штићеног простора или објекта или на правцу кретања од оператера у контролном центру.
- Полиција прима обавештење о привременом задржавању лица од службеника обезбеђења.

Од поменутог издвојили бисмо тренутно само активност упућивања службеника обезбеђења на лекарски преглед, ако се оправдано посумња да више не испуњава

психофизичке услове за вршење послова. У потпуности је нејасно на основу којих параметара овлашћени полицијски службеник одлучује о потреби за преиспитивањем психофизичких услова за вршење послова. Која то знања има на основу којих процењује психофизичке услове за вршење послова, односно психофизичко стање службеника обезбеђења.

Други облици сарадње

Поред поменутих активности сарадња између државних органа и субјеката из области приватног обезбеђења може се сагледати кроз области:

- Обезбеђење јавних скупова;
- Обезбеђење спортских приредби;
- Обезбеђење транспорта новца и других вредносних пошиљки;
- Заштита критичне инфраструктуре;
- Заједничко деловање у ванредним ситуацијама и
- Размене информација.

Обезбеђење јавних скупова – одредбе Закона о приватном обезбеђењу, Закона о полицији и Закона о јавном окупљању:

– Закон о приватном обезбеђењу као послове приватне безбедности одређује послове *одржавања реда на **јавним скуповима**, спортским приредбама и другим местима окупљања грађана у делу који није у надлежности Министарства унутрашњих послова.*

– Закон о полицији као полицијске послове одређује послове обезбеђења *одређених **јавних скупова**, личности, објеката и простора.*

– Закон о јавним окупљањима одређује *ангажовање редарске службе* за одржавање мирног окупљања.

Обезбеђење спортских приредби – одредбе Закона о приватном обезбеђењу, Закона о полицији и Закона о спречавању насиља и недоличног понашања на спортским приредбама:

– Закон о приватном обезбеђењу као послове приватне безбедности одређује послове *одржавања реда на јавним скуповима, **спортским приредбама** и другим местима окупљања грађана у делу који није у надлежности Министарства унутрашњих послова.*

– Закон о полицији као полицијске послове одређује послове *одржавања јавног реда и мира, спречавање насиља на **спортским приредбама**, пружање помоћи у извршењима у складу са законом.*

– Закон о спречавању насиља и недоличног понашања на спортским приредбама одређује *образовање одговарајуће редарске службе или ангажовање правног лица или предузетника ради обављања послова физичког обезбеђења и одржавања реда на спортској приредби*.

Обезбеђење транспорта новца и других вредносних пошиљки – одредбе Закона о приватном обезбеђењу, Закона о полицији и Уредбе о врстама услуга које пружа Министарство унутрашњих послова и висини такси за пружене услуге:

– Закон о приватном обезбеђењу као послове приватне безбедности одређује послове *обезбеђења транспорта и преноса новца и вредносних пошиљки у делу који није у надлежности Министарства.*
– Закон о полицији одређује да Министарство може да остварује приходе *пружањем услуга* у вези са основном делатношћу Министарства.
– Уредба о врстама услуга које пружа Министарство унутрашњих послова и висини такси за пружене услуге као услуге Министарства одређује пратњу *новца, хартија од вредности* итд. за потребе Народне банке Србије, пословних банака, установа, организација и других правних лица.

Заштита критичне инфраструктуре – одредбе Закона о приватном обезбеђењу и Закона о критичној инфраструктури:

– Закон о приватном обезбеђењу одређује да се *заштита обавезно обезбеђених објеката, у складу са општим актом о организацији и систематизацији, обавља уговорним ангажовањем* ***субјеката лиценцираних за обављање делатности приватног обезбеђења или као организована самозаштитна делатност***.
– Закон о критичној инфраструктури не препознаје приватно обезбеђење као компоненту заштите; с тим да се на основу одредбе да *у заштити критичне инфраструктуре пре, за време и после ометања или прекида у функционисању критичне инфраструктуре, учествују сви надлежни органи и организације, грађани и* ***други субјекти*** може закључити да су и субјекти из области приватног обезбеђења укључени у заштиту.

Упоређујући одређење критичне инфраструктуре (Закон о критичној инфраструктури) и одређење обавезно обезбеђених објеката (Закон о приватном обезбеђењу) закључује се да обавезно обезбеђени објекти спадају у критичну инфраструктуру.

Заједничко деловање у ванредним ситуацијама – одредбе Закона о приватном обезбеђењу и Закона о смањењу ризика од катастрофа и управљању ванредним ситуацијама:

– Закон о приватном обезбеђењу одређује вршење послова приватног обезбеђења без наглашавања услова у погледу редовног и ванредног стања или ванредне ситуације.
– Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама не препознаје приватно обезбеђење као компоненту система смањења ризика од катастрофа и управљања; с тим да се на основу одредаба где се *привредна друштва и друга правна лица и предузетници* препознају као субјекти система, односно, *организације чија је делатност од посебног интереса за развој и функционисање система* као снаге

система, може закључити да су и субјекти из области приватног обезбеђења укључени у овај систем.

Размена информација – законски је уређено да субјекти из области приватног обезбеђења имају обавезу извештавања Министарства унутрашњих послова (и полиције) о појединим питањима из делокруга свог рада. Пример је (видети детаљније у претходном тексту) обавештење и извештај о употреби средстава принуде, обавештење о привременом задржавању лица, обавештење о вршењу кривичних дела или прекршаја са елементима насиља, обавештење и план обезбеђења јавног скупа, обавештење о закљученим уговорима, обуци или престанку рада правних лица или предузетника. Са друге стране, ***у полицијским прописима се нигде експлицитно не спомиње неопходност размене информација са сектором приватног обезбеђења***.

Више о сарадњи и проблемима остваривања сарадње и партнерства полиције и приватног обезбеђења може се видети у:

- Акциони план за унапређење јавно-приватног партнерства у сектору безбедности за период 2014/2015. године.[4]
- Радивојевић, Н. (2020). *Јавно-приватно партнерство у области јавне безбедности у развијеним земљама са посебним осртом на Републику Србију* (Докторска дисертација). Универзитет у Новом Саду Правни факултет у Новом Саду.

***

На крају можемо да наведемо да се приватно обезбеђење помиње још у три значајна документа и у једном закону.

Стратегија развоја МУП-а за период 2018–2023. године, Службени гласник РС, број 78/2018, прописује *пуну примену Закона о приватном обезбеђењу.*

Стратешки план полиције за период 2018–2021. године – јавна верзија, тежи *пуној примени Закона о приватном обезбеђењу, како би сектор приватног обезбеђења у наредном периоду постао партнер полицији у очувању безбедности грађана и имовине и одржавању стабилног јавног реда и мира*.[5]

Стратешка процена јавне безбедности за период 2022–2025. године наводи: У области приватног обезбеђења и детективске делатности остварени су следећи резултати: применом Закона о приватном обезбеђењу издато је 96 овлашћења

[4] Укратко о документу видети на https://www.ekapija.com/news/1006487/verifikovan-akcioni-plan-saradnje-u-sektoru-bezbednosti

[5] МУП Дирекција полиције. (2017). *Стратешки план полиције за период 2018–2021. године – јавна верзија. МУП*. Преузето са: http://www.mup.rs/wps/wcm/connect/c206983b-503f-4ebf-bf5b-8d5bc65ca8e3/Strateski+plan+policije+-+Javna+verzija-WEB.pdf?MOD=AJPERES&CVID=m3r4AMv

центрима за обуку, одржане су 192 комисије за полагање стручног испита, издато је 15.198 лиценци физичким лицима и 872 правним лицима, одузето је 212 лиценци, издато је 25.756 легитимација, извршено је 1.408 надзора над радом субјеката приватног обезбеђења и поднете су 542 прекршајне пријаве. [6]

Закон о полицији[7] нигде се изричито не бави приватним обезбеђењем, изузев што као врсту полицијских послова одређује *извршавање послова утврђених прописима о оружју,* ***приватном обезбеђењу*** *и детективској делатности.*

Закључак

Спроведена анализа указује на то да Стратегија из 2019. године добија примат у односу на навођење субјеката приватне безбедности и одређивање делатности – вршење послова приватног обезбеђења. Овакво одређење, иако доста широко, оправдано је из разлога што је ова стратегија усвојена када је приватно обезбеђење већ имало своју засебну законску регулативу. Слично је и са одредбама које се тичу уређености ове области и сарадње, које су обухваћене Стратегијом из 2009. године, али изостављене у Стратегији из 2019. године. Када је реч о одредбама које се односе на уређеност, Стратегија из 2019. године заправо је индиректно на неки начин и њих обухватила наводећи да послове унутрашње безбедности обављају и правна лица, предузетници и физичка лица која врше послове приватног обезбеђења, *у складу са законом.* Међутим, сарадња између субјеката из области приватног обезбеђења и других субјеката, у првом реду Министарства унутрашњих послова, иако је обухваћена низом законских решења, у Стратегији националне безбедности, као највишег стратешког документа у области националне безбедности, потпуно је изостављена.

Оно у чему Стратегија из 2009. године остварује примат јесте наглашавање спровођења политике унутрашње безбедности, што је доста обухватније подручје деловања од вршења послова унутрашње безбедности.

На основу свега до сада изнетог, јасно је да се не користи термин „приватна безбедност“ већ искључиво термин „приватно обезбеђење“, што се не уклапа у дистинкцију јавне и приватне компоненте безбедности, на основу које би требало разликовати јавну и приватну безбедност. Ово може увести забуне и створити неусаглашености међу научном и стручном јавношћу, а нарочито међу онима који се не баве овом проблематиком.

---

[6] МУП Дирекција полиције. (2021). *Стратешка процена јавне безбедности за период 2022-2025. године*. Преузето са: http://www.mup.gov.rs/wps/wcm/connect/98632591-2b0d-4cba-9cd1-e7ff993705a6/Strateska+procena+javne+bezbednosti+MUP.pdf?MOD=AJPERES&CVID=nYH6yro

[7] „Сл. гласник РС“, бр. 6/2016, 24/2018 и 87/2018.

Не залазећи у ову проблематику у овом раду, не могу бранити став да су приватна безбедност и приватно обезбеђење синоними. Реч је о два засебна концепта, која се налазе у корелацији, и то као виши појам – приватна безбедност и његов део, нижи појам – приватно обезбеђење, које суштински, у складу са Законом који регулише ову област, обухвата само физичко и техничко обезбеђење. Самим тим, сматрам да треба унапредити одредбе које се односе на субјекте извршног дела система националне безбедности.

Узимајући у обзир да је реч о највишем стратешком документу у овој области, најпре би требало да прецизно утврди субјекте унутрашње безбедности, уважавајући и јавну и приватну компоненту безбедности. Следеће би било да стратегија, поред коришћења терминолошки адекватних појмова, обухвати прецизно одређене субјекте приватне безбедности, њихову делатност и опис послова, укључујући наглашавање њихове сарадње са другим субјектима система националне безбедности, а избегавајући одредбе које нису јасне и уносе забуну (представљено у потпоглављу *Анализа Стратегије националне безбедности из 2019. године*).

Библиографија

1. Закон о јавном окупљању. (2016). *Службени гласник РС*, 6/16.
2. Закон о критичној инфраструктури. (2018). *Службени гласник РС*, 87/18.
3. Закон о полицији. (2016). *Службени гласник РС*, 6/16, 24/18 и 87/18.
4. Закон о приватном обезбеђењу. (2013). *Службени гласник РС*, 104/13, 42/15 и 87/18.
5. Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама. (2018). *Службени гласник РС*, 87/18.
6. Закон о спречавању насиља и недоличног понашања на спортским приредбама. (2003). *Службени гласник РС*, 67/03, 101/05 – др. закон, 90/07, 72/09 – др. закон, 111/09, 104/2013 – др. закон и 87/18.
7. МУП Дирекција полиције. (2017). *Стратешки план полиције за период 2018–2021. године – јавна верзија. МУП*. Преузето са: http://www.mup.rs/wps/wcm/connect/c206983b503f4ebfbf5b8d5bc65ca8e3/Strateski+plan+policije+-+Javna+verzija-WEB.pdf?MOD=AJPERES&CVID=m3r4AMv
8. МУП Дирекција полиције. (2021). *Стратешка процена јавне безбедности за период 2022–2025. Године*. Преузето са: http://www.mup.gov.rs/wps/wcm/connect/986325912b0d4cba9cd1e7ff993705a6/Strateska+procena+javne+bezbednosti+MUP.pdf?MOD=AJPERES&CVID=nYH6yro
9. Правилник о боји и саставним деловима униформе службеника обезбеђења. (2019). *Службени гласник РС*, 49/19.

10. Правилник о садржини, изгледу и начину употребе легитимације службеника приватног обезбеђења. (2016). *Службени гласник РС*, 3/16, 30/19.
11. Правилник о ближим условима за издавање овлашћења за спровођење обуке за вршење послова приватног обезбеђења и редарске службе. (2019). *Службени гласник РС*, 15/19.
12. Правилник о ближим условима које морају да испуне правна и физичка лица за спровођење стручне обуке за вршење послова приватног обезбеђења. (2014). *Службени гласник РС*, 117/14.
13. Правилник о начину вршења послова техничке заштите и коришћења техничких средстава. (2019). *Службени гласник РС*, 91/19.
14. Правилник о начину примене овлашћења службеника обезбеђења. (2019). *Службени гласник РС*, 59/19.
15. Правилник о начину употребе средстава принуде у вршењу послова приватног обезбеђења. (2015). *Службени гласник РС*, 30/15.
16. Правилник о програмима и начину обављања стручне обуке за вршење послова приватног обезбеђења и редарске службе. (2019). *Службени гласник РС*, 15/19.
17. Правилник о стручном испиту за вршење послова приватног обезбеђења и редарске службе. (2019). *Службени гласник РС*, 74/19.
18. Стратегија националне безбедности Републике Србије. (2009). *Службени гласник РС*, 88/09.
19. Стратегија националне безбедности Републике Србије. (2019). *Службени гласник РС*, 94/19.
20. Стратегија развоја Министарства унутрашњих послова за период 2018–2023. године. (2018). *Службени гласник РС*, 78/18.
21. Уредба о ближим критеријумима за одређивање обавезно обезбеђених објеката и начину вршења послова њихове заштите. (2016). *Службени гласник РС*, 98/16.
22. Уредба о врстама услуга које пружа Министарство унутрашњих послова и висини такси за пружене услуге. (2019). *Службени гласник РС*, 51/ 19, 86/19 – др. закон, 80/22.

NATIONAL SECURITY STRATEGY OF THE REPUBLIC OF SERBIA AND PRIVATE SECURITY

Abstract

Although the main law regulating the field of private security, the Law on Private Security, was adopted only in 2013, this fact does not dispute the earlier regulation of this area by some other documents. Namely, the importance and role of private security in the implementation of the internal security policy was recognized by the National Security Strategy of the Republic of Serbia from 2009. It also indicated the need and necessity of private security cooperation with other subjects of national security, primarily state administration bodies, as well as a greater degree of organization in this area both normatively and doctrinally, which unequivocally indicates the importance of private security in protection national values and interests. On the other hand, in the National Security Strategy of the Republic of Serbia from 2019, a significantly different approach to private security can be observed, given the lack of consistency in defining certain elements of this area. Due to the lack of provisions that would regulate the issue of cooperation as well as the regulation of private security, all with the aim of preserving and improving national security, it gives the impression that an omission has been made that could potentially have long-term consequences. Although the issue of cooperation is dealt with in detail in the Law on Private Security, the legitimacy of the provisions of a lower legal act can be questioned, which does not find adequate support for its provisions in the highest strategic documents of a country, such as the national security strategy. However, the justification for the lower level of generality/comprehensiveness of the strategy from 2019 compared to the one from 2009 can be found precisely in the adoption of the Law, to which the task of defining and regulating some issues in the mentioned area was conditionally "delegated", while from for objective reasons, the same possibility did not exist in 2009.

Keywords: *national security strategy, private security, Law on Private Security*.

(НАЦИОНАЛНА) ЛОГИСТИКА У СТРАТЕГИЈСКИМ ДОКУМЕНТИМА ПЛАНИРАЊА ОДБРАНЕ РЕПУБЛИКЕ СРБИЈЕ

Дејан Вулетић [1]

Апстракт

У раду је објашњено појмовно одређење, у ужем и ширем смислу, националне логистике, њена улога и значај. Са аспекта елемената националне логистике анализирана су стратегијска документа планирања одбране Републике Србије, Стратегија националне безбедности и Стратегија одбране, усвојене крајем 2019. године. Исказани предмет истраживања је у директној вези са циљем рада који је усмерен на указивање и објашњење елемената (националне) логистике садржаних у наведеним документима, сагледавање њихове усаглашености, као и указивање на уоченим недостацима, с обзиром на то да је реч о „динамичним“ документима који се периодично мењају услед промењених изазова, ризика и претњи по националну безбедност. Основна хипотеза је да је ефикасна (национална) логистика неопходан услов за функционисање друштва, као и за реализацију мисија и задатака управљачког и извршног дела система безбедности (војне и полицијске снаге, службе безбедности, ватрогасно-спасилачкејединице, јединице цивилне заштите, привредна друштва, грађани и друго) у миру, а нарочито у периоду криза или оружаних сукоба. Из суштине проблема и хипотетичких ставова произилази основно истраживачко питање које гласи: „Да ли је и у којој мери (национална) логистика обухваћена у стратегијским документима планирања одбране Републике Србије?“. Поред општих научних метода, с обзиром на предмет и циљ истраживања, тежишно су коришћене компаративна метода, којом су анализирани и упоређивани садржаји наведених стратегијских докумената, као и метода анализе садржаја, имајући у виду да су као извори

[1] Институт за стратегијска истраживања, Београд, e-mail: dejan.vuletic@mod.gov.rs.

Рад је настао у оквиру пројекта Фонда за науку Републике Србије „Идеје“ – Пројекат акцелерације иновација и подстицања раста предузетништва у Републици Србији – Management of New Security Risks – Research and Simulation Development – NEWSIMR&D, #7749151.

сазнања коришћена званична документа, научни радови и друге публикације. На основу изнете аргументације у раду, може се закључити да национална логистика као термин није препозната у стратегијским документима планирања одбране, већ само њени одређени елементи који су разматрани, углавном, у мањој мери.

Кључне речи: логистика, национална логистика, логистичка подршка, стратегијска документа.

Увод

Термин „логистика“ потиче од грчке речи *logistikos*, што значи „вешт у прорачуну“. У досадашњој теорији и пракси, логистички концепти се често користе са не баш јасно дефинисаним разликама, што додатно компликује тако сложену област у смислу разумевања појединих терминолошких дефиниција, па чак и до њиховог погрешног тумачења и погрешне примене у пракси. У практичном смислу, термин „логистика“ означава вештину која се бави проблемима обезбеђивања ресурса и пружања подршке у постизању циљева и функција подржаног система. У научном смислу, термин „логистика“ означава одређену дисциплину која настоји да пронађе методе планирања, управљања и оптимизације токова материјала, услуга, енергије, информација и капитала у циљу постизања одређених ефеката. У суштини представља процес планирања, имплементације и управљања кретања производа, услуга и информација од једне тачке до друге (Milenkov at al., 2020, p. 82–83).

Логистика, као научна дисциплина, омогућава интеграцију широког спектра логистичких активности у јединствен логистички систем, користећи различита научна и практична достигнућа. На овај начин се постиже ефикасно управљање логистичким захтевима и логистичким активностима, са места и времена њиховог настанка до места и времена њиховог задовољења (Milenkov at al., 2020, p. 82–83).

Логистика је главна компонента модерних система производње и дистрибуције и важан допринос макроекономском развоју одређене земље. Логистички индекс учинка (*Logistics Performance Index* – LPI) Светске банке представља логистички профил, односно логистичке перфомансе одређене земље.[2] Светска банка израчунава LPI за око 160 земаља и објављује одговарајуће рангирање у периодичним извештајима. Немачка се појављује као референтни пример у овој области, с обзиром на то да представља водећу индустријску и комерцијалну државу у Европи и истакнут значај који се придаје њеном систему транспорта терета и логистике, кључном елементу њене конкурентности. Три од шест

[2] Према подацима за 2018. годину водећа Немачка имала је LPI 4.20, док је Србија била рангирана на 68. месту када је LPI износио 2.84. https://lpi.worldbank.org/

највећих глобалних логистичких провајдера налазе се у Немачкој – *DHL, DBSchenker* и *Kuehne+ Nagel* (Savy, 2016, p. 413–414).

Последњих година, нарочито након усвајања Резолуције о заштити суверенитета, територијалног интегритета и уставног поретка, све више се говори о тзв. националној логистици. Поменутом резолуцијом, Народна скупштина Републике Србије доноси одлуку о проглашењу војне неутралности Републике Србије у односу на постојеће војне савезе, што подразумева значајан ослонац на сопствене ресурсе и снаге (Резолуција 2007).

Националну логистику могуће је одредити кроз њен потенцијал – ресурсе и инфраструктуру, и операционализацију искоришћења тих ресурса и инфраструктуре. Под ресурсима се подразумева све оно што је природа дала и оно што је настало као последица међудржавних и међународних односа. Ту се подразумевају резерве минералних сировина, пољопривредно земљиште (у свим својим облицима), извори енергије итд. У ресурсе се, такође, убрајају и водотокови, излаз на море, геополитички и саобраћајни положај земље, климатски услови итд. Инфраструктура обухвата све оно што је човек створио ради омогућавања искоришћења постојећих ресурса – путеви, железница, енергетска постројења, канали, луке, складишта, велики системи за наводњавање итд. Привреда, односно привредни систем једне земље јесте операционализација искоришћавања тих ресурса и инфраструктуре. Национална логистика у ширем смислу подразумева задовољавање логистичке потребе народа, војске и других састава у кризним ситуацијама (Станојевић, Мишковић и Мишев, 2017).

Национална логистика у ужем смислу подразумева националну подршку привреди земље, односно управљање током робе (информација и услуга) од тачке где се захтев генерише до тачке где се нека специфична потреба задовољава. Основни чинилац логистике, у овом смислу, јесу корисници њених услуга или привреда која, у ствари, генерише потребе за логистичким процесима превоза, складиштења, дистрибуције итд. Војне и безбедносне институције, организације и агенције (војска, полиција, цивилна заштита, службе безбедности итд.) главни су корисници националног логистичког система у случају ратова и свих врста криза. Задовољавање њихових потреба, у случају Србије (или било које земље у већим кризама – сукобима), немогуће је одвојити од задовољавања свих потреба становништва и привреде земље у кризним стањима (Станојевић, Мишковић и Јефтић 2017, стр. 297–300).

Националном логистиком се обезбеђују неопходна средства за живот становништва и оружаних снага и за функционисање свих елемената друштва. Циљ националне логистике јесте задовољавање оперативних потреба војних и безбедносних институција, али и становништва и државе у целини како би се обезбедило што нормалније функционисање у миру, кризним ситуацијама и у

рату. Национални логистички систем, дакле, чини систем копнених и водених путева, аеродрома, лука, телекомуникационе мреже и других, за функционисање државе, важних инфраструктура (Fechner, 2010, p. 9–18). Поред разматрања логистике у контексту привреде земље неизоставан сегмент разматрања одбране земље и заштите националних интереса представља логистичка подршка војних снага. Такође, у војној сфери логистика, односно логистичка подршка, представља неопходан услов за успешно извођење операција.

Логистика је кључна не само за евентуално ангажовање војске у случају сукоба већ и за обезбеђивање свакодневне спремности снага. Војне јединице не могу да обављају своју мисију без неопходних ресурса. Доступност и испорука делова и резервних компоненти, способност одржавања и способност да се повећа обим одржавања у кратком року, могућност уговарања додатне подршке када је то потребно и други логистички изазови од суштинског су значаја за војну ефикасност. Значај логистике расте експоненцијално када се узме у обзир све већа сложеност стратешких логистичких ресурса као што су мрежа националних и међународних ауто-путева, железнице, луке, информациона инфраструктура и друго (Wissler, 2018, p. 96–97).

На први поглед, изазови логистике за потребе система одбране могу изгледати као исти, или барем врло слични, изазовима са којима се суочавају *FedEx, Walmart, Amazon, DHL* или било која друга велика компанија која се бави дистрибуцијом пошиљки на глобалном нивоу. Међутим, разлике су огромне. За разлику од комерцијалних фирми које се могу припремити и деловати према плану и направљеном распореду, војска мора да функционише не знајући след будућих догађаја, у условима изненадних промена, деловања противника и друго. Војне снаге морају добити логистичку подршку без обзира на то колико је њихов приступ интернету ограничен или повремен, док непријатељ непрекидно напада, уништава ланце снабдевања, прекида комуникационе канале, саобраћајну инфраструктуру и друго. Изазови логистичке подршке војске су јединствени и веома комплексни (Wissler, 2018, p. 97).

Важност и улога логистичке подршке је наглашена и у оквиру НАТО алијансе. Комитет за логистику (*Logistics Committee* – LC) је највише „тело“ НАТО-а задужено за логистику. Стратешки концепт алијансе је операционализован кроз флексибилне и интероперабилне логистичке принципе и политике логистике, које су садржане у документу MC319/1 (*NATO Principles and Policies for Logistics*). У документу се наводи да се колективна одговорност постиже кроз блиску координацију и сарадњу између појединачних држава и НАТО-а као организације, током фазе планирања и извођења операције, и укључује веће разматрање ефикасног коришћења цивилних комерцијалних ресурса. Државе треба да обезбеде националне и мултинационалне логистичке капацитете и ресурсе који су потребни уз уступање одговарајућих овлашћења како би се

омогућило команданту НАТО-а да изврши своју мисију. Координисано логистичко планирање је, дакле, суштински аспект ефикасног и економичног коришћења ресурса (NATO Logistics Handbook, 2012, p. 19–20).

Логистичка подршка војних снага у савременим условима намеће потребу изградње одрживог логистичког система, довољно способног да се прилагоди новим изазовима и да подржи различите циљеве и мисије ангажованих снага у свим условима. Дакле, при извођењу операција командантима је потребан логистички систем који је довољно флексибилан, динамичан и отпоран да обезбеди неопходне ресурсе када и где су потребни, односно да обезбеди поуздан и брз логистички одговор на оперативне захтеве ангажованих снага (Milenkov at al., 2020, p. 100–101).

У Војсци Србије је препознат значај логистике за функционисање команди, јединица и установа и извршавање мисија и задатака у различитим операцијама. Обезбеђење Војске Србије у оружаном сукобу, као што је то уосталом случај и са другим армијама, знатно је сложеније због већег и динамичнијег утрошка ресурса. Поред логистичке подршке, обезбеђење Војске Србије обухвата читав низ различитих врста обезбеђења као што су кадровско, обавештајно, безбедносно, телекомуникационо-информатичко и друго.

Разматрање логистике у стратегијским документима планирања одбране Републике Србије

У Закону о одбрани Републике Србије наводи се да је „систем одбране Републике Србије део система националне безбедности који представља јединствену, нормативно, структурно и функционално уређену целину, чији је циљ заштита суверенитета, независности, територијалне целовитости и безбедности Републике Србије од свих облика спољњег и унутрашњег угрожавања у миру, ванредном стању и рату“ (Закон о одбрани, 2007, члан 4, став 1 и 1а). Да би се обезбедила одговорајућа припрема за одбрану земље и функционисање свих субјеката система одбране како у миру тако и у рату, припремају се одговарајућа документа планирања одбране (стратегијско-доктринарни документи, документи планирања развоја и документи планирања употребе снага). Основне стратегијске документе планирања одбране представљају Стратегија националне безбедности Републике Србије (у даљем тексту СНБ РС) и Стратегија одбране Републике Србије (у даљем тексту СО РС), усвојене крајем 2019. године (Закон о одбрани, 2007, члан 7). Наведене стратегије као и друга документа морају бити усаглашени да би се обезбедило рационално коришћење расположивих ресурса, ефикасно функционисање система одбране, односно да би се обезбедиле неопходне оперативне и функционалне способности МО и ВС. Стратегијска документа

планирања одбране јесу динамичног карактера и мењају са променом чинилаца који утичу на безбедносно окружење и економску моћ Републике Србије.

Ради утврђивања заступљености (националне) логистике у стратегијским документима планирања одбране анализираће се елементи који чине националну логистику, разврстани у две широке групе – ресурси и инфраструктура.

Логистика у Стратегији националне безбедности Републике Србије

У СНБ РС се наводи да је то „највиши стратешки документ у којем су исказани основни ставови, опредељења и мере које ће Република Србија предузети ради заштите и остваривања националних интереса и очувања основних националних вредности". „СНБ РС подразумева заједничко ангажовање свих субјеката и потенцијала друштва и државе у супротстављању изазовима, ризицима и претњама безбедности и заштити и остваривању националних интереса Републике Србије" (Стратегија националне безбедности РС, 2019).

Приликом разматрања стратегијског окружења, у СНБ РС се наводи да „у условима глобализоване економије, макроекономске последице финансијске нестабилности у функционисању глобалног тржишта одражавају се и на стање безбедности у свету. Последице светске економске кризе у појединим државама могу да доведу до политичке нестабилности, социјалних немира, као и до интензивирања улагања у војноиндустријски комплекс и пораста трке у наоружању. Спорији раст у развијеним економијама негативно утиче на државе у развоју, док су светска трговина и инвестиције у неповољном положају". С обзиром на растући број свеобухватних уговора о слободној трговини и кретању капитала, очекује се да ће јачање економске међузависности наставити да резултира ограничавањем надлежности националних држава. Имајући у виду климатске промене, као и све израженији дефицит природних ресурса, процењује се да ће у свету бити повећан број сукоба изазваних надметањем за обезбеђење енергената и других природних сировина, питке воде и хране. Поред тога, повећање ризика од напада на инфраструктуру за транспорт енергената утицаће на државе да знатно ојачају заштиту критичне енергетске инфраструктуре, укључујући употребу војних снага (Стратегија националне безбедности РС, 2019). Поред наведеног, неопходно је извршити диверсификацију снабдевања, пре свега када су у питању енергенти.

Процењује се да ће се „на глобалном нивоу наставити са доминантним коришћењем фосилних горива, пре свега нафте, а очекује се знатно повећање потражње за природним гасом. Необновљивост најкомерцијалнијих и најдоступнијих енергената савременог света, угља, нафте и гаса, неповољно се одражава на перспективу одрживог развоја, нарочито због мале вероватноће да ће енергија

добијена из обновљивих извора знатно увећати свој удео у глобалној потрошњи“ (Стратегија националне безбедности РС, 2019).

„Процењује се, такође, да ће развој науке и технологије наставити да буде подложан различитим видовима злоупотреба, што ће доводити до негативних безбедносних импликација. Динамика глобалног развоја информационих технологија условиће даље интензивирање активности у сајбер простору чију безбедност ће, превасходно, угрожавати сајбер шпијунажа, напади на критичну инфраструктуру, неовлашћени продори у базе тајних података, као и ширење лажних вести и дезинформација путем друштвених мрежа“ (Стратегија националне безбедности РС, 2019).

У СНБ РС се наводи да „имајући у виду геостратегијски положај југоисточне Европе, преко које пролазе важни енергетски и комуникацијски правци, сукобљавања интереса држава у коришћењу транзитних праваца и располагању ресурсима могу довести до настанка регионалних криза и угрожавања безбедности и стабилности држава региона, али и ван њега. С друге стране, регион Балкана, као простор за транзит енергената, могао би да повећа свој укупни геоекономски значај“ (Стратегија националне безбедности РС, 2019).

Приликом разматрања економске ситуације у државама југоисточне Европе, наводи се да је економска ситуација неповољна и да је додатно уздрмана последицама економске кризе. Привреду земаља у региону карактерише и слабо развијена технолошка и индустријска база. Економску ситуацију земаља у региону карактеришу и недостатак инвестиција, слаба домаћа тражња и ниска конкурентска позиционираност на тржиштима. Такође, присутни су проблеми у вези са планирањем буџета, тешкоће у санирању дефицита, као и раст сиромаштва услед смањења куповне моћи становништва. Државе региона изложене су ризику од дугорочног пораста јавног дуга, негативног биланса и других врста дефицита, те високој стопи незапослености, изостанку стратешких пројеката и све већој енергетској зависности. Поред наведеног, негативне импликације на економију земаља региона представљају демографске карактеристике (Стратегија националне безбедности РС, 2019).

У делу који се односи на стратегијско окружење, процењује се да је Република Србија, као и остале државе региона, суочена са опасношћу од тероризма и организованог криминала. На безбедност Републике Србије неповољно утиче и ниво њене привредне развијености, нарочито имајући у виду велике регионалне разлике по тим питањима. Такође, све већи безбедносни ризик представља стање у демографској сфери које карактерише ниска стопа наталитета, миграције становника из руралних у урбане средине, као и одлазак школованог кадра у иностранство. Значајан утицај на безбедносну ситуацију могу имати елементарне непогоде (поплаве, суше, пожари, земљотреси) и друге катастрофе изазване

људским фактором (нпр. техничко-технолошке несреће). Неповољан аспект представљају и енергетски ресурси Републике Србије услед њиховог недостатка, неравномерне распоређености, ограничене могућности увоза и складиштења одређене робе (Стратегија националне безбедности РС, 2019).

Као изазови, ризици и претње безбедности у СНБ РС наведени су проблеми економског развоја који настају као последица деловања спољашњих и унутрашњих чинилаца. Геополитичке тензије су препознате као проблем који може утицати на смањење извоза, погоршање финансијске ситуације, слабљење директних страних инвестиција, а што се неминовно може одразити и на животни стандард грађана. Поред могућности злоупотребе нових технологија, посебно је наглашена енергетска безбедност која може угрозити редовно и стабилно снабдевања енергентима како привреде тако и грађана (Стратегија националне безбедности РС, 2019). Очување унутрашње стабилности и безбедности препознат је у СНБ РС као национални интерес ради непрекидног развоја свих делова друштва, рационалне употребе расположивих ресурса и задовољења потреба грађана (Стратегија националне безбедности РС, 2019).

Анализом СНБ РС са аспекта националне логистике приметно је да она није препозната у наведеној стратегији. У стратегији се разматра шири контекст (глобални и регионални), актуелно стање, последице светске економске кризе, као и предвиђања будућих дешавања. Глобалном и регионалном аспекту је посвећена већа пажња него националном. Велика пажња и са аспекта логистике посвећена је анализи стратегијског окружења, знатно мање разматрању изазова, ризика и претњи безбедности и веома мало разматрању националних интереса Републике Србије.

По питању ресурса поменути су само енергетски ресурси (недостатак, распоређеност, ограничења увоза и проблем складиштења). Остали ресурси су занемарени. Са аспекта инфраструктуре истакнут је ниво привредне развијености и економског развоја. Разматран је и могућ утицај елементарних непогода и демографски проблеми (миграције, одлив становништва), као и последице деловања различитих спољних и унутрашњих чинилаца на економско стање Републике Србије.

Логистика у Стратегији одбране Републике Србије

Приликом разматрања безбедносног окружења у СО РС, наводи се да се „степен развоја националних економија одражава на могућности држава да самостално обезбеде адекватне способности и капацитете за одбрану. У таквим условима повећава се значај спремности држава да кроз одговарајућу међународну војну сарадњу, учешћем у међународним безбедносним и одбрамбеним интеграцијама и мултинационалним операцијама, закључивањем и спровођењем међународних споразума и конвенција, као и војно-економском сарадњом, унапређују

националне способности и остварују повољан утицај на стање глобалне безбедности. Процењује се да ће у свету бити повећан број сукоба изазваних надметањем за обезбеђење енергената и других природних ресурса, питке воде и хране. У таквим условима приоритети великих сила биће обезбеђивање приступа енергетским ресурсима и контрола нафтних и гасних токова, због чега се, у регионима значајним са овог аспекта, могу очекивати нове тензије и кризе“ (Стратегија одбране РС, 2019).

Као изазови, ризици и претње безбедности од значаја за одбрану истакнути су високотехнолошки криминал и угрожавање информационо-комуникационих система. У стратегији су наглашени сајбер напади на критичне инфраструктуре као и ширење лажних вести и дезинформација, што се све може негативно одразити на функционисање елемената система одбране. Стога су заштита и надзор објеката критичне инфраструктуре посебно наглашени у делу „Политика одбране“ са акцентом на превентивне мере заштите (Стратегија одбране РС, 2019). Законом о информационој безбедности Републике Србије, члан 6, дефинисани су ИКТ системи од посебног значаја, што подразумева и примену посебних мера заштите таквих система (Закон о информационој безбедности РС, 2016). Недавни напади на информациони систем Републичког геодетског завода Републике Србије, као и повремено дојаве, путем електронских платформи, о подметнутим бомбама у школама и другим објектима указују на размере и последице таквог деловања.

У СО РС се наглашава да ће се „стварање услова за одбрану реализовати ослонцем на сопствене снаге и потенцијале, посвећивањем посебне пажње планирању развоја система одбране и спровођењу планова и програма развоја. Оперативне способности Војске Србије и других снага одбране биће одржаване на захтеваном нивоу. Такође, обезбедиће се и одржавати потребан ниво попуне робних и ратних материјалних резерви. Од посебног значаја за одбрану, која се ослања на сопствене снаге и потенцијале, биће даљи развој одбрамбене индустрије, те непрекидно стварање услова за функционисање привреде и друштва у ванредном стању и рату. Економским развојем Републике Србије створиће се услови за значајније улагање у развој система одбране и модернизацију Војске Србије и других снага одбране.“ Имајући у виду безбедносно опредељење Републике Србије, приликом разматрања стратегијског концепта одбране, наводи се да се ангажовања система одбране ради заштите и остваривања одбрамбених интереса заснива на моделу тоталне одбране (Стратегија одбране РС, 2019).

Приликом разматрања безбедносног окружења истакнуто је надметање за енергетским ресурсима, што може довести до тензија и криза. Као и у СНБ РС, дакле, истакнути су само енергетски ресурси. Улога и значај инфраструктуре нису разматрани. У СО РС као изазови, ризици и претње од значаја за одбрану истакнути су високотехнолошки криминал и угроженост информационо-

комуникационих система, те се наглашава важност заштите критичних инфраструктура. Наглашава се важност „ослонца“ на сопствене снаге, развој војне индустрије, значај економског развоја и модернизација Војске Србије, чиме ће се створити повољни услови за развој привреде и друштва. У СО РС су недовољно садржани ресурси, док је потпуно занемарена инфраструктура, као неизоставан део (националне) логистике.

Улога и значај логистике у концепту тоталне одбране

Концепт војне неутралности заснован је на добровољном несврставању држава у постојеће војне савезе. Војно неутралне државе принуђене су да развијају одбрамбене стратегије и доктрине засноване на сопственим одбрамбеним националним капацитетима. Политике одбране војно неутралних држава засноване су на концепту тоталне одбране који подразумева интегрално ангажовање свих субјеката одбране и одбрамбених потенцијала, како војних, тако и цивилних, ради оснаживања одбрамбених способности државе (Врачар и Станојевић, 2019, стр. 308). Одређени број држава (нпр. Швајцарска и Аустрија) су се, као и Србија, определиле да буду војно неутралне.

Примена концепта тоталне одбране подразумева интегрисано ангажовање субјеката система одбране и одбрамбених потенцијала државе. По својој суштини он представља облик одбрамбено-безбедносног организовања не само државе у ужем смислу него и друштва у целини. Опредељење Републике Србије да своју одбрану заснива на концепту тоталне одбране исказано је у СНБ РС и СО РС. Примена концепта тоталне одбране треба да омогући свеобухватно, јединствено и интегрално ангажовање свих субјеката система одбране и одбрамбених потенцијала у заштити и остварењу одбрамбених интереса Републике Србије.

Тотална одбрана обухвата војну и цивилну одбрану, а планира се, организује и спроводи у миру, ванредном стању и рату. Постоји потреба да се, поред управљачког дела система одбране како је наведено у СО РС (Народна скупштина, председник Републике, Влада, Министарство одбране, Генералштаб ВС, Савет за националну безбедност), формира и одређено „тело“[3] које би управљало пословима одбране и које би било стручни орган Савета за националну безбедност. Формирањем Врховне команде, на чијем челу би био председник Републике, обезбедило би се ефикасно командовање и војном и цивилном одбраном. Војна одбрана, као део одбране Републике Србије, усмерена је на

[3] Наведено тело би формирала Влада, вероватно би њиме руководио министар одбране, а у његовом саставу би били представници МО, МУП-а, служби безбедности (БИА, ВБА), Војнообавештајне службе (ВОА), као и представника одређених министарстава Републике Србије.

припреме за одбрану и одбрану Републике Србије употребом Војске Србије и других наоружаних снага одбране. Војска Србије обједињава све учеснике у борбеним операцијама и командује свим снагама које изводе борбена дејства у ванредном стању и рату. Цивилна одбрана је део одбране Републике Србије усмерен на припреме за одбрану и одбрану Републике Србије невојним средствима. Реализује се у миру, ванредном стању и рату кроз скуп мера и активности са циљем обезбеђивања успешног функционисања државних органа, органа аутономних покрајина и јединица локалне самоуправе, привредних друштава и других правних лица; стварања услова за живот и рад грађана; задовољења потреба снага одбране; планирања и спровођења планова обуке грађана за одбрану земље; координације послова заштите и спасавања; извршавања војне, радне и материјалне обавезе, као и мобилизације (Стратегија одбране РС, 2019). За успешну реализацију задатака из домена војне одбране одговоран би био Штаб врховне команде на чијем челу би био начелник Генералштаба. Поред формирања Штаба врховне команде, неопходно је формирати и штабове цивилне одбране (републички, покрајински, општински, градски). Основу за припреме и спровођење тоталне одбране представља ослонац на сопствене потенцијале, што не искључује сарадњу са другим државама и међународним организацијама, у складу са одбрамбеним интересима и могућностима.

Извршавање материјалне обавезе према потребама Војске Србије и другим потребама одбране земље обезбеђује Министарство одбране преко територијалних органа, а извршавају је власници материјалних ствари (грађани, привредна друштва, друга правна лица и предузетници). Цивилна одбрана, као део одбране Републике Србије, усмерена је на припреме и одбрану Републике Србије ангажовањем дела или целокупног система одбране у заштити и остварењу одбрамбених интереса Републике Србије (Закон о војној, радној и материјалној обавези, 2009, чланови 96–100).

Цивилну одбрану треба да изводе државни органи, органи државне управе, органи аутономних покрајина, органи јединица локалне самоуправе, јединице цивилне заштите, ватрогасне и ватрогасно-спасилачке јединице, привредна друштва, друга правна лица, предузетници од значаја за одбрану и грађани. Носилац националне логистике јесте цивилна одбрана као део одбране Републике Србије. Одговорност по питању националне логистике јесте у надлежности врховне команде, односно републичког штаба цивилне одбране на чијем челу би био министар одбране.

Законом о одбрани Републике Србије прописана је обавеза планирања припрема за одбрану, а плановима одбране утврђују се задаци субјеката одбране у погледу организације снага, средстава, мера и поступак за рад државних органа и употребу Војске Србије и других снага одбране у

ванредном и ратном стању. Да би систем одбране Републике Србије адекватно реаговао на претње, неопходно је адекватно процењивати изазове.

Закључак

Систем националне безбедности Републике Србије критично је зависан од националне логистике, нарочито у ванредним и кризним ситуацијама. Привреда и ресурси су најпоузданија и најзначајнија логистичка база одбране земље, те је стога најбољи приступ ослањању на сопствене ресурсе. То је нарочито важно имајући у виду безбедносно опредељење Републике Србије. Познавање стања и могућности привреде, као и расположивих ресурса и инфраструктуре, помоћи ће разумевању тренутних и будућих захтева који се могу поставити пред националну логистику (Станојевић, Мишковић и Мишев, 2017).

Променом физиономије савремених оружаних сукоба, у којима се у оквиру војних операција захтева стална мобилност и троше велике количине залиха, национална логистика добија на значају. Ради успешног остварења одбране државе, у току припрема за одбрану и у току извођења одбране, системски се морају на нивоу државе решавати бројни проблеми националне логистике који омогућавају функционисање субјеката одбране (Андрејић, Соколовић и Миленков, 2010, стр. 41). Логистика је кључна за успех на бојном пољу. Да би логистика допринела остваривању победе у оружаном сукобу, мора се константно прилагођавати новим технологијама и концептима (Wissler, 2018, p. 102).

Значај националне логистике се огледа у обезбеђивању неопходних ресурса и пружању различитих услуга како у миру тако и рату. Приликом разматрања стања у Републици Србији треба сагледати да ли је постојећи систем функционисања (националне) логистике развијен у довољној мери да може да подржи извођење борбених операција, односно да ли може испунити све захтеве по питању заштите националних интереса у неизвесним условима, какви су тренутно услед сукоба између Русије и Украјине.

Логистика показује интензивну и разноврсну еволуцију која се неће успорити у наредним годинама. Глобализација кретања робе и транспортних и логистичких мрежа, преношење ширег спектра услуга провајдерима, дигитализација управљања логистиком, аутоматизација складиштења и вожње возила, промене у обрасцима производње, трговине, дистрибуције и потрошње, кључне су компоненте у развоју и напретку логистичких система.

Анализом стратегијских докумената планирања одбране Републике Србије приметно је да национална логистика није препозната као термин, али се у одређеној мери разматрају елементи који је чине (ресурси и инфраструктура). Када су у питању ресурси, у оба документа истакнути су само енергетски, док

осталима није посвећена пажња. Приликом размат рања инфраструктуре приметно је да она није уопште разматрана осим што је у СО РС препозната важност критичних инфраструктура и наглашена потреба њихове заштите од различитих претњи у информационом простору. Поред наведеног, у разматрању одређених елемената (националне) логистике већа је пажња посвећена глобалном и регионалном него националном аспекту.

Библиографија

1. Андрејић, М., Соколовић, В. и Миленков, М. (2010). Концепт развоја служби логистике. *Војнотехнички гласник* 4: 37–62.
2. Врачар, М. и Станојевић, Г. (2019). Стратешка култура Србије и концепт тоталне одбране. *Војно дело* 8: 294–315.
3. Закон о војној, радној и материјалној обавези. (2009). *Службени гласник Републике Србије*, бр. 88/2009, 95/2010 и 36/2018.
4. Закон о одбрани. (2007). *Службени гласник Републике Србије*, бр. 116/07, 88/09, 88/09 – др. закон, 104/09 – др. закон, 10/15 и 36/18.
5. Закон о информационој безбедности Републике Србије. (2016). *Службени гласник Републике Србије*, бр. 6/2016, 94/2017 и 77/2019.
6. Milenkov, M., Sokolović, V., Milovanović, V. i Milić, M. (2020). Logistics – its role, significance and approaches.*Vojnotehnički glasnik* 68 (1): 79–106.
7. NATO Logistics Handbook. (2012). Brussels: *NATO HQ*.
8. Резолуција Народне скупштине о заштити суверенитета, територијалног интегритета и уставног поретка Републике Србије. (2007). Приступљено 15.09.2022. https://www.srbija.gov.rs/kosovo-metohija/index.php?id=80729
9. Savy, M. (2016). Logistics as a political issue. *Transport Reviews* 36(4): 413–417.
10. Станојевић, П., Мишковић, В. и Јефтић, З. (2017). Савремено тумачење појма Национална логистика. *Војно дело* 3: 280–302.
11. Станојевић, П., Мишковић, В. и Мишев, Г. (2017). *Национална логистика и безбедност*. Београд: Факултет безбедности.
12. Стратегија националне безбедности Републике Србије. (2019). *Службени гласник Републике Србије*, бр. 94/2019.
13. Стратегија одбране Републике Србије. (2019). *Службени гласник Републике Србије*, бр. 94/2019.
14. Fechner, I. (2010). Role of logistic centres in national logistics system. *Electronic scientific journal of logistics* 6(2): 9–18.
15. Wissler, J. (2018). Logistics: The Lifeblood of Military Power. Accessed July 5, 2022. https://www.heritage.org/sites/default/files/201809/2019_IndexOfUSMilitaryStrength_CHAPTERS_WISSLER.pdf

(NATIONAL) LOGISTICS IN STRATEGIC DEFENSE PLANNING DOCUMENTS OF THE REPUBLIC OF SERBIA

Abstract

The paper explains the conceptual definition, in the narrower and broader sense, of national logistics, its role and importance. The strategic defense planning documents of the Republic of Serbia, the National Security Strategy and the Defense Strategy, adopted at the end of 2019, were analyzed from the aspect of elements of national logistics. The stated subject of the research is directly related to the goal of the work, which is aimed at indicating and explaining the elements of (national) logistics contained in the mentioned documents, reviewing their compliance, as well as pointing out the perceived shortcomings, considering that these are "dynamic" documents that are periodically updated due to changed challenges, risks and threats to national security. The basic hypothesis is that efficient (national) logisticsis a necessary condition for the functioning of society as well as for the realization of missions and tasks of the management and executive part of the security system (military and police forces, security services, fire-rescueunits, civil protection units, commercial companies, citizens and others) in peace, and especially in periods of crises or armed conflicts. From the essence of the problem and hypothetical attitudes, the basic research question arises: "Whether and to what extent (national) logistics is included in the strategic documents of defense planning of the Republic of Serbia." In addition to general scientific methods, given the subject and goal of the research, the comparative method was mainly used to analyze and compare the contents of the mentioned strategic documents, as well as the method of content analysis, bearing in mind that official documents, scientific works and other publications were used as sources of knowledge. Based on the argument presented in the paper, it can be concluded that national logistics as a term is not recognized in the strategic documents of defense planning, but only its specific elements that are considered, mostly, to a lesser extent.

Keywords: logistics, national logistics, logistic support, strategic documents.

ПРЕДЛОГ ДИНАМИЧКОГ МОДЕЛА ЗА ПЛАНИРАЊЕ И УПРАВЉАЊЕ СТРАТЕШКИМ НАФТНИМ РЕЗЕРВАМА

Милош Јовичић[1]

Апстракт

Одрживо снабдевање есенцијалним енергентима представља приоритет економије сваке државе. Са повећањем међузависности економија на глобалном нивоу, од великог је значаја препознати постојање ризика у кључним ланцима снабдевања храном, производима и енергентима. Један од битних ланаца снабдевања за свакодневно функционисање економије јесте ланац снабдевања нафтом и нафтним дериватима. У раду је анализиран концепт стратешких нафтних резерви (СНР) као алата за сузбијање низа дисрупција у одрживом снабдевању нафтом и нафтним дериватима. Циљ спроведеног истраживања је проналажење оптималног приступа у моделирању националног ланца снабдевања нафтом и структуре стратешких нафтних резерви. Креирани симулациони модел омогућава анализу стања нафтних резерви на нивоу државе и пружа могућности анализе различитих политика управљања у условима прекида снабдевањем сировом нафтом или нафтним дериватима. Циљ модела је да анализира резилијантност националног ланца снабдевања под утицајем различитих екстерних и интерних стресора.

Кључне речи: *динамика система, симулације, ризик, нафтне резерве*

---

[1] Истраживачко-развојни институт за вештачку интелигенцију Србије, Фрушкогорска 1, Нови Сад, Србија e-mail: milos.jovicic@ivi.ac.rs

Рад је настао у оквиру пројекта Фонда за науку Републике Србије „Идеје“ – Пројекат акцелерације иновација и подстицања раста предузетништва у Републици Србији – Management of New Security Risks – Research and Simulation Development – NEWSIMR&D, #7749151.

Увод

Национална енергетска безбедност која се манифестује кроз поуздан приступ енергената становништву, привреди и јавном сектору представља приоритет сваке државе. Почетком седамдесетих година прошлог века, појављује се једна од првих интеграција области управљања ризиком и стратегије националне енергетске безбедности, кроз формирање концепта стратешких енергетских резерви (Leffler and Melvyn, 1985). Концепт стратешких енергетских резерви подразумева набавку и презервацију различитих фракција енергената, који имају дефинисан циклус употребе према безбедоносним и економским околностима у којима се једна држава налази. Ове резерве служе као бафер за ублажавање ефеката нежељених догађаја у случају неконтролисане волатилности цена енергената или у условима неизвесности са стране произвођача или добављача одређеног енергента. Најчешће анализиране резерве енергената од стране регулаторних тела као и економских агената јесу стратешке нафтне резерве (у даљем тексту СНР). Формирање стратешких нафних резерви постају битна државна политика на глобалном нивоу седамдесетих година прошлог века (Davis and Ruth, 1981). Због енергетске кризе изазване Арапским нафтним ембаргом који је трајао од 1973. до 1974. године, Конгрес Сједињених Америчких Држава одобрава формирање стратешких нафтних резерви, као и низа регулаторних тела која имају за циљ очување националне енергетске безбедности (Andrews and Pirog, 2012). Са формирањем СНР 1975. године, Сједињене Америчке Државе на својој територији покрећу стратешки државни пројекат за обезбеђивање енергетске резилијантноси државе. Донети акт САД о енергетској политици и конзервацији националних интереса стриктно дефинише услове под којима стратешке нафтне резерве могу бити коришћене (Hubbard Weiner, 1985). САД се такође обавезују да ће користити своје стратешке резерве нафте, према потребама успостављања енергетске стабилности држава чланица Интернационалне енергетске агенције (ИЕА). У складу са дефинисаним регулативама ИЕА, све државе чланице су у обавези да формирају систем стратешких нафтних резерви који обезбеђује доступност 90 дана нето увоза нафте (Van de Graaf and Lesage, 2009). Све форме СНР се сагледавају као стратегија митигације ризика или полиса осигурања за државну енергетску безбедност. Поред директне важности формирања система енергетских резерви за државу, СНР као и друге резерве енергената могу имати изузетан утицај у одржавању економске стабилности и кооперације између различитих држава једног региона. Постоји низ начина на који стратешке нафтне резерве као и друге енергетске резерве једне државе могу бити формиране. Највећи фактор у детерминацији структуре система енергетских резерви представља ниво капиталних инвестиција које је држава спремна да издвоји за осигуравање енергетске безбедности. Истраживачки рад предлаже симулациони модел за анализу енергетске резилијантности државе и сагледавање

опција за формирање или унапређење постојећих СНР. Кроз истраживање је сагледан концепт стратешких енергетских резерви, као алата за митигацију различитих ризика енергетског сектора. Циљ дизајнираног модела је омогућавање симулирања ефеката различитих социоекономских криза и природних катастрофа, и могућност енергетског система да на поуздан начин одговори на потребе тржишта.

Резилијантност енергетских система и процена ризика

Постојећи приступ у процени ризика

У периоду од 1950. године до друге деценије 21. века, регистровано је више од 30 енергетских криза везаних за расположивост сирове нафте и нафтних деривата. Само време реализације наведених дисрупција варира од два узастопна квартала до вишегодишњег периода трајања (Chen et al., 2020). Поред повремене неизвесности у цени и расположивости нафте, битно је истаћи и важност енергетске стабилности у снабдевању природним гасом. Глобално снабдевање природним гасом за потребе индустрије и домаћинстава сагледава значајан раст на годишњем нивоу, због своје економичности као и ниског утицаја на процес глобалног загревања (Yousaf and Lin, 2022). Међутим, енергетски ризици везани за снабдевање овим енергентом дошли су у први план са почетком руско-украјинског рата 2022. године (Mbah and Wasum, 2022).

Државе Европске уније имају формиран легални систем за поступање у кризним ситуацијама изазваним енергетском кризом (Mastropietro, 2022). Нежељени догађаји на светским тржиштима енергената, поред легалне инфраструктуре, захтевају и адекватан приступ управљању ризиком ка остваривању националне енергетске безбедности. Препознавање трендова који утичу на националну енергетску безбедност, као и одрживо снабдевање енергентима регионалних комплекса, од кључног је значаја за успостављање методологије за енергетски ризик (Stanojević, 2022). Методе за енергетски ризик морају да укажу на стратегије мерења, митигације (ублажавања) и даље превенције нежељених стресора, који долазе са волатилним догађајима на светским тржиштима енергената. Алати и методе за планирање енергетске безбедности морају бити у могућности да сагледају целокупни енергетски систем једне државе, и са адекватним нивоом поузданости прикажу динамичко понашање система у различитим условима. Разумевање лимитација сваког алата за анализу ризика комплексних система, попут ланца снабдевања нафтом, од кључног је значаја у процесу планирања, тј. сам процес планирања мора бити усклађен према лимитацијама у прецизном предвиђању како ће динамички систем реаговати на нежељени догађај. Глобални ланци снабдевања нафтом су под великим утицајем политичких одлука, што захтева честу анализу политичког ризика у доношењу

одлука (Gebelein et al., 1978). Алати за детерминацију политичког ризика због своје честе зависности од инпута експертског мишљења, које представља непоуздан алат за анализу ризика (Shiller, 2002), могу угрозити интегритет остатка модела.

Већина алата за мерење и митигацију ризика у оквиру тржишта енергената адаптирана је за потребе финансијских институција, у креирању вредности кроз финансијске трансакције везане за цене енергената (Eydeland et al., 2002). Иако ови алати могу бити коришћени за одређене аспекте националне енергетске сигурности, постоји потреба за развојем методологија специјализованих за изазове националне енергетске безбедности. Енергетски систем сваке државе може бити класификован као комплексни систем, и самим тим анализирање ризика коришћењем конвенционалних метода попут ВаР-а (*VaR – value at risk*) јесте неадекватно (Sadeghi et al., 2006), и са собом носи низ недостатака и потенцијалних хазарда (Geman et al., 2015). Висок степен непоузданости често коришћених економетријских алата треба узети у обзир приликом анализе комплексних нелинеарних система (Taleb, 2009). Постоји низ истраживања из области менаџмента ризиком која указују на недостатке високо комплексних статистичких модела у њиховој практичној примени у односу на једноставније моделе засноване на доброј хеуристици (Makridakis and Taleb, 2009).

Концепти резилијантности и антифрагилности система

Један од недостатака традиционалних метода за анализу ризика у случају комплексних система може се сагледати и у њиховом непрепознавању феномена резилијантности и антифрагилности система. Резилијантност дефинише способност система да након нежељеног догађаја или стресора поврати своје капацитете у првобитно стање (Afgan and Veziroglu, 2012). Концепт антифрагилности је значајно комплекснији у односу на појам резилијантности и базиран је на успостављеном приступу моделирања и мапирања динамичког понашања код комплексних система (Taleb and Douady, 2013). Антифрагилност дефинише способност система да након нежељеног догађаја или стресора дође у супериорније стање од иницијалног (Aven, 2015). Антифрагилни системи попут биолошких организама налазе се у континуалној фази адаптације, тј. учења на претходним грешкама и стресорима. Једна од честих критика стратегија за постизање резилијантности код компанија или ланаца снабдевања јесте недостатак у припреми система за наредни ризик који може имати већи интензитет и комплексност од већ реализованих догађаја. Биолошки системи након изложености нежељеном догађају имају тенденцију да уђу у стање прекомерне компензације (*overcompensation*) (Tomov, 2019), тј. да креирају резервне капацитете да у будућности превазиђу нежељени догађај већег интензитета.

Предмет истраживања је сагледавање оптималног приступа за моделирање и симулацију нафтног ланца снабдевања, формирања структуре стратешких нафтних резерви, као и анализа резилијантности система. Поред конвенцијалног приступа креирања способности система да буде резилијантан, анализиране су могућности и стратегија за остваривање одређеног нивоа антифрагилности националног ланца снабдевања нафтом. Концепт стратешких резерви нафте сагледан је као динамички систем, који захтева континуалну адаптацију ка бољем омогућавању енергетске безбедности државе. Разлог за предлагање да национални систем снабдевања нафтом мора бити више него резилијантан произилази из убеђења да нежељени догађаји у будућности за анализирани систем неће имати исту динамику као већ реализовани ризици (Taleb, 2012).

Моделирање нафтног ланца снабдевања

Глобални ланци снабдевања нафтом (у даљем тексту ЛСН) сачињени су од три оперативно зависна сегмента: апстрим (*upstream*) производње, мидстрим (*mid-stream*) логистичко-транспортног сектора и даунстрим (*downstream*) сектора прераде и промета (Hadi et al., 2014). Сва три наведена сегмента обухватају различите облике складиштења нафте или нафтних деривата, што захтева поуздану логистичку координацију између агената који се налазе у различитим секторима ланца снабдевања. Оператери који се налазе у различитим сегментима ланца снабдевања, тј. секторима екстракције енергената, прераде, транспорта и дистрибуције, значајно се разликују у инфраструктури и операцијама које спроводе, као и у ризицима којима су изложени.

Апстрим производња обухвата све системе првобитне екстракције и складиштења нафте и гаса; економски ентитети овог сегмента се суочавају са највећим степеном ризика и неизвесности у проналажењу и ефикасној екстракцији енергената. Процес евалуације потенцијалних инвестиција представља комплексан и неизвестан процес, међутим, однос ризика и потенцијалне добити у овом сектору изузетно је висок у односу на остале сегменте нафтног ланца снабдевања (Surbhi, 2012). Остали сегменти ЛСН са собом носе значајно ниже ризике и засновани су на процесу транспорта, складиштења, прераде и операција промета нафтом и нафтним дериватима. Независно од позиције у ЛСН државни и приватни економски ентитети међусобно су зависни и ефикасна функција целокупног система зависи од избегавања дисрупција у било којем делу ланца.

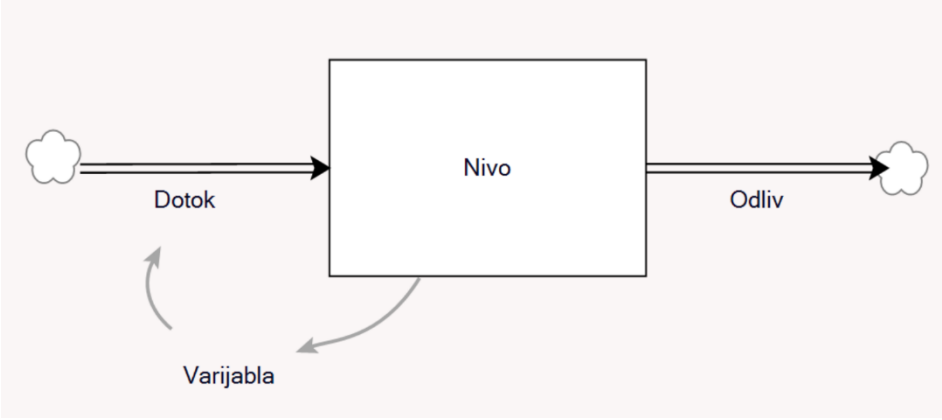
Комплексни системи попут ланаца снабдевања нафтом, из погледа математичког моделирања, по својој структури су нелинерани, сачињени од низа повратних петљи и функција застоја (*delay functions*). Један од приступа у анализи комплексног система попут ланца снабдевања нафтом јесте коришћење симулационих технологија. Моделирање и симулације система различитих нивоа

апстракција може бити спроведено кроз коришћење три симулациона приступа: динамиком система, симулацијама дискретних догађаја и симулацијама заснованим на агентима (Borshchev et al., 2014). Наведени приступи пружају могућности у симулирању сегмената ниске апстракције у енергетском систему, попут физичких мрежа нафтовода и енергетских складишта (Bauer et al., 2019), до могућности нумеричке анализе елемената високе апстракције, попут енергетске политике и система понуде и потражње (Daneshzand at al., 2018). Битно је истаћи да комплексни феномени у ланцима снабдевања, попут ефекта бича (*bullwhip effect*), иницијално су концептуализовани након настанка симулационох методологија, попут динамике система (Hadžimetović and Vujošević, 2017). Креирање и развој симулационих методологија пружило је низ могућности у симулирању и оптимизацији система попут: здравствених система (Stainsby, Taboada, Luque, 2009), ланаца снабдевања (Angerhofer and Angelides, 2000), инфраструктурних пројеката (Han et al., 2013), комуналних система (Winz et al., 2009) итд. Симулационе методологије пружају могућности да се графички и нумерички концептуализује било који комлексни систем, са циљем спровођења оптимизације или жељеног облика анализе.

Моделирање динамиком система

За анализу националног ланца снабдевања нафтом одабрана је динамика система (у даљем тексту ДС) као примарна симулациона метода. Ова симулациона методологија заснована је на структури система нелинеарних диференцијалних једначина првог реда као и интегралних једначина. Динамика система као симулациона методологија настаје почетком педесетих година прошлог века, као резултат истраживања професора Џеја Форестера (*Jay Forrestert*) (Radzicki and Taylor, 2008). Професор Форестер је један од раних пионира компјутерске револуције 20. века због његовог доприноса у изградњи Вирлвинд 1 (*Whirlwind I*) дигиталног електронског компјутера 1951. године (Forrester, 1990). Циљ креирања динамике система као филозофског и математичког приступа за управљање комплексним системима јесте превазилажење лимитација код стандардних статистичких метода научног менаџмента и економије. Динамика система је брзо пронашла апликације у решавању кључних стратешких проблема индустријског менаџмента (Forrester, 1968) и урбаног планирања (Forrester, 1970). Ова симулациона методологија је имала и кључну улогу у покретању области еколошких наука, кроз креирање модела лимита раста (*limits to growth*), који је допринео промени свести на глобалном нивоу о начину експлоатације природних ресурса и одрживом економском расту држава (Meadows et al., 2018). Један од највећих бенефита коришћења динамике система јесте у могућности лаке визуелне инспекције модела. Сама методологија је заснована на објектно

оријентисаном моделирању и користи пет основних објеката за концептуализацију структуре: доток, ниво, одлив, варијабле и повратна петља (стрелица) (Слика 1).



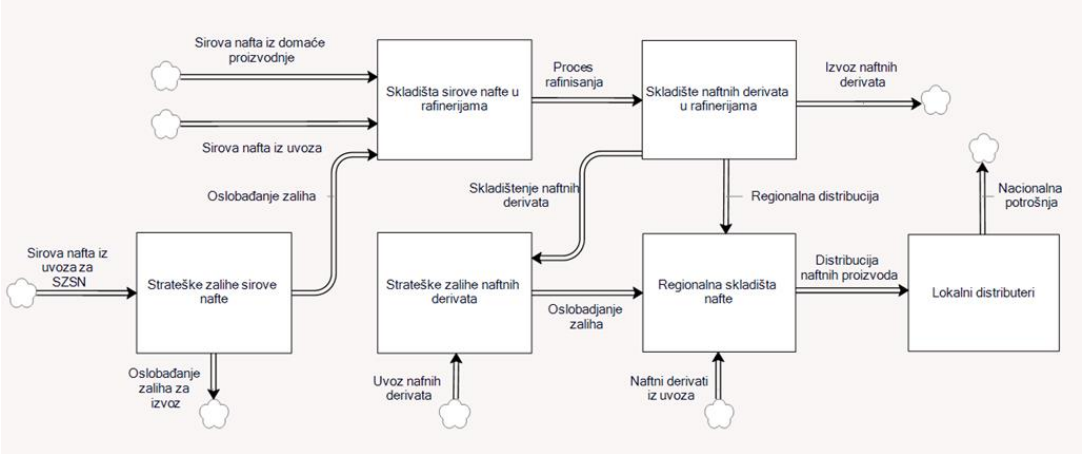
Слика 1: Основни објекти за моделирање у динамици система

Објектно оријентисано моделирање пружа могућности да се симулациони модели дизајнирају и анализирају у групама стејкхолдера (*stakeholder*), где већина стејкхолдера не мора бити обучена у коришћењу самог алата (Peck, 1998). Кључни објекат у сваком ДС моделу је ниво који омогућава складиштење информација или материјала. Структуру приказану на слици 1 треба сагледавати као функционисање једноставног резервоара, док су промене вредности у објекту нивоа могуће само кроз нумеричке промене у дотоку или одливу. На слици 1 приказане су и стрелице (повратне петље) које повезују објекат нивоа са варијаблом и дотоком. Ова једноставна структура кроз коришћење повратних петљи омогућава регулацију објекта дотока кроз објекат варијабле која може бити заснована на прорачуну тренутног стања објекта нивоа и жељеном стању у којем објекат ниво треба да се налази.

Предлог модела за анализу стратешких нафтних резерви и резилијантноси система

Модел за управљање стратешким нафтним резервама треба да обухвата функционисање целокупног ланца снабдевања једне државе, тј. модел СНР представља само део структуре модела који симулира шири систем. У случају да држава у оквиру свог енергетског система садржи и производњу нафте и гаса, модел може имати низ бенефита у обухватању и тог сегмента ланца снабдевања. Дизајнирани модел је сачињен од више нивоа апстракције ланца снабдевања нафтом и нафтним дериватима. На слици 2 приказан је макромодел операција стратешких резерви нафте и целокупног ланца снабдевања. Макромодел обухвата

сагледавање стратешких резерви сирове нафте као и нафтних деривата, при чему је велика важност стављена на адекватно дефинисање структуре протока СНР унутар ланца снабдевања нафтом.

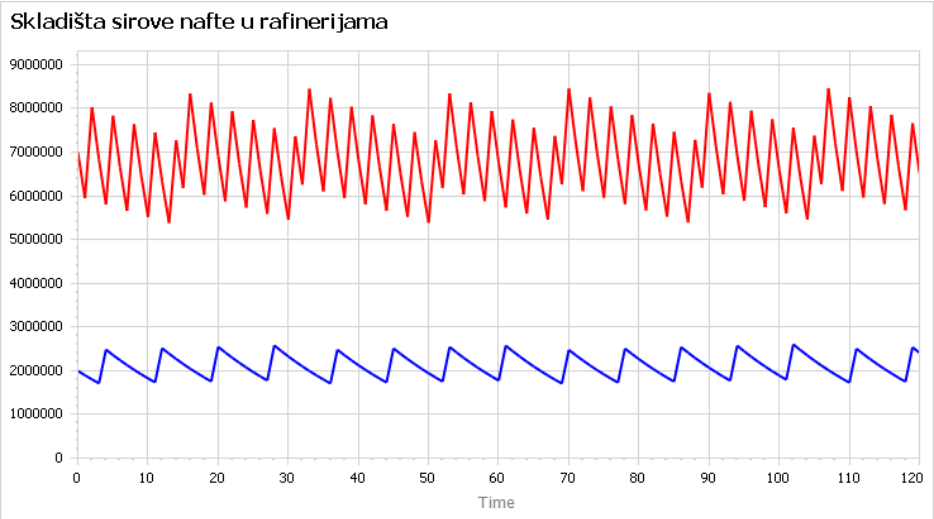


Слика 2: Макромодел СНР и ланца снабдевања нафтом

Проток нафте и нафтних деривата у макромоделу функционише из смера леве стране производње и увоза нафте ка десној страни извоза и промета. У макромоделу СНР су дефинисане са два нивоа: стратешке залихе сирове нафте (у даљем тексту СЗСН) и стратешке залихе нафтних деривата (у даљем тексту СЗНД). Вредност нивоа СЗСН је регулисана променама у дотоку сирова нафта из увоза за СЗСН и одливима ослобађање залиха и ослобађање залиха за извоз. Одлив ослобађање залиха омогућава да се сирова нафта из СЗСН пусти у национални систем, тј. да се попуне залихе сирове нафте у рафинеријама.

Дизајнирани модел ланца снабдевања нафтом садржи популације различитих агената. Модел је дизајниран да садржи популацију државних ентитета за: складиштење нафте, прераду, транспорт и промет. Самим тим, модел прави разлику између државних залиха нафте и нафтних деривата које се налазе у систему и залиха које су у приватном власништву. На слици 3 приказане су вредности залиха сирове нафте у рафинеријама које су под државним власништвом (црвено) и под приватним власништвом (плаво). Модел користи експерименталне податке о капацитетима рафинерија у енергетском сектору Европе за 2022. годину (Klepikov et al., 2022).

На слици 3 симулирана је стратегија обавезивања државних и приватних рафинерија да не дозвољавају да им залихе сирове нафте падају испод одређене количине (вредности су исказане у барелима сирове нафте).



Слика 3: Вредност нивоа складишта сирове нафте у рафинеријама

Битно је нагласити да модел може прорачунавати различиту политику према стратешким нафтним резервама, од коришћења и проширења државних капацитета до политике креирања СНР у оквиру приватног сектора. Постоји низ структура за организацију стратешких резерви нафте – од система државног власништва над резервама до интеграције са приватним сектором (Colgan, 2009). Макромодел на слици 2 приказује одлив тј. ослобађање залиха за извоз, што указује на продају залиха сирове нафте или размене са другим државама. Сам модел има могућности да симулира различиту политику према ослобађању резерви сирове нафте у систем и политику према резервама нафтних деривата. Сама политика према ослобађању резерви нафтних деривата у систем у случају дисрупције треба бити посебно анализирана како са локалног микронивоа тако и са макронивоа државе.

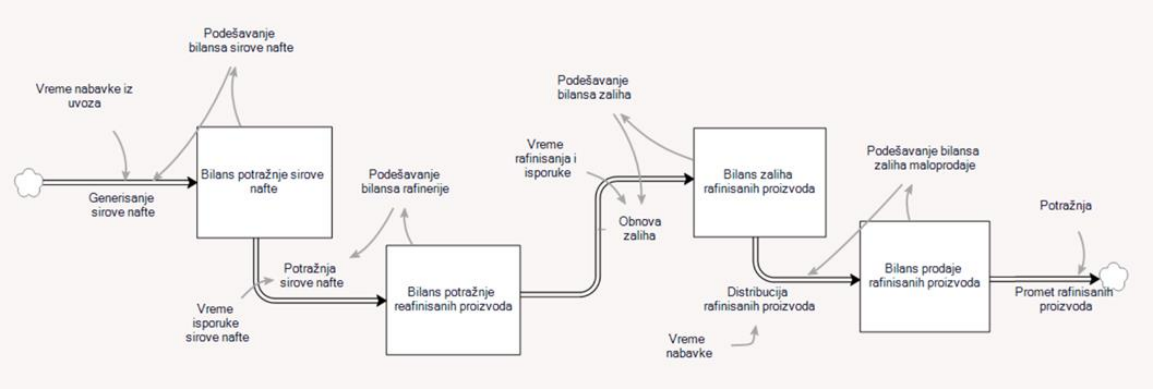
Макромодел на слици 2 је дефинисан са више подмодела који прорачунавају вредности за дотоке и одливе у макромоделу. Одлив ослобађање залиха приказан на слици 2, који одређује количине сирове нафте које треба пустити у систем у случају дисрупције, добија вредности из подмодела приказаног на слици 4. Варијабла периодична тест продаја има за циљ да иницира мање продаје/ослобађања резерви сирове нафте. Варијабла периодична тест продаја СНР користи се као алат за анализу ефикасности операција система, тј. идентификацију свих нерегуларности, застоја и уских грла приликом функционисања СНР. Од изузетног је значаја да сви проблеми у дистрибуцији сирове нафте из СЗСН буду идентификовани у мањим ослобађањима. Важност

спровођења тест продаја је потенцијално највећа у случају да је држава дизајнирала своје стратешке резерве енергената у партнерству са компанијама приватног сектора, што чини систем потенцијално комплекснијим за управљање. Друга форма мањег ослобађања сирове нафте из СЗСН јесте спровођење размене сирове нафте. Варијабла размена сирове нафте симулира процес дистрибуције мањих количина резерви сирове нафте ка приватним ентитетима који се налазе у краткорочним застојима у сервисирању тржишта. Овај процес има за циљ да ублажи краткорочне проблеме дистрибуције нафте и нафтних деривата на тржишту. Размена сирове нафте се може сагледавати као облик „краткорочног кредита“ који држава склапа према приватном дистрибутеру, тако да се размена искључиво спроводи са нафтом и од дистрибутера се, поред повраћаја сирове нафте у СНР, очекује да плати и прописану премију.

Слика 4: Подмодел за прорачун вредности одлива ослобађање залиха

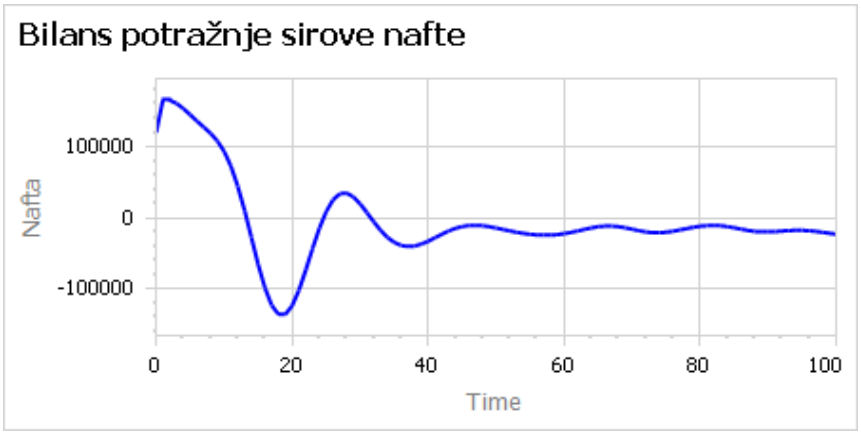
Ослобађање залиха нафте из СЗСН обавља се превасходно према санирању већих дисрупција у ланцу снабдевања, што представља и примарни циљ овог система. Модел је дизајниран за унос различитих врста дисрупције, где се кроз прорачун обима прекида и расположивих капацитета за дистрибуцију из СЗСН одређује нумеричка вредност за одлив варијабле ослобађање залиха нафте.

Битан сегмент модела је и подмодел за прорачун односа понуде и потражње, пре свега у анализи ефекта „бича“ у ланцу снабдевања. Подмодел има сличну структуру као постојећи симулациони модели за анализу ефекта „бича“ у снабдевању нафтом (Zhang, J. H. and Zhang, Q. Q., 2013). Подмодел је сачињен од четири нивоа: биланс потражње сирове нафте, биланс потражње рафинисаних производа, биланс залиха рафинисаних производа и биланс продаје рафинисаних производа. Подмодел анализира однос потражње нафтних деривата од стране тржишта и могућности система у испуњавању захтева тржишта. Сваки ниво у подмоделу прорачунава биланс понуде и потражње и самим тим нова вредност може бити негативна. Биланси не представљају физичке залихе нафте у систему, где, у том случају, било који од четири нивоа не би могао да има вредност испод 0. Кретање информација у моделу протиче са десне на леву страну, тј. тржиште креира пул ефекат (*pull effect*). Сваки од нивоа представља сегмент ланца снабдевања: увоз сирове нафте, складиштење, процес прераде и даље складиштење и дистрибуцију.



Слика 5: Подмодел за прорачун односа понуде и потражње

Приликом анализе ефекта бича у ланцу снабдевања од великог је значаја доћи до прецизног времена застоја између сегмената ланца. Време процесирања или време застоја између ентитета у дистрибутивном ланцу игра кључну улогу у функцији целокупног ланца. За потребе рада узете су експерименталне вредности из радова који су проучавали овај феномен користећи динамику система (Zhang, J. H. and Zhang, Q. Q., 2013). На слици 6 приказане су вредности за биланс потражње сирове нафте који се налази на почетку подмодела. Тржишна потражња дефинисана је функцијом RandomUniform (135000, 160000), јединице за функцију су барел/дан.



Слика 6: Биланс потражње сирове нафте

Слика 7: Биланс продаје рафинисаних производа

Слика 7 приказује биланс продаје рафинисаних производа који показује велику нестабилност у периоду првих 20 дана операција. Осцилације приказане подмоделом указују на велике застоје у ланцу снабдевања, као и неадекватно држање залиха у ланцу. Битно је назначити да генерални економски интерес стејкхолдера у ланцима снабдевања јесте избегавање држања прекомерних количина залиха, из разлога што таква политика доводи до погоршања кешфлоа фирме (*cashflow*) и креира низ оперативних ризика. Као што је већ назначено, у подмоделу нису приказане вредности физичких залиха нафте или рафинисаних производа, тако да саме залихе не могу бити негативне. Важност овог сегмента модела је да укаже на потенцијалне осцилације у ланцу снабдевања на које систем СНР може да одговори.

Закључак

Дизајниран је динамички модел за стратешко планирање државне енергетске политике. Кроз коришћење модела могуће је утврдити колико је резилијантан национални ланац снабдевања нафтом према различитим дисрупцијама. Динамички модел сагледава проток и складиштење државних и приватних резерви сирове нафте и нафтних деривата. Из модела могуће је закључити колико дуго је национална економија у могућности да функционише у условима ограниченог снабдевања нафтом и различите политике према стратешким нафтним резервама. Модел омогућава тестирање различитих политика према стратешким нафтним резервама, као и могућност сагледавања алтернатива за реконструкцију целокупног система, кроз повећање учешћа приватног сектора у систему СНР. Будућа истраживања могу бити усмерена ка проширењу модела да анализира резерве и других енергената, као и функционисање дистрибутивних капацитета у различитим ванредним ситуацијама.

Библиографија

1. Afgan, N. and Veziroglu, A. (2012). Sustainable resilience of hydrogen energy system. *International Journal of Hydrogen Energy* 37 (7): 5461–5467.
2. Andrews, A. and Pirog, R. (2012). *The strategic petroleum reserve: authorization, operation, and drawdown policy*. Congressional Research Service, Library of Congress.
3. Angerhofer, B. J. and Angelides, C. M. (2000). System dynamics modelling in supply chain management: research review. *In 2000 Winter Simulation Conference Proceedings* (Cat. No. 00CH37165), vol. 1, pp. 342–351. IEEE
4. Arora, S. (2012). Investment decision making in the upstream oil industry: An analysis. Available at SSRN 1983123.
5. Aven, T. (2015). The concept of antifragility and its implications for the practice of risk analysis. *Risk analysis* 35(3): 476–483.
6. Bauer, V. I., Bazanov, V. A., Kozin, S. E., Nemkov, M. V. and Mukhortov, A. A. (2019). Optimization of technological transport sets using anylogic simulation environment. *Journal of Mechanical Engineering Research and Developments* 42(2): 41–43.
7. Borshchev, A., Brailsford, S., Churilov, L. and Dangerfield, B. (2014). Multi-method modelling: AnyLogic. *Discrete-event simulation and system dynamics for management decision making*, 248–279.
8. Chen, S., Zhang, M., Ding, Y. and Nie, R. (2020). Resilience of China's oil import system under external shocks: A system dynamics simulation analysis. *Energy Policy* 146: 111795.
9. Colgan, J. D. (2009). The international energy agency. Challenges for the 21st Century. *GPPi Energy Policy Paper* 6.
10. Daneshzand, F., Amin-Naseri, M. R., Elkamel, A. and Fowler, M. (2018). A system dynamics model for analyzing future natural gas supply and demand. *Industrial & Engineering Chemistry Research* 57 (3): 11061–11075.
11. Davis, R. M. (1981). National strategic petroleum reserve. *Science* 213(4508): 618–622.
12. Eydeland, A. and Wolyniec, K. (2002). Energy and power risk management: New developments in modeling, pricing, and hedging. Vol. 97. *John Wiley & Sons*.
13. Forrester, J. W. (1968). Industrial dynamics — a response to Ansoff and Slevin. *Management Science* 14 (9): 601–618.
14. Forrester, J. W. (1970). Urban dynamics. *IMR; Industrial Management Review* (pre-1986) 11, no. 3: 67.
15. Forrester, J. W. and Everett, R. R. (1990). The Whirlwind computer project. *IEEE Transactions on Aerospace and Electronic Systems* 26(5): 903–910.

16. Gebelein, C. A., Pearson, E. C. and Silbergh, M. (1978). Assessing political risk of oil investment ventures. *Journal of Petroleum Technology* 30(5): 725–730.
17. Geman, D., Geman, H. and Taleb, N. N. (2015). Tail risk constraints and maximum entropy. *Entropy* 17 (6): 3724–3737.
18. Hadžimetović, M. D. and Vujošević, B. M. (2017). Zavisnost efekta biča od sklonosti ka riziku učesnika u lancu snabdevanja. *TEHNIKA – MENADŽMENT 67*.
19. Han, S., Love, P. and Peña-Mora, F. (2013). A system dynamics model for assessing the impacts of design errors in construction projects. *Mathematical and Computer Modelling* 57(9–10): 2044–2053.
20. Hubbard, R. G. and Weiner, J. R. (1985). Managing the strategic petroleum reserve: energy policy in a market setting. *Annual review of energy* 10(1): 515–556.
21. Klepikov, V. P. and Klepikova, L. V. (2022). Trends in capacity changes in oil refining in the European energy sector. *Energy Reports* 8: 586–592.
22. Leffler, M. P. (1985). Strategy, Diplomacy, and the Cold War: The United States, Turkey, and NATO, 1945–1952. *The Journal of American History* 71(4) :807–825.
23. Makridakis, S. and Taleb, N. (2009). Living in a world of low levels of predictability. *International journal of forecasting* 25(4): 840–844.
24. Mastropietro, P. (2022). Energy poverty in pandemic times: Fine-tuning emergency measures for better future responses to extreme events in Spain. *Energy Research & Social Science* 84: 102364.
25. Mbah, R. E. and Forcha Wasum, D. (2022). Russian-Ukraine 2022 War: A review of the economic impact of Russian-Ukraine crisis on the USA, UK, Canada, and Europe. *Advances in Social Sciences Research Journal* 9(3): 144–153.
26. Meadows, D. H., Meadows, L. D., Randers, J. and Behrens, W. W. (2018). The limits to growth. *In Green planet blues*, pp. 25–29. Routledge.
27. Peck, S. (1998). Group model building: facilitating team learning using system dynamics. *Journal of the Operational Research Society* 49(7): 766–767.
28. Radzicki, M. J. and Taylor, A. R. (2008). Origin of system dynamics: Jay W. Forrester and the history of system dynamics. *US Department of Energy's introduction to system dynamics*.
29. Raza, M. Y. and Lin, B. (2022). Natural gas consumption, energy efficiency and low carbon transition in Pakistan. *Energy* 240: 122497.
30. Sadeghi, M. and Shavvalpour, S. (2006). Energy risk management and value at risk modeling. *Energy policy* 34(18): 3367–3373.

31. Sahebi, H., Nickel, S. and Ashayeri, J. (2014). Strategic and tactical mathematical programming models within the crude oil supply chain context – A review. *Computers & Chemical Engineering* 68: 56–77.
32. Shiller, R. J. (2002). Bubbles, human judgment, and expert opinion. *Financial Analysts Journal* 58(3): 18–26.
33. Stainsby, H., Taboada, M. and Luque, E. (2009). Towards an agent-based simulation of hospital emergency departments. In *2009 IEEE International Conference on Services Computing*, pp. 536–539. IEEE
34. Stanojević, P. Model za prognozu trendova u ostvarivanju energetske bezbednosti zemalja i regionalnih kompleksa. *Sociološki pregled* 56(3): 797–831.
35. Taleb, N. N. (2012). The future has thicker tails than the past: Model error as branching counterfactuals. *arXiv preprint arXiv:1209.2298*.
36. Taleb, N. N. and Douady, R. (2013). Mathematical definition, mapping, and detection of (anti) fragility. *Quantitative Finance* 13(11): 1677–1689.
37. Taleb, N. N. (2009). Errors, robustness, and the fourth quadrant. *International Journal of Forecasting* 25(4): 744–759.
38. Taleb, N. N. (2009). Errors, robustness, and the fourth quadrant. *International Journal of Forecasting* 25(4): 744–759.
39. Tomov, L. (2019). Is Agile Antifragile? *Small* 58(38): 4.
40. Van de Graaf, T. and Lesage, D. (2009). The International Energy Agency after 35 years: Reform needs and institutional adaptability. *The Review of International Organizations* 4 (3): 293–317.
41. Winz, I., Brierley, G. and Trowsdale, S. (2009). The use of system dynamics simulation in water resources management. *Water resources management* 23(7): 1301–1323.
42. Zhang, J. H. and Zhang, Q. Q. (2013). The System Dynamics Analyses of Bullwhip Effect in China Processed Oil Supply Chain. *In Applied Mechanics and Materials*, Trans Tech Publications Ltd, vol. 295, pp. 3310–3317.

PROPOSAL OF A DYNAMIC MODEL FOR PLANNING AND MANAGEMENT OF STRATEGIC OIL RESERVES

Abstract

Providing a sustainable petroleum supply to the economy is the priority of every country. With the increase of interconnectivity between the economies on the global level, it is essential that the presence risks that effect the key supply chains (food, consumer goods and energy), is recognized. One of the crucial supply chains for the everyday operations of the economy, is the crude oil and refined products supply chain. The research has analyzed the concept of strategic petroleum reserves (SPR) as a tool for buffering the disruptions in a petroleum supply chain. The goal of the conducted research is to find an optimal modeling approach for conceptualization and analysis of the national petroleum supply chain (NPSC), and the SPR structure that exists within the NPSC. The created simulation model provides the analysis of the available petroleum supplies on the national level, as well as providing capabilities in analyzing different policies in addressing the disruptions in crude oil and refined products supply. The main goal of the model is to determine the resilience of the national petroleum supply chain under the influence of different external and internal stressors.

Keywords: *system dynamics, simulations, risk, oil reserves*.

ЛОГИСТИКА НАФТЕ И НАФТНИХ ДЕРИВАТА У СРБИЈИ

Петар Станојевић[1]

Апстракт

Логистика нафте и нафтних деривата у Србији приказана је са више аспеката у овом раду. Описана је логистика сирове нафте, деривата и анализирани су капацитети за увоз сирове нафте и деривата. Начињен је преглед и анализа могућности лучких нафтних терминала за снабдевање српског тржишта. Урађена је анализа потреба српског тржишта за нафтом и дериватима и урађена је процена потребних логистичких капацитета за увоз нафте и деривата нафте различитим видовима транспорта. Посебно су анализирани рафинеријски капацитети за пријем и прераду као ограничавајући логистички фактор. Посебна пажња је дата постојећим капацитетима који би се могли искористити за обезбеђење сигурности снабдевања српског тржишта и могућим новим правцима снабдевања који укључују нове нафтоводе, ревитализацију пруга и возног парка, као и повећање дунавске танкерске флоте.

Потврдила се претпоставка да логистика нафте и снабдевање нафтним дериватима у Србији имају уско грло у Јадранском нафтоводу. Други капацитети за увоз сирове нафте могли би да задовоље само минимум потребан за континуиран рад рафинерије. Капацитети за увоз деривата су довољни, ако би се могли набавити и пребацити до разматраних лука. Као повољни са становишта снабдевања могли би се оценити луке Солун, Констанца и Омишаљ. Мање повољни су Бургас, Бар и Копар. Остали терминали представљају луке које би се могле користити само у нужди.

---

[1] Факултет безбедности, Универзитета у Београду, e-mail petr.stanojevic@fb.bg.ac.rs; petstano45@gmail.com,

Рад је настао у оквиру пројекта Фонда за науку Републике Србије „Идеје“ – Пројекат акцелерације иновација и подстицања раста предузетништва у Републици Србији – Management of New Security Risks – Research and Simulation Development – NEWSIMR&D, #7749151.

Закључено је да Србија мора размотрити алтернативне правце снабдевања као што су нафтоводи у правцу Мађарске, Румуније, Македоније, Грчке и Албаније. Могућа решења су и у унапређењу пруга Београд–Бар и Београд–Солун, које би биле знатно веће пропусне могућности уз куповину одговарајућих капацитета у локомотивама и вагон-цистернама. Слично би се могло урадити кроз куповину „резервне“ флоте баржи којима би се нафта и деривати могли транспортовати у кризним ситуацијама. Потребна су и улагања у складишни простор за нафту и деривате. У свакој од могућих варијанти, Србија мора уложити додатна средства у обезбеђење своје енергетске сигурности, имајући у виду да енергетска несигурност највише кошта.

Кључне речи: логистика, нафта и нафтни деривати, нови нафтоводи, логистичка решења.

Увод

Транспорт сирове нафте у Републици Србији обавља се првенствено цевоводним путем уз одређену могућност снабдевања железничким, бродским и друмским видом транспорта. До рафинерије највећи део сирове нафте се допрема цевоводним, а значајно је мањи обим допреме сирове нафте друмским, железничким и речним путем. Деривати се од рафинерије до терминалских постројења углавном превозе железничким и бродским транспортом, а до крајњих потрошача, друмским. Већина деривата на српском тржишту потиче из Рафинерије Панчево, док се део, који потиче из увоза, преко складишних терминала упућује до бензинских станица и корисника.

Сирова нафта

Једини давалац услуга цевоводног транспорта сирове нафте у Републици Србији јесте Транснафта АД Панчево. Делатност овог предузећа су транспорт нафте нафтоводима на целој територији Републике Србије. Када су нафтоводи у питању, расположиви капацитети за увоз сирове нафте нису у потпуности искоришћени, па се капацитет нафтовода, којим управља Транснафта, и који износи девет милиона тона годишње, тренутно користи око 30% (Министарство рударства и енергетике, 2021). С обзиром на то да Рафинерија Нови Сад више не ради, а за коју је био резервисан капацитет од три милиона тона годишње, капацитет правца ка Панчеву од шест милиона тона годишње искоришћен је нешто преко 50%. Не постоји могућност извоза и реверзибилног транспорта постојећим, а ни других нафтовода којима би се могао вршити увоз или извоз произведене домаће нафте путем цевоводног транспорта (Министарство рударства и енергетике, 2021).

На слици 1 дат је приказ регионалног система нафтовода. Јадрански нафтовод (ЈАНАФ) је нафтовод који полази од луке Омишаљ и на који се наставља систем Транснафте од српске границе.

Слика 1. Регионални систем нафтовода (извор: аутор)

Данас, алтернативу цевоводном увозу значајних количина сирове нафте представља увоз пловним објектима (баржама) Дунавом из Констанце или из правца Мађарске, али постоји више фактора који утичу на неефикасност таквог вида транспорта, због чега се при уобичајеним околностима не примењује или се врло ограничено примењује. Главни разлог је непостојање капацитета речне флоте која би у оптималном времену могла допремити неопходну количину сирове нафте према планским потребама прераде, а други је променљиви водостај Дунава који не омогућава да се капацитет баржи искористи у потпуности (Компаније, 2022).

Стање и носивост железничких колосека у Републици Србији представља ограничавајући фактор за значајну примену при увозу сирове нафте. Главни железнички правци који повезују Србију са Омишљем, Копром и Солуном имају међуосовинско оптерећење од 22,4 т. Остали не прелазе 16 т (Компаније, 2022).

Домаћа сирова нафта се допрема нафтоводима и ауто-цистернама са отпремних станица до Рафинерије Нови Сад, а затим се отпрема даље за Рафинерију Панчево. Нафта типа Велебит се због својих за транспорт лоших реолошких особина мора намешати са увозном или домаћом сировом нафтом ради побољшања реолошких особина и тек довођењем на услове прописане Правилима рада транспортног

система Транснафта транспортовати за Рафинерију Панчево (Министарство рударства и енергетике, 2021).

Технички гледано, постоји могућност транспорта сирове нафте произведене у земљи и пловним објектима са отпремних станица до рафинерије. Највеће отпремне станице НИС а.д. Нови Сад, Надрљан и Елемир поседују пристан и могућност отпреме сирове нафте баржама, али се такав вид транспорта у регуларном раду нафтовода не спроводи (Министарство рударства и енергетике, 2021).

Транспорт сирове нафте цистернама врши се само са домаћих нафтних поља (Турија, поља Јужног Баната и Стига), и то са сабирних станица које нису повезане цевоводима са отпремним станицама претходно поменутим. У питању су количине које не прелазе 22% укупно произведених у Србији, односно око 176.000 т годишње или 14.700 т месечно (Министарство рударства и енергетике, 2021).

Капацитети за увоз и извоз деривата нафте

На тржишту постоји значајан број лиценцираних компанија који деривате увозе железницом, ауто-цистернама, речним пловним објектима (речни танкери, барже и самохотке) у свом власништву или у закупу (Министарство рударства и енергетике, 2021).

Увоз деривата железницом у највећој мери се врши вагон-цистернама власништва НИС а.д. Нови Сад или *Standard Logistic*, док увоз пловним објектима, осим НИС а.д. Нови Сад, обавља неколико привредних субјеката са својом флотом као што су: Speed d.o.o, Naftachem d.o.o, Казук д.о.о, Лађар Купра, Rubicon Chiping, Dunav Oil Trans, Јудра д.о.о, Лађар Транспорт д.о.о, Еуро Гас Суботица, MB Gas Oil, Марио МилТранс д.о.о (Компаније, 2022).

НИС а.д. Нови Сад је модернизацијом рафинерије у Панчеву и постизањем квалитета деривата на европском нивоу смањио увоз, док су водећи увозници остали МОЛ, OMB и Лукоил (Министарство рударстава и енергетике, 2020).

Извоз деривата нафте претежно врши НИС а.д. Нови Сад, и то железничким транспортом вагон-цистернама, пловним објектима и друмским ауто-цистернама.

Могући правци снабдевања сировом нафтом и дериватима нафте

На слици 2 дат је преглед терминала и рафинерија преко којих се може снабдевати српско тржиште сировом нафтом и дериватима нафте (терминали су обележени симболом танкера, а рафинерије симболом реактора/колона).

Слика 2. Терминали и рафинерије преко којих се може снабдевати српско тржиште сировом нафтом и дериватима нафте (извор: аутор)

Луке из којих се Србија може снабдевати су: Солун (Лука Солун, 2022), Драч (Порто Романо) (Лука Порто Романо, 2022), Бар (Лука Бар, 2022), Плоче (Лука Плоче, 2022), Задар (Лука Задар, 2022), Ријека/Омишаљ (Лука Омишаљ, 2022), Копар (Лука Копар, 2022), Констанца (Лука Констанца, 2022) и Бургас (Лука Бургас, 2022). Постоје и неке мање као што су Турн Северин, Русе, Фиер и Рени (Енергетска заједница, 2021). Сировом нафтом се Србија може снабдевати из свих лука сем Копра, Задра и Плоча. Напомена: снабдевање нафтом преко Драча (Порто Романо) је могуће, али није у пракси рађено већи број година ни за потребе Албаније.

Деривати се у Србију могу увозити са „отвореног мора“ и рафинерија Швехарт, Сасхалмбата, Братислава, Ријека, Бургас и више румунских рафинерија.

Потребе српског тржишта

Према последњем извештају о маркирању горива од 29.03.2022. године у Србији је у марту конзумирано рекордних 288.426 т белих деривата нафте (дизел, бензин и ТНГ) или просечно дневно 9.614 т (слична бројка се добија када се саберу дневни извештаји о потрошњи које добија Министарство рударства и енергетике) (Министарство рударства и енергетике, 2022). Ови бројеви представљају вишегодишњи рекорд. Први следећи месец по величини потрошње јесте јул 2021. када је потрошено 263.340 т. За прорачун обавезних резерви се узима податак од 8.689 т на дан као релевантан (прорачун има сложену методологију и неће се шире образлагати). Уколико као базну усвојимо потрошњу за март 2022. године, Србија ће у 2022. години конзумирати 3.461.112 т белих деривата нафте или просечно **288.426 т** месечно. Овај последњи податак представља **максимум** потреба српског тржишта и узеће се као референтан за оцену довољности потребних логистичких капацитета у случају максималне тражње.

Према Енергетском билансу за 2019. (узет као референтни због веће потрошње) у Србију је увезено 2.346.332 т сирове нафте[2] (Министарство рударства и енргетике, 2020). Истовремено је произведено **850.469 т** домаће нафте, односно укупно је конзумирано 3.196.801 т сирове нафте. Просечно се увозило 195.527 т сирове нафте месечно 2019. године. Треба напоменути да, поред домаће прераде, српска нафтна привреда задовољава своје потребе мањим увозом деривата, али и извози одређене количине деривата. У 2019. години увезено је 77.250 т бензина и 673.911 т дизела, а извезено 111.289 т бензина и 250.040 т дизела. Укупно је деривата (плус мазут, ТНГ и сл.) за потребе српског тржишта нето увезено 507.872 т. Укупно је нето сирове нафте и деривата увезено 2.854.204 т или 237.850 т месечно. Податак о **203.348 т** увоза сирове нафте и **44.016 т** деривата узеће се као референтни за оцену довољности потребних логистичких капацитета у случају очекиване тражње (количине из 2019. године увећане 4%)[3]. Када урачунамо домаћу производњу нафте, добијемо да је за задовољење прогнозираних потреба српског тржишта потребно укупно **3.871.657 т** еквивалента сирове нафте годишње или **322.638 т** месечно, или као што је већ речено – **3.461.112 т** белих деривата нафте или просечно **288.426 т** месечно. С обзиром на то да постоји домаћа производња сирове нафте, ове бројке се могу умањити за величину домаће

[2] Потрошњу из 2019. године треба увећати за 4% да би се добили подаци за 2021. годину, на основу извештаја о маркирању од 28.03.2022. године. Подаци из 2019. са претходном корекцијом се могу узети као релевантни за 2022. годину.

[3] *Напомена:* Нису узете у обзир карактеристике разних врста сирове нафте, нити различити могући режими рада рафинерије којима се добијају различите количине појединих деривата. У податак о **247.364 т** урачунате су потребе за мазутом, путним битуменом и другим дериватима нафте.

производње од **850.469 т** сирове нафте годишње или око **770.000 т** деривата који би се из ње добили.

Уколико би дошло до прекида снабдевања путем нафтовода ЈАНАФ из правца Омишља, Србија би се морала оријентисати на алтернативне начине увоза сирове нафте и деривата нафте.

Процена потребних логистичких капацитета за увоз нафте и деривата нафте

Према прикупљеним подацима од Министарства надлежног за послове саобраћаја, НИС-а и анкетирањем компанија дошло се до следећих података приказаних у табели 1[4] (Компаније, 2022). За прорачунски период је узет један месец. Претпостављено је да се сирова нафта транспортује у Рафинерију Панчево, а деривати на складишта лиценцираних енергетских субјеката. Резултати унети у табелу су просечне вредности.

Доњи прорачун је дат за луке до којих воде пруге са међуосовинским оптерећењем од 22,4 т, или Омишаљ, Констанца и Солун. На осталим правцима треба рачунати са мањим теретима, нпр. од Плоча може 750 т по композицији.

Практично нема ограничења на Дунаву, јер капацитет за конвој на преводници на Ђердапу износи око 11.000 т, а реално нема толико баржи.

	Нафта			**Дизел и бензин**		
	Ауто-цистерне	Вагон-цистерне	Барже	Ауто-цистерне	Вагон-цистерне	Барже
Број	30 (мазутне)	24–48 (НИС, мазутне)	10*****	1000 (1304)****	255 (НИС)	22****
Претпостављени просечни капацитет*	20т	50т	1200т	20т	60т	1200т
Прорачунски месечни обрачунски капацитет за увоз **	6.000 т	12.000 т	30.000–60.000т ******	200.000 т	76.500 т	66.000–132.000т

Табела 1. Расположиви логистички капацитети у Србији (извор: аутор)

[4] Ове податке треба узети са одређеном резервом, јер део ових капацитета није оперативан или не одговара АДР, техничким или еколошким захтевима.

* Нема тачних података о капацитетима појединачних ауто и железничких резервоара (не води се адекватна евиденција), тако да се просек може само претпоставити на основу искуства. За барже је усвојен капацитет од 1.200 т колико се може превозити у случају када је нижи водостај (конзервативна претпоставка) на Дунаву и ако им просечни капацитет варира од 1.500 до 2.800 т.

** Претпоставља се да ауто-цистерни треба 3 дана за једну туру до неке од могућих лука и назад, вагон-цистернама-возовима 5–8 дана (усвојено за прорачун 6), а баржама 12 дана до Констанце и 6 дана до рафинерије Сасхаламбата у Мађарској (Компаније, 2022).

*** 1.304 цистерне су регистроване, али осим деривата нафте превозе и друге течне терете као нпр. киселине, отпад, оксидирајуће материје итд. Претходно је разлог умањења овог броја.

**** Подаци за Рубикон Шипинг, Лађар Купра, Казук, Нафтахем, Спид, Еурогас Суботица, добијени анкетирањем компанија (Компаније, 2022).

***** С обзиром на то да барже које транспортују нафту морају имати грејаче, број баржи је мањи.

****** НИС-ова процена је да то у данашњим условима није више од 12.000 т. Задржана је већа вредност у табели, јер се подразумевало да ће држава ангажовати све своје капацитете и употребити све могућности којима располаже (Компаније, 2022).

Треба констатовати да је за подухват коришћења свих расположивих ресурса за увоз потребно 1–3 месеца мобилизације капацитета, разраде рута, решавања комерцијалних питања, закључивања уговора, усклађивања планова транспорта, претовара и дотура и сл.

Рафинеријски капацитети за пријем и прераду

Данас се у Рафинерији Панчево прерађује од 9.000 до 12.000 т сирове нафте на дан. Минимална прерада сирове нафте у Рафинерији Панчево је 6.750 т дневно (условљено капацитетом постројења С-2100), тј. на месечном нивоу од приближно 209.000 т (назваћемо овај случај: кризна варијанта 1). У случају нужде, прерада може пасти на 3.200 т дневно (условљено капацитетом постројења С-100), тј. на месечном нивоу око 100.000 т (назваћемо овај случај: кризна варијанта 2). Уколико се догоди неки од последња два сценарија, секундарна рафинеријска постројења ће морати да раде сваки други или трећи месец, јер ће се у супротном рафинерија суочити са великим бројем унутрашњих логистичких проблема (нпр. складиштење полупроизвода, недовољни квалитет и сл.).

Потребне залихе увозне сирове нафте у Рафинерији Нови Сад[5] (НС) су на месечном нивоу од око 70.000 тона због мешања и транспорта домаће нафте (65.000 тона) до Рафинерије Панчево. Дакле, део увезене нафте би се довозио директно у Рафинерију Панчево, а део у Рафинерију НС.

За потребе рафинерије би се морало увести 35.000 т месечно (варијанта 2) да би се омогућио рад рафинерије на минимуму. Пожељан увоз би био 144.000 т (умањена или варијанта 1).

Логистичка – технолошка ограничења

Пријем сирове нафте у Рафинерији Панчево и Рафинерији Нови Сад речним транспортом је једна баржа дневно, тј. у идеалним условима око 3.000 тона дневно или 90.000 т месечно.

Капацитет пријема сирове нафте у Рафинерији Панчево железницом износи 500–1.000 тона дневно или до 30.000 т месечно. У Новом Саду тренутно није могућ пријем сирове нафте железницом.

Укупни максимални капацитети за пријем су 120.000 т (90.0000 т + 30.000 т).

Као што је већ речено, за потребе рафинерије морало би се увести најмање 35.000 т месечно да би се омогућио рад рафинерије на минимуму, а пожељан увоз би био најмање 144.000 т. Истовремено, максимални пријемни капацитети (без нафтовода) нису већи од 120.000 т. Количина од 35.000 т месечно би се могла увести постојећим логистичким капацитетима (видети табелу 1), док увоз од 144.000 т није могућ како са становишта увоза, тако ни са становишта пријема у рафинерији. Последње значи да, уколико се затвори ЈАНАФ, могућ је рад рафинерије само у варијанти 2, која значи дисконтинуирани режим. Рад у варијанти 1 је могућ, али у дисконтинуираном режиму. Претходно указује на то да би, уколико се прекине снабдевање ЈАНАФ-ом, рад рафинерије био могућ само у дисконтинуираном режиму, односно у једном од два кризна.

Према анкети која је спроведена (Компаније, 2022), трошкови алтернативног транспорта нафте би у односу на снабдевање нафтоводом знатно порасли. Тренутни трошкови нафтоводом из Омишља до Сотина су 15,20 УСД/т (Компаније, 2022). Трошкови транспорта баржама су: Констанца–Панчево 33 ЕУР/т, а Констанца–НС 35 ЕУР/т. Цена транспорта железницом би била приближно 48 ЕУР/т (у зависности од низа фактора, спот/дугорочни уговор, услови испоруке итд.).

[5] Демонтирана, данас у функцији складишта-терминала за нафту и деривате.

Преглед логистичких могућности лучких нафтних терминала за снабдевање српског тржишта

Поред сагледавања потреба тржишта и „унутрашње-логистичких“ капацитета и ограничења везаних за транспортне капацитете и рафинеријска постројења, потребно је размотрити и могућности лучких терминала (лука) у окружењу, одакле би се Србија потенцијално могла снабдевати нафтом и нафтним дериватима. У табели 2 дате су основне карактеристике терминала који се могу користити за снабдевање Србије.

Терминал	Капацитет складишта нафте и деривата	Максимална тонажа брода који може да пристане	Годишњи капацитет претовара	Деривати	Нафта	Пут	Пруга	Река
Солун*	1.200.000 т	Више од 300.000 т	до 8 мнт нафте и деривата	Да	Да	Да	Да	Не
Драч	400.000 м^3	до 35.000 т	до 1,2 мнт укупног терета	Да	Да	Да	Не	Не
Бар	116.000 м^3	до 180.000 т	до 1 мнт укупног терета	Да	Да	Да	Да	Не
Плоче	50.000 м^3	до 25.000 т	0,8 мнт течних терета, до 5 мнт укупно	Да	Не	Да	Да	Не
Задар	60.000 м^3	до 40.000 т	до 0,2 мнт деривата	Да	Не	Да	Да	Не
Омишаљ	1.400.000 м^3 нафта и 80.000 м^3 деривати	Више од 300.000 т	Нема ограничења	Да	Да	Да	Да	Не
Копар	480.000 м^3	Више од 200.000 т	25 мнт укупно	Да	Не	Да	Да	Не
Констанца	1.700.000 м^3	до 165.000 т	67,5 мнт укупног терета, до 12 мнт нафте и деривата	Да	Да	Да	Да	Да
Бургас**	490.000 м^3	до 117.000 т	50 мнт укупног терета, до 10,5 мнт нафте и деривата	Да	Да	Да	Да	Да

Табела 2. Карактеристике нафтних терминала (лука) погодних за снабдевање Србије (извор: аутор)

* Постоји нафтовод капацитета 2,5 мнт годишње до Скопља. Постоји могућност да се нафтовод преради у продуктовод.

** Постоји продуктовод до Софије којим се могу допремати дизел и бензин (по потреби). Капацитет продуктовода је релативно мали, око 50.000 т годишње. Под могућношћу речног транспорта подразумевају се бродови који из Црног мора могу прећи у Дунав или веза преко луке Русе на Дунаву (Transconsult MP Ltd., 2014).

Из претходне табеле се види да се сви терминали могу користити за снабдевање Србије дериватима нафте. Нафтом се Србија не може снабдевати преко Плоча, Задра и Копра. Свима је могуће приступити друмским саобраћајем. Барже могу да се користе на Дунаву и до Бургаса. У терминале Драч, Плоче и Задар могу да уплове само мањи танкери (25–40.000 т) (Ministarstvo mora, prometa i infrastrukture Republike Hrvatske, 2022), (Лука Задар, 2022), (Лука Порто Романо, 2022). Терминал Драч то чини непогодним за снабдевање са Блиског истока одакле плове већи танкери са сировом нафтом од наведене тонаже. Пруга Драч–Скадар не функционише, што овај терминал чини најлошијим са становишта снабдевања.

Као повољни са становишта снабдевања нафтом и дериватима нафте могли би се оценити Солун, Констанца и Омишаљ. Мање повољни су Бургас, Бар и Копар. Остали представљају луке које би се могле користити само у нужди.

Уколико је потребно снабдевање сировом нафтом у количинама наведеним за варијанту 1 и 2, то данас није могуће учинити без речног транспорта, а то издваја Констанцу и евентуално Бургас као једне терминале.

Према прелиминарним доступним информацијама, у луци Констанца може да се обезбеди 40.000–80.000 тона сирове нафте (РЕБ, СРС, Азери, Киркук) месечно (Port Constantia, 2022).

Постојећи капацитети који би се могли искористити за обезбеђење сигурности снабдевања српског тржишта

У окружењу постоји неколико складишних терминала који би се могли искористити за складиштење резерви нафте или деривата за потребе српског тржишта. Попуњавање ових складишта могло би донети додатну сигурност српском тржишту. Ово је могуће не само путем комерцијалних аранжмана већ и путем примене Директиве Европске уније (European Union, 2009), којом је предвиђена сарадња на плану обезбеђивања „обавезних резерви“ нафте и деривата. У случају Србије, на располагању је неколико капацитета:

Рафинерија Босански брод је имала експлозију 2018. године на Хидрокрекеру и од тада не ради. Има 530.000 м^3 складишних капацитета, од чега 160.000 м^3 за нафту (Рафинерија Босански брод, 2022). Нафта би могла да се допрема нафтоводом, складишти и камионима допрема у Србију.

Окта Скопље има капацитете за нафту од 150.000 тона (Hellenik Petroleum, 2022). Ова рафинерија је нафтоводом (у власништву Хеленик петролеума) повезана са Солуном. План је да се нафтовод претвори у продуктовод. До Скопља би нафта могла да се допрема и возом и камионима. Два маршрутна воза би дневно могли да буду допремљени из Солуна или 2.000 т.

Нафтни терминал Омишаљ. Укупни капацитет је 1.400.000 т нафте и 80.000 т за нафтне деривате (ЈАНАФ, 2022).

Лука Бар има капацитет складиштења нафтних деривата од 116.000 м^3 (Лука Бар АД, 2022). Да би се деривати допремили до Србије, морала би се пруга Београд–Бар ставити у пуну функцију.

Нови правци снабдевања

Догађаји у Украјини и санкције које је Европска унија увела на трговину и транспорт руске нафте и деривата наводе на размишљања о новим правцима снабдевања српског тржишта. Логика је једноставна и састоји се у чињеници да са бројем могућих праваца снабдевања расте број могућих снабдевача, а са њим сигурност снабдевања. Растом броја снабдевача, појачава се тржишна утакмица и пада цена. Ову логику Европска унија примењује већ дуже време у домену снабдевања природним гасом и електричном енергијом. За земље које немају сопствене морске луке (*land locked*) важи исто правило. То је посебно дошло до изражаја када су уведене санкције на транспорт руске нафте за треће земље тзв. Шестим пакетом санкција, а које нису дерогиране тзв. Седмим пакетом санкција (European Union, 2022), које финасијски погађају Србију.

У српској јавности појавиле су се неке варијанте могућих решења (Новости, 2022), приказане на слици 3. Слика објављена у наведеном извору послужила је као основа за елаборацију могућих решења у овом раду, па је с тим у вези дорађена. У наведеном извору приказана су три могућа решења. Зеленом пуном линијом је приказан могући нафтовод до мађарских нафтних поља у околини Сегедина. Одатле до Дружбе, односно мађарске рафинерије Сасхаламабата (видети слику 1), већ постоји нафтовод капацитета око 1,2 милиона тона годишње (обележен плавом линијом и бројем 1). Када би се од Сегедина до Новог Сада изградио нафтовод капацитета 2,4 милиона тона, онда би реверсним током из Дружбе до Сегедина могло да дође око 1,2 милиона тона нафте, а потом би се ту придодало још 1,2 милиона тона мађарске нафте, тако да би до Новог Сада дошло 2,4 милиона тона. Ово подразумева дугорочни „SWOP" тј. аранжман замене између руских и мађарских компанија којим би Мађари добили 1,2 милиона тона више руске нафте да би своје количине уступили за Рафинерију Панчево.

Слика 3. Могући будући нафтоводи (извор: Новости, 2022. и аутор)

Дужа и скупља, али зато већег капацитета, могла би бити варијанта да се изгради нафтовод Нови Сад – Будимпешта. Он би се директно конектовао на нафтовод Дружба (приказан црвеном испрекиданом линијом).Тамноплавом испрекиданом линијом је приказан нафтовод Панчево – Скопље – Драч. Овај нафтовод би „заобилазио“ територију Европске уније и не би формално био подложан евентуалним санкцијама. Проблем са овим нафтоводом јесте тај што би био веома скуп, имајући у виду дужину, као и да би требало проширивати капацитете луке Драч да би могла да прими веће бродове. Такође, морао би да савлада планине Кораб или Јабланица у Македонији које су висине од 2.200 до 2.700 метара надморске висине и планинске ланце у Албанији који нису испод 2.200 метара надморске висине. Први релативно нижи прелаз из Македоније у Албанију јесте у висини Охридског језера, што би продужило ову трасу у некој сличној варијанти.

Чини се да је повољније повезати нафтовод од Панчева до Скопља на постојећи нафтовод до Солуна капацитета 2,5 милиона тона годишње. Тиме би се остварило значајно јефтиније решење (плава линија на карти обележена бројем 2) и веза са великом и развијеном луком у којој је Србија раније имала своју слободну зону.

На правцу ка Црном мору од раније су разматране две варијанте нафтовода: ПЕОП (Паневропски нафтовод) од Констанце, преко Србије и Хрватске до Трста, капацитета око 50 милиона тона годишње, и краћа и мања варијанта од Питештија до Панчева дужине око 170 км капацитета око 10 милиона тона годишње (Петар Станојевић, 2017). Обе варијанте су биле намењене скраћивању пута за руску и казашку нафту до европских тржишта, заобилажењем уског грла у Босфору и Дарданелима.

Поред повећања сигурности снабдевања нафтом, ови нафтоводи би могли да се искористе на више начина. Нафтовод Панчево – Скопље пролази поред Алексинца у којем су највеће српске резерве нафтних шкриљаца, што би омогућило да се „уље“ добијено из шкриљаца транспортује на најјефтинији начин до Рафинерије у Панчеву (500–800.000 т годишње), што би домаћу производњу сирове нафте повећало готово за 80–100%. Трасе нафтовода би се могле искористити да се поред њих изграде продуктоводи којим би се производи српске рафинерије (или рафинерија у будућности) могли извозити на околна тржишта или „отворено море“. Слично би се могло урадити и са интерконективним гасоводом између Србије и Северне Македоније.

Поред наведених варијанти требало би размотрити и унапређења на пругама Београд–Бар и Београд–Скопље–Солун, јер ако би тим пругама могло проћи дневно 10 композиција са по 1.000 т нафте, нафтоводи не би били потребни. Истина, трошкови транспорта би били већи.

Закључак

Логистика нафте и снабдевање нафтним дериватима у Србији имају уско грло у нафтоводу ЈАНАФ. У случају прекида снабдевања ЈАНАФ-ом рафинерија би радила у дисконтинуираном режиму, односно сваки други или трећи месец, и имала би значајно повећане трошкове прераде.

Други капацитети за увоз сирове нафте омогућавају увоз од 48.000 до 78.000 т месечно (табела 1), односно могли би да задовоље само минимум потребан за континуиран рад рафинерије (кризна варијанта 2).

Србија би могла да обезбеди увоз деривата расположивим логистичким капацитетима (подразумева се ангажовање готово свих постојећих транспортних капацитета), односно капацитет је преко 330.000 т, а потребе су око 214.000 т месечно (видети табелу 1).

Уколико се прекид снабдевања ЈАНАФ-ом догоди, за подухват коришћења свих расположивих ресурса за увоз потребно је 1–3 месеца мобилизације капацитета, разраде рута, решавања комерцијалних питања, закључивања уговора, усклађивања планова транспорта, претовара и дотура и сл. У прва три месеца се мора рачунати на 60% од потребних количина док се „руте не уходају“ и не реше проблеми. Треба напоменути да је током 2019. године НИС употребом свих расположивих ресурса за пет месеци успео да увезе само додатних 180.000 т деривата.

Додатни ограничавајући фактор ће бити расположивост робе на терминалима и у рафинеријама, као и број и квалитет расположивих логистичких капацитета.

Као повољне са становишта снабдевања нафтом и дериватима нафте могле би се оценити луке Солун, Констанца и Омишаљ. Мање повољне су Бургас, Бар и Копар. Остали терминали представљају луке које би се могле користити само у нужди. Сем Бара и Драча (који је најмање повољан од свих), сви остали терминали припадају земљама ЕУ и на њих се директно односе прописи ЕУ о санкцијама према РФ.

Потребне количине сирове нафте се не могу обезбедити без Јадранског нафтовода, сем за апсолутни минимум производње.

Уколико дође до прекида снабдевања нафтом путем ЈАНАФ-а, цене нафтних деривата ће се повећати због повећаних трошкова прераде, логистике и трговачких премија у условима снабдевања алтернативним правцима**.**

Србија мора размотрити алтернативне правце снабдевања као што су нафтоводи у правцу Мађарске, Румуније, Македоније, Грчке и Албаније. Могућа решења су и у унапређењу пруга Београд–Бар и Београд–Солун, које би биле знатно веће пропусне могућности уз куповину одговарајућих капацитета у локомотивама и вагон-цистернама. Слично би се могло урадити кроз куповину „резервне“ флоте баржи којима би се нафта и деривати могли транспортовати у кризним ситуацијама. Потребна су и улагања у складишни простор за нафту и деривате, али се њима само ограничено време превазилазе потенцијални проблеми.

У свакој од могућих варијанти, Србија мора уложити додатна средства у обезбеђење своје енергетске сигурности, имајући у виду да енергетска несигурност највише кошта.

Библиографија

1. Енергетска заједница. (2021). *Report_Oil_Dimension*. Беч. Accessed 2 October 2022 https://energycommunity.org/dam/jcr:4de4cc54700a4fe88db4dd43df94d0c0/PHLG122009_Report_Oil_Dimension.PDF

2. European Union. (2009). *Emergency oil stocks Directive 2009/119/EC*. Accessed 30 October 2022 https://energy.ec.europa.eu/topics/energysecurity/euoilstocks_en#:~:text=Under%20the%20EU%27s%20Oil%20Stocks%20Directive%20%282009%2F119%2FEC%29%3A%20EU,allocated%20quickly%20to%20where%20they%20are%20most%20needed
3. European Union. (2022). Accessed 30 October 2022 *https://eu-solidarity-ukraine.ec.europa.eu/eu-sanctions-against-russia-following-invasion-ukraine_en*.
4. ЈАНАФ. (2022). Accessed 25 October 2022 *https://janaf.hr/sustav-janafa/terminali/terminal-omisalj*.
5. Компаније, Н. (2022, март 15). Капацитети речног, друмског и железничког транспорта (М. р. енергетике, Новинар).
6. Лука Бар. (2022.). Accessed 24 October 2022 Преузето са https://lukabar.me/me/kapaciteti-i-usluge/.
7. Лука Бар АД. (2022). *Kapaciteti i usluge – Luka Bar AD / JSC Port of Bar*.
8. Лука Бургас. (2022). Accessed 26 October 2022*https://www.portseurope.com/port-of-burgas-cargo-volumes-rise-to-pre-pandemic-levels/*.
9. Лука Задар. (2022). Accessed 27 October 2022a https://www.luka-zadar.hr/.
10. Лука Констанца. (2022). Accessed 26 October 2022*https://www.portofconstantza.com/pn/en/home*.
11. Лука Копар. (2022). Accessed 26 October 2022*Terminal Instalacija Sermin (gov.si)*.
12. Лука Омишаљ. (2022). Accessed 26 October 2022*Terminal Omišalj - JANAF, d.d.*
13. Лука Плоче. (2022). Accessed 26 October 2022Преузето са https://www.luka-ploce.hr/.
14. Лука Порто Романо. (2022). Accessed 26 October 2022*https://portimbm.al/port-zone-about-us/*.
15. Лука Солун (2022). *Port of Thessaloniki (dogedaos.com)*.
16. Министарство рударстава и енергетике. (2020). *Енергетски биланс за 2020. годину.* Београд: Министарство рударства и енергетике.
17. Министарство рударства и енергетике. (2022). *Извештај о маркирању горива од 29.03.2022. г.* Београд: Министарство рударства и енергетике.
18. Министарство рударства и енргетике. (2020). *Енергетски биланс за 2019. годину.* Београд: Министарство рударства и енергетике.
19. Миностарство рударства и енергетике. (2021). *Извештај о сигурности снабдевања.* Београд: Министарство рударства и енергетике.
20. Ministarstvo mora, prometa i infrastrukture Republike Hrvatske. (2022). *Luka Ploče.* Преузето са Ministarstvo mora, prometa i infrastrukture Republike Hrvatske – Luka Ploče (gov.hr)
21. Новости (2022, October 10). DO NAFTE PREKO MAĐARSKE I DRAČA: Povezivanjem na Družbu. *Новости*.

22. Port Constantia. (2022). Accessed 26 October 2022 *https://portbusiness.ro/en/membri/oil-terminal-s-a/*.
23. Рафинерија Босански брод. (2022). Accessed 21 October 2022*https://rafinerija.com/?lang=sr-Cyrl-RS*.
24. Станојевић, П., Мишковић, В. и Мишев, Г. (2017). *Национална логистика и безбедност (National Logistics and Security)*. Београд: Факултет Безбедности. doi: ISBN 978-86-80144-17-7
25. Transconsult MP Ltd. (2014). *FEASIBILITY STUDY FOR THE PORT OF BURGAS*. Accessed 20 October 2022 https://pdf4pro.com/cdn/feasibility-study-for-the-port-of-burgas-176797.pdf
26. Hellenik Petroleum. (2022). Accessed 21 October 2022 *https://www.helpe.gr/en/the-group/where-we-are-active-abroad/okta-crude-oil-refinery-ad/*.

LOGISTICS OF OIL AND OIL DERIVATIVES IN SERBIA

Abstract

The logistics of oil and oil products in Serbia is presented from several aspects in this paper. The logistics of crude oil and oil products is described and the capacities for importing crude oil and oil products are analyzed. An overview and analysis of the possibilities of port oil terminals for supplying the Serbian market was performed. An analysis of the needs of the Serbian market for oil and oil products was carried out and an assessment of the necessary logistics capacities for the import of oil and oil products by various modes of transport was carried out. Refinery capacities for receiving and processing were analyzed in particular as a limiting logistical factor. Special attention was given to existing capacities that could be used to ensure security of supply to the Serbian market and to possible new supply routes that include new oil pipelines, revitalization of railways and rolling stock, as well as an increase in the Danube tanker fleet.

The assumption that oil logistics and the supply of oil products in Serbia have a bottleneck in the Adriatic pipeline has been confirmed. Other capacities for the import of crude oil could only meet the minimum required for the discontinuous operation of the refinery. Capacities for importing oil products are sufficient, if they could be procured and transferred to the considered ports. The ports of Thessaloniki, Constanta and Omišalj could be rated as favorable from the point of view of supply. Burgas, Bar and Kopar are less favorable. Other terminals represent ports that could only be used in an emergency.

It was concluded that Serbia must consider alternative supply routes such as oil pipelines in the direction of Hungary, Romania, Macedonia, Greece and Albania. Possible solutions are in the improvement of the Belgrade-Bar and Belgrade-Thessaloniki railways, which would have significantly greater capacity, coupled with the purchase of appropriate capacities in locomotives and tank wagons. The same could be done through the purchase of a "reserve" fleet of barges that could be used to transport oil and oil products in crisis situations. Investments in storage capacities for oil and oil products are also needed. In each of the possible variants, Serbia must invest additional funds in ensuring its energy security, bearing in mind that energy insecurity costs the most.

Keywords: logistics, oil and oil derivatives, new oil pipelines, logistics solutions.

МАШИНСКО УЧЕЊЕ И САЈБЕР БЕЗБЕДНОСТ

Ана Ковачевић[1]

Апстракт

Сајбер напади су у експанзији, повећава се њихов број, софистицираност, суровост и губитак прихода од сајбер напада. Значајни фактори за губитак прихода су злонамерни програми, напади засновани на вебу (*веб*), напади одбијања услуга, злонамерни инсајдер, социјални инжењеринг и др. Недостатак кадрова у области сајбер безбедности евидентан је већ више година, а са порастом броја напада, њиховом софистицираношћу и суровошћу тај проблем постаје и израженији. Једна од могућности превазилажења недостатка кадрова јесте коришћење вештачке интелигенције, односно машинског учења у контроли сајбер безбедности. Машинско учење се показало добрим за анализу велике количине података и уочавање патерна (шаблона) који раније нису били познати, ни очигледни, а могу бити корисни. Машинско учење се односи на способност софтверског система да генерализује на основу претходног искуства, при чему се под искуством сматра скуп података о појавама/ентитетима који су предмет учења, а генерализација се примењује на појаве/ентитете које раније нису биле познате. Машинско учење се користи у откривању сајбер напада, као и за блокирање нападача. Међутим, машинско учење би могло да се користи и приликом напада на циљани систем, за анализирање инфилтрирања у систем жртве, откривање софтверских рањивости у систему. Поред тога, код напада на моделе машинског учења, односно код супарничког учења (*adversarial learning*)

[1] Факултет безбедности, Универзитета у Београду, Београд, e-mail: kana@fb.bg.ac.rs
Рад је настао у оквиру пројекта Фонда за науку Републике Србије „Идеје“ – Пројекат акцелерације иновација и подстицања раста предузетништва у Републици Србији – Management of New Security Risks – Research and Simulation Development – NEWSIMR&D, #7749151

испитују се слабости самих система машинског учења и података који од њих зависе.

У раду ће бити анализиране могућности примене машинског учења на сајбер безбедност. Да ли ће машинско учење убрзати сајбер нападе или помоћи у решавању? Да ли се поред предности коришћења машинског учења у обради велике количине података уносе неки нови ризици у сајбер простор? Да ли злонамерни корисници уз примену машинског учења могу да креирају још суровије и софистицираније нападе? Да ли машинско учење додаје комплексност традиционалном вектору напада, повећавајући ризик сајбер операција без потпуног разумевања начина рада и потенцијалних ефеката? Разумевање могућности и ограничења машинског учења есенцијално је за спречавање његовог погрешног коришћења.

Кључне речи: сајбер напади, вештачка интелигенција, супарничко учење, злонамерни програм, фишинг, обрада природног језика.

Увод

Сајбер напади свакодневно постају суровији, софистицираније и бројнији. Институт Понемон (*Ponemon Institut)* процењује да економске последице сајбер напада износе око пола трилиона долара годишње, при чему број, као и вредност напада, константно расте (Ponemon, 2017). Константан тренд пораста сајбер напада евидентан је и према истраживању где је уочен пораст од 11% у односу на претходну годину, док пораст броја напада у последњих пет година износи 67% (Accenture, 2017). Са појавом пандемије и свеприсутношћу рачунара проблем безбедности у сајбер простору још је значајнији. Сајбер безбедност је дисциплина заснована на рачунарству која укључује технологију, људе, информације и процесе да омогући безбедне операције у контексту противника (Cybersecurity Curricula, 2017). С друге стране, сајбер напади често остају дуже времена неоткривени, као што је био на пример напад на хотелски резервациони систем Старвуд (*Starwood*): подаци су цурели из ланца хотела Мериот (*Marriot*) од 2014. године, а напад је тек четири године касније откривен и било је угрожено преко 500 милиона гостију (Sobers, 2020). Ово није усамљени случај и према истраживању IBM-а (*International Business Machines*) просечно време потребно за откривање напада крађе података било је најдуже у индустрији забаве (287 дана), потом здравствене заштите (255 дана), медија (225 дана), образовања (208 дана) (Sobers, 2020).

Према извештају које је спровео *Oracle&KPMG* (2019) 53% испитаних организација је навело да су у области сајбер безбедности имали проблематичан недостатак вештина. Слично показује и истраживање Ацентуре где је само 16% испитаника, који су шефови службе за информациону безбедност (CISO – *Chief*

Information Security Officer), изјавило да су њихови запослени довољно одговорни да се изборе са изазовима сајбер безбедности (Accenture, 2017). Поред тога, према истом истраживању 79% пословних лидера сматра да нови бизнис модели уносе технолошке рањивости брже него што могу да се заштите (Accenture, 2017).

Порастом броја уређаја који су повезани на интернет (процена је да данас има преко двадесет милијарди повезаних уређаја) проблем безбедности у сајбер простору постаје још израженији због бројних рањивости IoT (*Internet-of-things*) уређаја. Истраживање које је спровео HP (*Hewlett Packard*) показује да има двадесет пет рањивости по уређају (80% уређаја није захтевало лозинку довољне комплексности и дужине, 70% није енкриптовало локалну и удаљену комуникацију, а 60% је имало рањиви кориснички интерфејс) (Kobialka, 2014).

Проблем недостатка кадрова у области сајбер безбедности, као и самог броја напада и њихове софистицираности, утицао је да као један од могућих начина превазилажења тог проблема буде примена вештачке интелигенције, односно машинског учења у откривању и блокирању сајбер напада. Међутим, треба размотрити могућност да ли машинско учење може да се примени и на откривање рањивости у систему, или за креирање нових типова злонамерних програма и/или уноси нове ризике у сајбер простор.

Вештачка интелигенција

Не постоји јединствена дефиниција вештачке интелигенције. Марвин Мински (*Marvin Minsky*), један од пионира вештачке интелигенције, дефинисао је вештачку интелигенцију као науку чињења где машине раде ствари које би захтевале интелигенцију уколико би их радио човек (Мински, 1968). Алан Тјуринг (*Alan Turing*) (1950) је поставио питање „Да ли машина може да мисли?“. Креирао је тест (касније познат као Тјурингов тест) где човек испитивач покушава да погоди да ли на његова питања одговара машина или човек. Уколико машина обмане човека и он помисли да је одговорио човек, тест је успешан, односно потврдан је одговор на почетно питање.

Вештачка интелигенција омогућава компјутерима и машинама да опонашају перцепцију, учење, решавање проблема и могућност одлучивања људског ума – учењем из примера, искуства, препознавање објеката, разумевање и одговарање, доношење одлука, решавање проблема и комбиновањем ових и других могућности да би извели функције које човек обавља (IBM, 2020). Данашњем процвату вештачке интелигенције претходила је велика количина података у дигиталном облику, као и напредак рачунара (хардвера).

Подела вештачке интелигенције према типу јесте на слабу и јаку вештачку интелигенцију. Данас је заступљена слаба вештачка интелигенција (W*eak Artificial Inteligence*) која је специјализована, тј. обучена само за једну врсту

задатка, као што су на пример Еплова (*Apple*) *Siri*, IBM-ов Вотсон (*Watson*), самовозећи аутомобили и слично. Самовозећи ауто зна како да управља возилом, који су саобраћајни закони, како да избегне судар, како да се понаша када се деси нешто неочекивано – као на пример да излети пас на пут. Слаба вештачка интелигенција зна много и може да донесе одлуке на основу тог знања, али само у ограниченом домену (Schneier, 2021).

Јака вештачка интелигенција је дефинисана као теоријски концепт и састоји се од опште интелигенције и вештачке супер интелигенције. Вештачка општа интелигенција је једнака људској интелигенцији, док вештачка супер интелигенција је супериорна у односу на људску интелигенцију. Иако су и јака и супер вештачка интелигенција за сада теоријски концепти, њихова практична примена је декадама далеко. Бројна су истраживања у разним областима (рачунарских наука, социологије, филозофије) како да се креирају системи тако да не раде ствари које ми не желимо, као на пример уништавање човечанства (Schneier, 2021).

Подскуп вештачке интелигенције који је почео да се развија осамдесетих година прошлог века јесте машинско учење (*machine learning*). Машинско учење има могућност самосталног учења, а дубоко учење (*deep learning*) је подскуп машинског учења које се самостално обучава са великом тачношћу, без људске интервенције.

Машинско учење

Људи су се показали добри у уочавању патерна и релација у подацима, али не могу да обраде велику количину података веома брзо и ефикасно. С друге стране, рачунари могу да обраде велику количину података брзо, али не знају како. Идеја је да се удружи ово двоје, односно да се људско знање комбинује са обрадом машина, тј. рачунари би могли да обрађују велику количину података самостално (или са минималном људском интервенцијом). Један од кључних разлога за примену машинског учења јесте прикупљање велике количине дигиталних података у разним областима: у медицини (о пацијентима и терапијама), у спорту (о утакмицама и игри појединих играча), у маркетингу (шта су корисници купили, како су оценили производе) и сл. Интелигентном анализом података откриће се патерни који нису били познати, ни очигледни, а могу бити корисни. Примена машинског учења је у бројним областима као што су: категоризација текстова према теми, осећањима, ставовима; машинско превођење текста, разумевање говорног језика, препознавање лица, сегментација тржишта, откривање упада у мрежу и друго.

Машинско учење се односи на способност софтверског система да генерализује на основу претходног искуства, при чему се под искуством сматра скуп података о појавама/ентитетима који су предмет учења. Користи се генерализација како би

се пружили одговори на питања која се тичу ентитета/појава са којима се систем раније није сретао. Према формалној дефиницији сматра се да компјутерски програм учи из искуства Е (*experience),* везаног за задатак Т (*task*) и меру перформанси П (*performance*), уколико се његове перформансе на задатку Т, мерене метрикама П, унапређују са искуством Е (Mitchell, 1997). На пример, ако бисмо посматрали програм који бинарно класификује електронску пошту и означава их као спам и не-спам, тада би задатак био класификација поште на оне које су спам или нису. Искуство је скуп електронске поште означених као спам и не-спам, док перформансе представљају проценат коректно класификоване поште.

Подела машинског учења према типу процеса одлучивања дели се на надгледано учење (*supervised learning*), ненадгледано учење (*unsupervised learning*) и учење уз подстицаје (*reinforced learning*).

Надгледано учење обухвата технике за решавање при чему програм за задати скуп улазних података има дефинисан скуп излазних вредности, односно задатак програма је да за нови необележени улазни податак додели излазну вредност. Уколико је излазна вредност номинална, примењује се класификација, а уколико је излазна вредност реалан број, тада се назива регресија. Пример надгледаног учења може бити пример бинарне класификације у филтрирању порука електронске поште (*email*), на поруке које су нежељена пошта (спам) или нису нежељена пошта. На основу постојећих (историјских) података где је дефинисано који су подаци нежељена пошта, а који нису, креира се модел. Уколико је модел задовољио тачност над тестним подацима, примењује се на класификацију нових података.

За разлику од надгледаног учење, где смо имали излазне податке, код ненадгледаног учење такви подаци не постоје, тј. не знамо жељену излазну вредност, односно програм добија само улазне податке. Задатак програма је да открије шаблоне (патерне), тј. скривене законитости у подацима. Један од примера ненадгледаног машинског учења јесте одређивање конфекцијских величина на основу висине/тежине људи, поделом људи у кластере, где су елементи једног кластера међусобно ближи него са елементима из других кластера. Пример ненадгледаног учења: банка хоће постојећим корисницима да уведе скуп нових финансијских производа базираних на профилима клијената. На основу својих карактеристика корисници се деле у групе, где су припадници једног кластера међусобно ближи него са припадницима других кластера. Свакој групи потом уводи се један или више финансијских производа најпогоднијих за карактеристике целокупног профила групе.

Код учења уз подстицај програм (агент) делује на окружење – извршавањем низа акција утиче на окружење, а оне повратно утичу на агента пружајући му повратне

информације које могу бити награда или казна. Циљ агента је да делује у датом окружењу са максималним наградама (или минималним казнама), што се примењује код компјутерских игара и аутономних возила.

Откривање вредности ван опсега, односно аутлајера (*outliera*), техника је машинског учења која се користи да идентификује аномалије, необичности и девијације које некада могу бити корисне приликом истраживања података. Детектовање аутлајера представља процес налажења података који је значајно различит или неконзистентан са осталим подацима у оквиру постојећег скупа. Откривање аутлајера је врло значајно за откривање превара, анализу мрежних података или анализу података са сензора.

Треба узети у обзир да рачунари не размишљају као људи: рачунари ће анализирати више могућих решења него ми, комплекснија решења или разматраће више типова решења о којима људи и не размишљају (Schneier, 2021). Програм вештачке интелигенције Алфаго (*AplhaGo*) победио је једног од најбољих играча гоа, што је било велико изненађење за заједницу вештачке интелигенције, као и за заједницу играча игре го. Најчувенији потез је био изузетно интересантан по томе што ниједан човек не би никада изабрао да га направи (Metz, 2016). Уз то, рачунари немају когнитивна ограничења која карактерише људе, тј. количина информација коју можемо симултано да обрађујемо магичан је број седам плус/минус два (Miller, 1956).

Рачунари су оптимизовани да буду оријентисани према циљу: робот који се користи за усисавање добијао је награду ако не удари у браник где се налази сензор, а пошто није постојао сензор са задње стране уређаја, робот је научио да иде уназад (@Smingleigh, 2018). Шнајер сматра да ће сваки добар систем вештачке интелигенције моћи да искористи недоследност или рупе у правилима, а да води до прихватљивог решења, што је дефинисано правилима (Schneier, 2021). Људи често подразумевају одређене ствари, па довољно добро не спецификују жеље и циљеве.

Треба имати на уму да се код модерних система машинског учења добија решење или одговор на постављано питање, али не и само појашњење процеса (одговора), чиме би се наше уверење у решење побољшало. Пример је програм Дип Пејшент (*Deep Patinet*) који има око 700.000 медицинских података и тестиран је да ли може да предвиди болести. Показало се да успешно може да предвиди психијатријске поремећаје, много пре лекара (Knight, 2017). Звучи изванредно, али Дип Пејшент не обезбеђује никакво објашњење за своју дијагнозу и истраживачи не знају како је дошао до решења. Доктор може да верује или игнорише рачунар, но не може да добије додатне информације. Поставља се питање колико можемо да будемо сигурни у процену система машинског учења. Уз то, да ли смо сигурни да није хакован, да су унесени лоши улазни подаци, па

је излаз нетачан (неадекватан)? Модерни системи машинског учења су у суштини црне кутије које дају резултат (излаз) за улазне податке. Немогуће је открити како је дошло до резултата, чак и проучавањем кода. Уколико дође до грешке у систему класификације, ми не знамо зашто зашто се то дешава (Schneier, 2021). Да би се добио бољи увид у системе машинског учења, DARPA (*Defense Advanced Research Project Agency*) 2017. године је уложила 75 милиона у истраживање у области појашњења процеса доношења одлуке система вештачке интелигенције и док постоји напредак у овом пољу, постоји компромис између могућности и објашњења функционисања sistema (Schneier, 2021; Gunning et al., 2019).

Машинско учење и сајбер безбедност

Машинско учење је ефикасно у обради велике количине информација, па би зато могло да се користи при откривању и блокирању упада у систем, као и при детектовању злонамерног кода. Међутим, машинско учење може да се примењује у нападу за откривање софтверских рањивости система и инфилтрирања у систем. Поред тога, треба имати на уму да примена машинског учења уводи неке нове рањивости у сајбер простор, као што су напади на моделе машинског учења, тј. супарничко учење (*adversarial learning*). Супарничко учење испитује слабости безбедности самих система машинског учења, као и података од којих зависе.

Примена машинског учења у откривању сајбер напада

Проблем откривања напада у сајбер простору јесте изражен и потребно је некад више месеци или година да би се детектовао напад (Sobers, 2020). Да ли би машинско учење могло да открије сајбер напад? Машинско учење може да побољша откривање сајбер напада, посебно са великом количином података која постоји у данашњим рачунарским системима.

Рањивост у програму представља основу за напад, а да ли би машинско учење могло да помогне у откривању рањивости у програму? Рањивости нултог дана постају кључни део напредних модерних сајбер операција, а применом метода машинског учења могли би да се побољшају резултати откривања нових рањивости.

Машинско учење би могло да се користи у првој фази откривања сајбер напада, а за напредније анализе би се користили људи. Поред откривања да ли би могло машинско учење да помогне у блокирању сајбер напада, односно ако машинско учење открије сајбер напад који се дешава у реалном времену, да ли може да га одложи или блокира – да ли ће онда машинско учење одговорити на адекватан начин? На пример: ненадгледано машинско учење (попут кластеризације) може да повеже делове кода и помогне у идентификовању група које могу да буду одговорне за нови напад.

По угледу на такмичење *Caputre the flag*[2] 2016. године DARPA је организовала такмичење *Grand Cyber Challenge* за аутоматизоване конкуренте где их је супротставила једне другима у домену сајбер безбедности (Song & Alives-Foss, 2016).

Идеја је била да се развије аутоматска одбрана система који би могао да открије, докаже и исправи рањивости софтвера у реалном времену. У почетку се такмичило 100 тимова, да би се, након завршених квалификованих рунди такмичења, седам финалиста такмичило у специјално дизајнираном тестном окружењу са прилагођеним софтвером који никад није био анализиран или тестиран. Такмичарима је било дозвољено да за десет сати нађу рањивости које би могли да искористе против других машина у такмичењу и да заштите себе од напада осталих. Победнички тим је од тада комерцијализовао технологију и она се, између осталог, примењује се у Министарству одбране Сједињених Америчких Држава (Simonite, 2020).

Системи машинског учења могу да буду посебно корисни у откривању рањивости. Комплексни системи су непријатељи безбедности, а новији оперативни системи имају милионе линија кода, и анализа таквог кода је изузетно временски захтевна и поприлично неинспиративна. Уколико би обучили системе машинског учења да препознају рањивост у софтверу, показало би се изузетно корисно да раде досадан/захтеван посао пролазећи хиљаде/милионе линија кода (Saavedra et al., 2019). Раде се интензивна истраживања у овој области и системи који користе машинско учење ће се побољшавати временом, пошто се побољшавају искуством и преко података за обучавање.

Примена машинског учења у сајбер нападу

Можемо да замислимо како би злонамерни корисник могао да искористи машинско учење за потребе социјалног инжењеринга, нпр. циљаног (персонализованог) фишинга (*spear phishing*). Фишинг мејл је порука од лажно представљеног пошиљаоца, са идејом да прималац уради нешто што не би требало у корист пошиљаоца. Уколико је фишинг порука генеричка, релативно је неефикасна и лако се открива. Међутим, много ефикаснији су персонализовани фишинг (*spear phishing*) мејлови где, на пример, злонамерни корисник који се лажно представља као директор тражи услуге од подређених у финансијском сектору, а још бољи ефекат се постиже коришћењем генерисане гласовне поруке (Affifi-Sabet, 2019).

[2] Такмичење *Caputure the Flag*, познато још од средине деведесетих, у основи је игра на отвореном (*outdoor game*) где тимови хакера бране сопствене рачунаре док нападају друге тимове.

Креирање персонализоване поруке је изузетно временски захтеван посао за човека: од налажења жртве, одређивање којој врсти поруке жртва може да верује, након тога креирања и слања поруке. Но, са напретком у обради природног језика, бројне су могућности примене машинског учења код циљаног фишинга (Radford et al., 2019). На тај начин би се омогућило креирање великог броја уверљивих порука у кратком временском периоду које избегавају аутоматско детектовање.

Такође, треба размотрити да ли машинско учење може да помогне у трансформацији злонамерних кодова. Шта би се десило ако би се модификовао злонамерни код попут стакснета (*Stuxnet*), који је напао нуклеарна постројења у Ирану? Да ли би напади били бржи, суровији или би их било теже открити? Да ли би машинско учење помогло у откривању багова у системима?

Напади на системе машинског учења

Намеће се питање колико је сам систем машинског учења рањив на сајбер нападе. Да ли се, поред рањивости које се појављују у традиционалним рачунарским системима, појављују и нове рањивости које омогућавају злонамерним корисницима смањивање ефикасности машинског учења у критичним моментима?

Колико је систем машинског учења безбедан насупрот покушајима обмане? Код машинског учења се често користи класификација за идентификовање категорије којој нешто припада, нпр. да ли је нешто спам или не, или код класификације слика. Неке преваре су интуитивне, док је друга врста превара везана за сам систем машинског учења – циљају на механизме како неутралне мреже обрађују информације и праве класификацију (што је различито од тога како људи обрађују информацију).

Промена од само неколико пиксела може утицати на класификацију слике, значајно мењајући резултате на начин да је скоро тотално непрепознатљива људском посматрачу (Goodfellow et al., 2014). Алкорт и др. су у свом раду приказали како променом само положаја објекта програм машинског учење даје погрешне резултате (Alcort et al., 2014). Систем за препознавање лица уз мали померај (шум) добија нетачне вредности (Li et al., 2019), или систем машинског учења не може да идентификује човека уколико је на његовој одећи лик човека (Wu et al., 2019).

Подаци за обуку су есенцијални код машинског учења и могућност напада остварује се променом улазних података, тј. „тровањем података“ (*data posioning*), чиме би се аутоматски променио и начин понашања. Ово представља посебну опасност за системе који се континуирано тренирају на корисничком упиту (Chen et al., 2017). Изменом улазних података током преноса података, као на пример при компјутеризованој томографији (*computerized tomography*), обманули би се и

машине и људи (Mirsky et al., 2019), што би представљао напад на интегритет података.

Да ли системи машинског учења могу да одају тајне информације? На пример, систем машинског учења је трениран на класификованим тајним подацима за задатак обавештајне анализе. Након тога је примењен у реалном, некласификованом окружењу у коме примењује овај задатак и анализира активности противника. Интеракцијом са моделом машинског учења, суптилном променом активности и применом технике познате како инверзија модела, противник може да утврди кључне карактеристике основних података на којима је систем обучен, у основи добијањем приступа поверљивим информацијама (Buchanan, 2020).

Алати за генерисање текста

Следећи проблем представља могућност алата за генерисање „кредибилног" текста, односно могућност генерисања реалних и уверљивих кампања са минимално напора коришћењем машинског учења. Сведоци смо бројних непоузданих информација, што је имало посебно значајно место у последњих пар година. Дезинформације хакују наше разумевање реалности (Schneier, 2021). Још 2019. године појавио се GPT-2 (*Generative Pretrained Transformer*) (фирме *Open AI*) алат за генерисање кредибилног текста са произвољним улазом (Radford et al., 2019). Коришћењем алата GPT-2 унета је иницијална реченица и посматрано је генерисање параграфа текста. Показано је да 72% корисника сматра да су „вести" генерисане са GPT-2 кредибилне (Kreps & McCain-a, 2020). Које су могућности овим отворене? Какве ће користи или последице бити по друштво? Уз помоћ рачунара могуће је да се појачају, ескалирају и обликују кампање.

Наследник програма GPT-2 је GPT-3 који има побољшане могућности за генерисање текста. У зависности од полазних података могуће је креирати истините приче или се оне могу хранити нетачним подацима и лажним вестима. Данас већ постоје програми који могу креирати персонализована писма редакцијама и изабраним званичницима, остављати интелигентне коментаре на новинским сајтовима и интелигентно расправљати о политици на социјалним медијима (Heaven, 2020). Са развојем обраде природног језика, ови системи ће постати бољи, софистицираније, и биће све компликованије открити да су машине.

У експерименту је генерисано хиљаду коментара помоћу програма за генерисање текста у одговору на владин захтев за постављање коментара за Медикаејд (*Medcaid*) систем (Weiss, 2019). Компјутерски генерисани коментари су изгледали различити, као да потичу од различитих људи, који заступају различите политичке позиције. Администратори *Medicaid.gov* нису посумњали да коментари потичу од машина.

Реалност је да програм вештачке интелигенције пише вести за новинске агенције попут Асосијејшн Прес (*Associtation Press*), где се у партнерству са Урбс Медијом (*Urbs Media*) аутоматски генерише око 30.000 локалних новинских прича сваког месеца (Marr, 2021).

Слика вреди више од хиљаду речи, а видео имао још већу тежину: помоћу дип фејк (*deep fake*) технологије креирају се уверљиви видеи лажних догађаја, где реални људи изговарају речи које нису никада изговорили, и може се само претпоставити какве су све могуће импликације (Sample, 2020).

Постоји „персона бот“ која шаље поруке на социјалним медијима, има историју, личност и стил комуникације попут праве особе, а с времена на време провуче неку пропагандну вест, при чему ће им системи попут GPT-3 олакшати да пронађу одговарајући интернет садржај, како би изгледали упућени у материју (Schneier, 2021). Једна персона бот неће имати утицаја на јавно мишљење, но какве ће последице бити ако хиљаде или милиони ботова буду слали оркестриране поруке?

Рачунарска пропаганда данас је свеприсутна и укорењена у наш свакодневни живот, а представља употребу алгоритама, аутоматизације, биг дејта (*big data*) за обликовање јавног мњења (Bradshaw and Howard, 2019). Према истраживањима Оксфордског интернет института (*Oxford Internet Institute*) из 2019. нађена је евиденција ботова за ширење пропаганде у педесет земаља (Bradshaw and Howard, 2019). Неограничене су могућности креирања дезинформација помоћу машинског учења, поготово што се тиче брзине креирања и могућности ширења.

Закључак

Број потенцијалних хакера расте, последице напада су веће, а напади по правилу злонамернији, при томе евидентан је недостатак кадрова у сајбер безбедности. Једно од могућих решења је и коришћење машинског учења за детекцију сајбер напада. Машинско учење може да има великих предности у откривању рањивости као и у блокирању сајбер напада. Но, изузетно је важно да се добро анализира примена машинског учења у било ком критичном окружењу, јер се појављују и неки нови ризици својствени машинском учењу. Машинско учење само по себи не прави већу штету него људи, али је у стању да то уради са компјутерском брзином и великим обимом који је незамислив људима.

Да ли ће нам машинско учење помоћи у откривању грешака у софтверу и детекцији и/или блокирању сајбер напада? Да ли ће нас системи машинског учење упозорити на лажне вести? Да ли ће машинско учење убрзати сајбер нападе или помоћи у њиховом решавању? Да ли ће применом машинског учења више користи имати нападачи или одбрана? Да ли су неке основне операције нападачке или одбрамбено доминантне? Разумевање могућности и ограничења машинског

учења есенцијално је за спречавање њиховог погрешног коришћења. Тренутно не знамо који је баланс између напада и одбране.

Оно што је данас евидентно јесте то да ће машинско учење додавати комплексност традиционалном вектору напада, подижући ризик од сајбер операција и трансформишући природу сајбер напада. Шнајер је причу о примени вештачке интелигенције упоредио са митом о краљу Миди, коме је бог Дионис испунио жељу тако да све што додирне претвори у злато (Schneier, 2021). Краљ Мида је завршио гладан и очајан када су његова храна, пиће и ћерка претворени у злато, јер је Мида погрешно програмирао свој циљ. Изузетно је важно да будемо свесни коришћења машинског учења.

Библиографија

1. Accenture. (2017). *Cost of cyber crime study*. *Accenture*. Accessed 20 October 2022 https://www.accenture.com/gb-en/insight-cost-of-cybercrime-2017.
2. Afifi-Sabet. (2019). *Fraudsters Use AI Voice Manipulation to Steal £200,000*. IT PRO, 2019. Приступљено 20.09.2022. https://www.itpro.co.uk/social-engineering/34308/fraudsters-use-ai-voice-manipulation-to-steal-200000.
3. Alcorn, M. A., Li, Q., Gong, Z., Wang, C., Mai, L., Ku, W. and Nguyen, A. (2019). *Strike (With) a Pose: Neural Networks Are Easily Fooled by Strange Poses of Familiar Objects*. *In 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 4840–49. Long Beach, CA, USA: IEEE, 2019. https://doi.org/10.1109/CVPR.2019.00498.
4. Bradshaw, S. and Howard, N P. (2019). *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, p. 27.
5. Buchanan, A. B. *A National Security Research Agenda for Cybersecurity and Artificial Intelligence CSET Issue Brief*, n.d.
6. Chen, X., Liu, C., Li, B., Lu, K. and Song, D. (2017). Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning. *ArXiv Preprint ArXiv:1712.05526*.
7. Goodfellow, I. J., Shlens, J. and Szegedy, C. (2014). Explaining and Harnessing Adversarial Examples. *ArXiv Preprint ArXiv:1412.657*.
8. Gunning, D., Stefik, M., Choi, J., Miller, T., Stumpf, S. and Yang, G. Z. (2019). XAI-Explainable Artificial Intelligence. *Science Robotics* 4 (37) (December 2019). https://doi.org/10.1126/scirobotics.aay7120.
9. Cybersecurity, C. (2017). *Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. New York, NY, USA: ACM. Accessed 24 October 2022 https://doi.org/10.1145/3422808.
10. Heaven, W. (2020). IBM's Debating AI Just Got a Lot Closer to Being a Useful Tool. *MIT Technology Review*. Accessed 26 October 2022. https://www.technologyreview.com/2020/01/21/276156/ibms-debating-ai-just-got-a-lot-closer-to-being-a-useful-tool/.

11. IBM. (2020). What Is Artificial Intelligence (AI)? | IBM. Accessed 21 October 2022 https://www.ibm.com/cloud/learn/what-is-artificial-intelligence.
12. Knight. (2017). The Dark Secret at the Heart of AI. *MIT Technology Review*, Accessed 21 October 2022 https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/.
13. Kobialka, D. (2014). HP: 70% of IoT Devices Vulnerable to Attack. *Channel Futures*, 5 August 2014. https://www.channelfutures.com/cloud-2/hp-70-of-iot-devices-vulnerable-to-attack.
14. Kreps, S. and McCain, M. (2022) Not Your Father's Bots. *Foreign Affairs*. Accessed 26 October 2022. https://www.foreignaffairs.com/print/node/1124547.
15. Li, Y., Yang, X., Wu, B. and Lyu, S. (2019). Hiding Faces in Plain Sight: Disrupting Ai Face Synthesis with Adversarial Perturbations. *ArXiv Preprint ArXiv:1906.09288*, 2019.
16. Marr, B. (2019). Artificial Intelligence Can Now Write Amazing Content – What Does That Mean For Humans? *Forbes*. Accessed 26 October 2022. https://www.forbes.com/sites/bernardmarr/2019/03/29/artificial-intelligence-can-now-write-amazing-content-what-does-that-mean-for-humans/.
17. Marvin, L. M. (1968). Semantic Information Processing. *The MIT Press*, n. d.
18. Metz. (2016). „n Two Moves, AlphaGo and Lee Sedol Redefined the Future | WIRED. Accessed 26 October 2022. https://www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future/.
19. Miller, G. A. (1956). THE PSYCHOLOGICAL REVIEW THE MAGICAL NUMBER SEVEN, PLUS OR MINUS TWO: SOME LIMITS ON OUR CAPACITY FOR PROCESSING INFORMATION 1.
20. Mirsky, Y., Mahler, T., Shelef, I. and Elovici, Y. (2019). CT-GAN: Malicious Tampering of 3D Medical Imagery Using Deep Learning. *arXiv*, Accessed 6 June 2019. https://doi.org/10.48550/arXiv.1901.03597.
21. Mitchell, T. (1997). MACHINE LEARNING. McGraw-Hill.
22. Oracle and KPMG. (2019). Defining Edge Intelligence: Closing Visibility Gaps with a Layered Defense Strategy ORACLE AND KPMG CLOUD THREAT REPORT 2019 Oracle and KPMG Cloud Threat Report 2019 2.
23. Ponemon Institute. (2018). 2017 Cost of data breach study: Global overview.
24. Radford. (2019). Better Language Models and Their Implications. *OpenAI*, Accessed 14 February 2019. https://openai.com/blog/better-language-models/.
25. Saavedra, G. J., Rodhouse, N. K., Dunlavy, M. D. and Kegelmeyer. W. P. (2019). A Review of Machine Learning Applications in Fuzzing, Accessed 2 June 2019. http://arxiv.org/abs/1906.11133.
26. Sample, I. (2020). What Are Deepfakes – and How Can You Spot Them? *The Guardian*, 13 January 2020, sec. News. https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them.

27. Schneier, B. (2021). The Coming AI Hackers, Paper, April 2021.
28. Simonite, T. (2022). Did a Person Write This Headline, or a Machine? *Wired*. Accessed 26 October 2022. https://www.wired.com/story/ai-text-generator-gpt-3-learning-language-fitfully/.
29. Song, J. and Alves-Foss, J. (2016). DARPA Cyber Grand Challenge: A Competitor's Perspective, Part 2. *IEEE Security and Privacy* 14 (1 January 2016): 71–81. https://doi.org/10.1109/MSP.2016.14.
30. Smingleigh, C. [@Smingleigh]. (2018). I Hooked a Neural Network up to My Roomba. Tweet. *Twitter*, 8 November 2018. https://twitter.com/Smingleigh/status/1060325665671692288.
31. Sobers, R. (2020). Data Breach Response Times: Trends and Tips. *17 June 2020*. Accessed 27 October 2022. https://www.varonis.com/blog/data-breach-response-times.
32. Simonite, T. (2022). This Bot Hunts Software Bugs for the Pentagon | WIRED. Accessed 27 October 2022. https://www.wired.com/story/bot-hunts-software-bugs-pentagon/.
33. Turing, A. M. (1950). COMPUTING MACHINERY AND INTELLIGENCE. *Computing Machinery and Intelligence. Mind*. Vol. 49, 1950.
34. Weiss, M. (2022). Deepfake Bot Submissions to Federal Public Comment Websites Cannot Be Distinguished from Human Submissions. *Technology Science*. Accessed 26 October 2022. https://techscience.org/a/2019121801/.
35. Wu, Z., Lim, N., Davis, S. L. and Goldstein, T. (2020). Making an Invisibility Cloak: Real World Adversarial Attacks on Object Detectors. In *European Conference on Computer Vision*, 1–17. Springer.

MACHINE LEARNING AND CYBER SECURITY

Abstract

Cyber attacks are expanding, and their number, sophistication, malicious nature and subsequent loss of income are on the increase. The most significant factors for the loss of income are malware, web-based attacks, denial-of-service attacks, malicious insider threats, and social engineering. The lack of cadre in the cyber security field has been evident for years, and with the number of attacks on the increase as well as their heightened sophistication and maliciousness this problem is becoming more pronounced. One of the possibilities of overcoming this shortage of cadre is the use of artificial intelligence, i.e. machine learning in controlling cyber security. Machine learning has proved to be efficient in big data analysis and spotting patterns which were not previously known or obvious, and could be useful. Machine learning refers to the ability of a software system to make generalisations on the basis of previous experience, whereby experience is considered a data set of the phenomena/entities which are the subject of learning, and generalisation is implemented on those phenomena/entities which were not previously known. Machine learning is used to detect cyber attacks as well as for blocking attackers. However, machine learning could also be used during an attack on a targeted system in real time to analyse the infiltration into the victims' system and disclose the software vulnerabilities within the system. In addition, with regard to attacks on machine learning models, i.e. adversarial learning, the weaknesses of the machine learning system itself and the data which depends on it are also investigated.

In this paper the possibilities of implementing machine learning in cyber security will be analysed with a particular focus on whether machine learning will serve to speed up cyber attacks or help to resolve them. In addition to the advantages of using machine learning in processing large amounts of data, will some new risks also be introduced into cyber space? Would the implementation of machine learning enable malicious users to create even more malicious and sophisticated attacks? Does machine learning add complexity to the traditional vector attack, increasing the risk of cyber operations without a full understanding of the operating method and potential effects? Understanding both the possibilities and limitations of machine learning is essential in order to preventing its wrongful use.

Keywords: *cyber attacks, artificial intelligence, adversarial learning, malicious program, phishing, natural language processing.*

КАЗНЕНОПРАВНИ ОКВИР ЗАШТИТЕ ПОДАТАКА У РЕПУБЛИЦИ СРБИЈИ

Младен М. Милошевић[1]

Апстракт

Прикупљање, обрада, анализа, оцена и заштита података, као и слободан јавни приступ одређеним подацима, представљају изазовну и комплексну материју за законодавно уређивање. У позитивном праву Републике Србије на снази су четири закона која непосредно регулишу ову материју, уз низ подзаконских аката и других прописа који се, посредно и/или делимично, баве питањима од значаја за област заштите података.

Имајући у виду сложеност и обимност прописа, аутор се опредељује да у границама рада прикаже и анализира казненоправни оквир заштите података. Циљ рада није да детаљно прикаже сва кривична дела, привредне преступе и прекршаје у вези са неовлашћеним прикупљањем, обрадом и одавањем свих категорија података, већ да критички преиспита законодавни приступ и укаже на могуће правце даљег легислативног развоја.

У централном делу рада аутор холистички сагледава оквир казненоправне заштите података, приказујући посебности разнородних категорија података, односно њиховог законског регулисања. Аутор се критички осврће на специфичности, али и недостатке кривичне, прекршајне (понегде и привреднопреступне) заштите: података о личности, тајних података, пословне и професионалне тајне и права на приступ информацијама од јавног значаја. Посебно је размотрен однос различитих врста казнене одговорности за поједина противправна понашања у светлу принципа „не двапут о истом“. Уочавају се и системске неусклађености и неуједначености прописа у овој области.

---

[1] Универзитет у Београду – Факултет безбедности; e-mail: milosevic@fb.bg.ac.rs.

Рад је настао у оквиру пројекта који финансира Фонд за науку Републике Србије у оквиру Програма „Идеје“ – Management of New Security Risks – Research and Simulation Development, NEWSIMR&D, #7749151.

У закључним разматрањима аутор даје аргументовану оцену законодавчевог приступа и сугерише да су неопходне измене и допуне појединих прописа у циљу њиховог међусобног усаглашавања и изградње солиднијег правног оквира. Нарочито се разматра основаност законодавних решења услед којих долази до својеврсног „судара“ прекршајне и кривичне одговорности. Аутор снажно истиче потребу за хармонизацијом споредног и главног кривичног законодавства у области заштите података и критикује приступ који ствара озбиљне тешкоће приликом практичне имплементације права.

Кључне речи: казненоправна заштита података, подаци о личности, пословне и професионалне тајне, тајни подаци, информације од јавног значаја.

Увод

Како год да се кроз историју називао и представљао, податак је био један од важних извора друштвене моћи. Познавање одређених чињеница, идеја и концепата који другима нису доступни увек је пружало компаративну предност у различитим сферама живота. Такође, чување одређених информацију у тајности, тако да су доступне само ограниченом кругу субјеката, одувек је један од предуслова личне или колективне безбедности и сигурности.

Савремено доба, а посебно неслућен развој информационо-комуникационих технологија, доноси велике изазове на овом пољу. Могућности које пружа дигитална обрада података, њихова доступност и невероватна брзина преноса и дељења, створиле су ризике по људска права, имовинску и личну сигурност грађана, пословање корпорација, па и саму националну и међународну безбедност. Речју, лакоћа, једноставност и комфор које је нам је пружио сајбер простор имају и „цену“ – изгледа високу.

Подаци у електронском облику неретко постају мета ловаца на незаконите профите. Они се купују, продају и на друге начине злоупотребљавају зарад стицања противправне имовинске користи. Такође, подаци се користе ради уцене, осветничке порнографије, увреде и клевете и сл. Изложеност ризицима у сајбер простору очигледно је већа него у физичком свету, јер су подаци у физичком облику мање доступни, теже преносиви и компликованији за компромитацију. Наравно, обе форме представљања чињеница (дигитални и физички облик) заслужују и потребују правну заштиту, што је утицало на законодавце широм планете, али и међународне организације да се позабаве овом проблематиком. Развој информационо-комуникационих технологија несумњиво је утицао на увођење нормативних новитета.

Предмет овог рада је казненоправна заштита података у савременој Србији. Покушаћемо сажето да представимо одредбе закона којима се уводи кривична, прекршајна и привреднопреступна одговорност за радње усмерене против

података, односно њихове безбедности, доступности и интегритета, без тенденције да их детаљно приказујемо и анализирамо, већ са циљем да укажемо на стратешка опредељења, одређене недостатке и системску неусаглашеност позитивноправне регулативе, као и могуће правце будућег развоја.

Подаци се могу класификовати на различите начине. Уколико као критеријум узмемо отвореност података према јавности, можемо их класификовати на: отворене, податке о личности, укључујући и личне тајне, као и посебно осетљиве информације о личности, пословне тајне, професионалне тајне, тајне податке и информације од јавног значаја. (Мандић, Путник и Милошевић, 2017; Milošević, 2021). Наведена подела узима у обзир и правни оквир у Републици Србији, односно разврстава их сагласно законској уређености њиховог прикупљања, обраде, преноса и заштите. Полазећи од ње, представићемо казненоправи оквир заштите тајних података, пословне и професионалне тајне, података о личности.

Информације од јавног значаја нису штићени подаци, већ информације које треба да буду доступне јавности, односно сваком заинтересованом лицу. Законодавац штити право на доступност тих информација, а не њихово одавање или незаконито прибављање односно коришћење (осим у случају злоупотребе права), те се у оквирима овог рада нећемо бавити њиховом казненоправном заштитом.

Тајни подаци

Казненоправна заштита тајних података у Републици Србији уређена је Законом о тајности података[2] (у даљем тексту ЗТП) и Кривичним закоником[3] (у даљем тексту КЗ). ЗТП је први домаћи закон који систематски уређује област одређивања, означавања, размене, чувања, обраде и заштите тајних података (Матић, 2012; Лазић, 2017). Иако се према тајним подацима примењују посебно строге мере заштите, они су изложени различитим ризицима и претњама, посебно у доба високих технологија (Маркагић, 2018).

Казнене одредбе ЗТП уводе кривичноправну и прекршајну заштиту. Члан 98 ЗТП прописује када постоји кривично дело против тајности података (иако законодавац не даје назив овом кривичном делу) (Ковачевић, Милошевић, 2022, стр. 98). Кривично дело, у основном облику, у чл. 98 ст. 1 ЗТП формулисано је на следећи начин: „ко непозваном лицу саопшти, преда или учини доступним податке или документа који су му поверени или до којих је на други начин дошао или прибавља податке или документа, а који представљају тајне податке са

[2] „Сл. гласник РС“, број 104/09.

[3] „Сл. гласник РС“, бр. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19.

ознаком тајности интерно или поверљиво, одређене према овом закону, казниће се затвором од три месеца до три године“.

Тежи облици су прописани у ст. 2 до 4. Облик из ст. 2 је присутан уколико је предмет извршења кривичног дела податак означен степеном тајности „строго поверљиво“ (запрећена казна од шест месеци до пет година затвора), док ст. 3 санкционише одавање податка класификованог као „државна тајна“ (од једне до десет година затвора). Ст. 4 уводи квалификовани облик који постоји ако је присутна једна од три предвиђене околности: користољубље, намера објављивања или коришћења тајних података у иностранству и извршење дела за време ратног или ванредног стања. Прописана казна зависи од степена тајности податка који представља предмет извршења, односно да ли је квалификаторна околност наступила при вршењу дела из ст. 1, 2 или 3. (Ковачевић и Милошевић, 2022, стр. 98, 99). У најтежем случају, односно ако је при извршењу дела из чл. 98 ст. 3 наступила једна од три наведене околности, запрећена је казна од пет до петнаест година затвора. Ставом 5 овог члана је прописан и нехатни облик одавања тајног податка. Запрећена казна и овде зависи од степена тајности.

Ипак, још пре доношења ЗТП, постојала је кривичноправна заштита тајних података, у оквиру главног кривичног законодавства. КЗ прописује неколико кривичних дела којима се штите тајни подаци, али уз значајне терминолошке и суштинске разлике. Реч је кривичним делима: одавање државне тајне (чл. 316 КЗ), одавање војне тајне (члан 415 КЗ) и одавање службене тајне (чл. 369 КЗ). Ова дела, осим основних, имају и допунске облике (квалификоване и привилеговане) (Милошевић, 2022; Милошевић, 2022а).

Овде, међутим, настаје озбиљан проблем који се огледа у неусаглашености прописа. Члан 321 ст. 3 КЗ прописује казну од најмање десет година затвора или доживотни затвор уколико су дела из чл. 314 до 319 КЗ учињена за време ратног или ванредног стања или оружаног сукоба. Али чл. 316 ст. 3 предвиђа казну од три до петнаест година затвора за идентично понашање (одавање државне тајне током ратног или ванредног стања, односно оружаног сукоба). Који од два прописана распоне казне важи? По кривичноправним принципима, важио би блажи распон казне, али је заиста тешко разумети зашто законодавац једноставно не отклони ову неусаглашеност (Милошевић, 2010; Ковачевић и Милошевић, 2022). Имајући у виду да и чл. 98 ст. 3 прописује трећи распон казне за садржински исто понашање, проблем постаје још озбиљнији (иако се у овом случају може бранити став да одредбе ЗТП важе само за податке који су категорисани по одредбама тог закона, док КЗ важи за „старе“ податке).

Проблем односа КЗ и ЗТП Ковачевић и Милошевић (2022) третирају на следећи начин: „поставља се питање да ли су у КЗ оправдано задржана кривична дела одавање службене тајне (чл. 369) и одавање војне тајне (чл. 415). Те категорије

тајних података укинуте су доношењем ЗТП (видети члан 109), али сигурно није извршено (или у јавности није познато) преиспитивање ознака свих докумената и података који су проглашени за војну или службену тајну по прописима који су важили до ступања на снагу ЗТП, иако је члан 105 став 2 овог прописа експлицитно одредио да је то потребно учинити у року од две године од ступања закона на снагу. Ипак, члан 105 став 1 ЗТП јасно одређује да документи и подаци означени по одредбама раније важећих прописа задржавају врсту и степен тајности које су имали (члан 105 став 1 ЗТП). Интенција законодавца да се преиспитају све раније утврђене ознаке тајности тешко је могла бити спроведена у пракси због претпостављеног обима и бројности означених података и докумената. Имајући у виду одредбу члана 105 став 1 ЗТП, јасно је да одредбе КЗ којима се инкриминишу одавање војне и службене тајне морају остати на снази докле год су присутни документи и подаци који су означени као наведене врсте тајних података“ (Ковачевић и Милошевић, 2022, стр. 101, 102).

Чињеница да је од доношења ЗТП протекло 13 година не улива оптимизам у погледу коначног уједначавања законских одредби о санкционисању друштвено опасних радњи против различитих категорија тајних података. У литератури се истичу и други недостаци законског одређења свих наведених кривичних дела. (Милошевић, 2022; Ковачевић и Милошевић, 2022).

Осим кривичноправне, законодавац прописује и прекршајну одговорност за неправилно поступање са тајним подацима. Чл. 99 ст. 1 тач. 1 до 17 ЗТП прописује прекршајне санкције за одговорно лице у органу јавне власти. Прописана новчана казна је између 5.000 и 50.000 динара. Прекршаји из наведених тачки обухватају разноврсне радње извршења, попут: преношења овлашћења за одређивање тајног податка на треће лице; неправилно означавање податка или документа степеном тајности (иако нису испуњени услови); означавање податка неодговарајућим степеном тајности; доношење одлуке о одређивању степена тајности без образложења; неопозивање тајности податка након истека законског рока, наступања датума или догађаја после кога престаје тајност податка, доношења решења Повереника за информације од јавног значаја и заштиту података о личности или одлуке надлежног суда о опозиву тајности; непрописивање општих и посебних мера заштите података у складу са одређеним степеном тајности, као и пропуштање да се оне организују и надзиру; неспровођење периодичне процене тајности податка; неорганизовање унутрашње контроле над заштитом тајних података; невођење евиденције о издатим сертификатима за приступ тајном податку итд.

Према чл. 100 ЗТП исти распон новчане казне је прописан за руковаоца тајним подацима који не предузима мере заштите тајних података у складу са чл. 34 истог закона. Према том члану, руковалац је дужан да: „предузима мере заштите тајних података и омогућава корисницима непосредан приступ тајним подацима, издаје

копију документа који садржи тајни податак, води евиденцију корисника и стара се о размени тајних података“ (ЗТП, чл. 34).

Помало је спорна радња извршења прекршаја из чл. 99 тач. 13 ЗТП, која постоји када лице „тајне податке достави правним и физичким лицима супротно одредби члана 46 овог закона“. Овде се ради о достављању тајних података на основу уговорног односа између органа јавне власти и правног или физичког лица које му пружа одређене услуге. Достављање тајних података у случају постојања оваквог уговорног односа могуће је уз испуњење законских услова (правно или физичко лице испуњава организационе и техничке услове за чување тајних података у складу са овим законом и другим прописима; за лица која обављају уговорене послове извршене су безбедносне провере и издати сертификати и она писаном изјавом потврђују да су упозната са овим законом и другим прописима који уређују чување тајних података и обавезују се да ће са тајним подацима поступати у складу са тим прописима; приступ тајним подацима је потребан ради реализације послова из уговора – чл. 46 ст. 1 тач. 1 до 4 ЗТП). Међутим, у пракси неће бити једноставно разграничити радњу овог прекршаја од радње нехатног облика кривичног дела (чл. 98 ст. 5 ЗТП), а понекад чак и од умишљајног облика дела. У оба случаја непозвано лице се упознаје са садржином тајног податка од стране овлашћеног лица (дакле, лица ком су тајни подаци поверени). Сматрамо да је биће овог прекршаја требало да буде уже и прецизније дефинисано, посебно знајући огромне разлике у одговорности и запрећеној казни између прекршаја и кривичног дела против тајности података.

Такође, чини нам се да је законодавац начинио пропуст тиме што није донео посебне казнене одредбе којим би ближе регулисао одговорност правног или физичког лица које по основу уговорног односа остварује увид у тајне податке органа јавне власти ради обављања послова предвиђених уговором. Мислимо да је материја довољно важна и осетљива, те да заслужује посебне одредбе, а не санкционисање кроз квалификовање путем других казнених одредби.

Пословне тајне

Казненоправна заштита пословне тајне предвиђена је одредбама КЗ и Закона о заштити пословне тајне[4] (у даљем тексту ЗЗПТ). За разлику од тајних података, код пословне тајне је јасно разграничено да се кривичноправна заштита обезбеђује одредбама КЗ, док су прекршајна и привреднопреступна у оквирима посебног закона (ЗЗПТ). Пословна тајна је податак од великог значаја у савременој тржишној привреди, заснованој на иновацијама, истраживању и технолошком развоју (Jovičić, 2018; Милошевић, 2022). Важан међународни

[4] „Сл. гласник РС“, број 53/21.

извор права у овој области јесте Директива 2016/943 Европског парламента и Савета од 8. јуна 2016. године о заштити неоткривених знања и искуства, те пословних информација (пословне тајне) од незаконитог прибављања, употребе и откривања (Службени лист ЕУ Л бр. 157/1). На глобалном плану значајан је тзв. ТРИПС споразум (Споразум о трговинским аспектима права интелектуалне својине – *The Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS)), Светска трговинска организација, 1994 (ступио на снагу 1995. године).[5] У РС је до 2021. године важио закон истог назива (Закон о заштити пословне тајне[6]), али је потреба за хармонизацијом са Директивом ЕУ условила доношење новог закона.

Кривично дело одавања пословне тајне прописано је одредбама чл. 240 КЗ. Основни облик (чл. 240 ст. 1 КЗ) постоји када извршилац непозваном лицу неовлашћено саопшти, преда или учини доступним податке који представљају пословну тајну, као и уколико прикупља такве податке у намери да их преда непозваном лицу. Запрећена је казна затвора од шест месеци до пет година затвора.

Важан недостатак формулације основног облика, како се наводи у литератури, јесте тај што њоме нису обухваћене радње незаконитог прибављања пословне тајне од стране трећег лица. Инкриминисано је одавање пословне тајне које учини њен законити држалац тако што је открије непозваном лицу. Али, ако би непозвано лице само прибавило пословну тајну, и то на незаконит начин, оно се не би могло сматрати извршиоцем овог кривичног дела, већ би сносило само грађанскоправну и прекршајну (у појединим случајевим привреднопреступну) одговорност (Милошевић, 2022, стр. 130, 131; Milošević, 2021a, стр. 60; Пресуда Основног суда у Нишу, К 65/14 од 23.04.2014. године).

Тежи облик (чл. 240 ст. 2 КЗ) постоји уколико је дело учињено из користољубља или у погледу нарочито поверљивих података. Предвиђена је казна од две до десет година затвора уз новчану казну (кумулативно). Законодавац је предвидео, објективно гледајући, веома строгу казну за квалификовани облик одавања пословне тајне. Иначе, и у погледу тежег облика се може упутити једна критика. Наиме, није јасно зашто законодавац није као квалификаторну околност предвидео ситуацију у којој учинилац одаје пословну тајну ради њеног коришћења у иностранству (тзв. индустријска шпијунажа). Ово решење је било присутно у ранијем кривичном законодавству (Милошевић, 2022, стр. 133; Срзентић и др., 1986, стр. 459, 460).

---

[5] Текст доступан на: https://www.zis.gov.rs/upload/documents/pdf_sr/pdf/trips.pdf (приступљено 31.05.2022. године).

[6] „Сл. гласник РС“, број 72/11.

Привилеговани облик постоји у случају одавања пословне тајне из свесног или несвесног нехата. Запрећена је казна до три године затвора. Овај облик је значајан и због превенције криминалног понашања у сфери заштите конкуренције и пословне тајне, као и ради јачања корпоративне безбедносне културе и свести (Мандић, Путник и Милошевић, 2017; Miloševíc, 2021a).

Прекршајна и привреднопреступна одговорност (грађанскоправна и радноправна одговорност нису предмет овог рада) регулисана је одредбама ЗЗПТ. Члан 21 ЗЗПТ прилично широком формулацијом прописује јединствену радњу извршења прекршаја и привредног преступа против пословне тајне. Да ли ће извршилац одговарати за привредни преступ или прекршај, зависи од његовог правног статуса и субјективитета – уколико је реч о одговорном лицу у правном лицу или самом правном лицу, дело се квалификује као привредни преступ; у случају да је обележја остварило физичко лице или предузетник, у питању је прекршај. Прописана је и мера обавезног одузимања, односно уништења предмета извршења привредног преступа или прекршаја (ЗЗПТ, чл. 1 ст. 5).

Радња је прописана одредбом чл. 21 ст. 1 ЗЗПТ и гласи: „Казниће се за привредни преступ новчаном казном у износу од 100.000 до 3.000.000 динара правно лице које у складу са чланом 4 овог закона незаконито прибави, користи или открије пословну тајну“. Ст. 2 до 4 прецизирају субјекте дела и тип казненог деликта: ст. 2 одређује привреднопреступну новчану казну од 50.000 до 200.000 динара за одговорно лице у правном лицу; ст. 3 прописује прекршајну новчану казну за предузетника у износу од 50.000 до 500.000 динара; док ст. 4 садржи запрећену прекршајну казну за физичко лице у износу од 20.000 до 150.000 динара.

Овако дефинисана радња извршења се у највећој мери поклапа са радњом кривичног дела из чл. 240 ст. 1 КЗ. Штавише, она је шира од радње кривичног дела јер обухвата и акте незаконитог прибављања и коришћења пословне тајне од стране непозваног лица, док се кривично дело односи само на одавање пословне тајне које учини овлашћени држалац пословне тајне. Имајући у виду изузетне разлике у запрећеним казнама (нпр. и казна за нехатни облик дела из чл. 240 далеко је строжа од прописаних казни због привредних преступа и прекршаја), констатујемо да је овде реч о озбиљним системским неусаглашеностима (Miloševíc, 2021a, стр. 62, 63). Оправдано се поставља питање да ли је кривичноправна заштита неопходна или је довољно да се држаоцу пословне тајне остави само заштита коју осигуравају друге гране права. Ако кривичноправна заштита јесте потребна, нужне су законске измене у циљу усаглашавања прописа.

Подаци о личности и професионалне тајне

Подаци о личности су постали важан предмет правне заштите последњих година (Prlja, 2018, стр. 89–90; Дилигенски и др., 2018). Од великог значаја за развој ове

материје било је доношење чувеног GDPR – Опште уредбе ЕУ о заштити података о личности (Општа Уредба (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године о заштити физичких лица у односу на обраду података о личности и о слободном кретању таквих података и о стављању Директиве 95/46/ЕЗ ван снаге; даље: Општа уредба ЕУ). Она је заменила Директиву ЕУ из 1995. године (Директива ЕУ о заштити грађана у вези са обрадом података о личности и о слободном кретању таквих података 1995/46).

Казненоправна заштита података о личности уведена је одредбама КЗ и Закона о заштити података о личности[7](у даљем тексту ЗЗПЛ), који је донет по угледу на Општу уредбу ЕУ. Пре доношења овог закона, важио је претходни истог назива (Закон о заштити података о личности[8]), али је потреба за усаглашавањем са европском регулативом довела до законодавних промена. Почнимо, ипак, од кривичноправне заштите.

У КЗ се налази више кривичних дела чији је предмет извршења податак о личности, иако се законски назив само једне инкриминације непосредно односи на ову материју (чл. 146 КЗ – неовлашћено прикупљање личних података). У литератури се истиче: „Анализа кривичноправних норми којима се штити право на заштиту података о личности треба да обухвати сва релевантна кривична дела, чијом радњом извршења може бити примарно повређено ово право. Осим дела из члана 146, то су и: неовлашћено откривање тајне (члан 141); прогањање (члан 138а став 1 тачка 3); повреда тајности писма (члан 142); неовлашћено прислушкивање и снимање (члан 143); неовлашћено фотографисање (члан 144) и неовлашћено објављивање и приказивање туђег списа, портрета и снимка (члан 145); па и кривично дело изношења личних и породичних прилика (члан 172), а можда и друга“ (Милошевић, 2021, стр. 117).

Уско посматрано, једино кривично дело које се по називу и садржину у потпуности односи на материју заштите података о личности јесте неовлашћено прикупљање података о личности. Основни облик дела је присутан када се подаци о личности који се прикупљају и обрађују на основу закона неовлашћено прибаве, саопште другима или употребе у сврху за коју нису намењени (КЗ, чл. 146 ст. 1). Чл. 146 ст. 2 одређује да је кривично дело и када учинилац противно закону прибавља личне податке или користи незаконито прикупљене податке. За оба облика је прописана казна до једне године затвора алтернативно са новчаном казном (Делић, 2021; Стојановић, 2018).

Гоњење се предузима по приватној тужби, што указује да је кривичноправна заштита личних података секундарна (Милошевић, 2021, стр. 119). Једино се

[7] „Сл. гласник РС“, број 87/18.

[8] „Сл. гласник РС“, бр. 97/08, 104/09, 68/12 и 107/12.

квалификовани облик из става 3, за који је запрећена новчана казна или затвор до три године, гони по службеној дужности.

Прекршајна заштита је обезбеђена одредбама ЗЗПЛ. Слично као и код пословне тајне, мада у мањој мери, јавља се проблем разграничења радње прекршаја и радње кривичног дела. Казнене одредбе су смештене у оквире члана 95 ЗЗПТ. Ставом 1 је прописан низ алтернативних радњи за чије извршење одговарају руковаоци и обрађивачи у зависности од својства: за правна лица запрећена је казна од 50.000 до 2.000.000 динара; за предузетнике од 20.000 до 500.000 динара (чл. 95 ст. 4 ЗЗПЛ); за физичко лице, односно одговорно лице у правном лицу, државном органу, органу територијалне аутономије и јединици локалне самоуправе, представништву или пословној јединици страног правног лица од 5.000 до 150.000 динара (чл. 95 ст. 5 ЗЗПЛ).

Законодавац набраја чак 32 алтернативне радње извршења прекршаја у ставу 1. Међу тим радњама се налазе и оне које се у претежном делу, па чак и у потпуности преклапају са радњом кривичног дела (нпр. ако руковалац или обрађивач обрађује податке у другу сврху; уколико обрађује податке о личности без сагласности лица на које се подаци односе, а није у могућности да предочи да је лице на које се подаци односе дало пристанак за обраду својих података; обрађује податке о личности у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе супротно члану 92 ЗЗПЛ; врши пренос података о личности у друге земље и међународне организације супротно закону).

Чл. 95 ст. 2 ЗЗПЛ прописује други (лакши) облик прекршаја, за који је прописана фиксна новчана казна од 100.000 динара за руковаоца, односно обрађивача у својству правног лица (казна за предузетника је 50.000 динара, а за одговорна лица у правним лицима и органима јавне власти 20.000 динара). Прописано је 6 алтернативних радњи извршења, међу којима су: када руковалац (обрађивач) не одреди свог представника у Републици Србији, или не води прописане евиденције о обради или не бележи радње обраде; не објави контакт податке лица за заштиту података о личности и не достави их Поверенику; не упозна примаоца са посебним условима за обраду података о личности прописним законом и његовом обавезом испуњења тих услова.

Посебан облик прекршаја је прописан у чл. 95, ст. 3. Радња овог прекршаја је остварена када учинилац не чува као професионалну тајну податке о личности које је сазнао током обављања послова. Извршилац може да буде физичко лице, а прописана је новчана казна од 5.000 до 150.000 динара. Ипак, овде се поставља питање судара са одговорношћу за кривично дело неовлашћеног откривања тајне из чл. 141 КЗ, посебно у светлу процесног правила *ne bis in idem* (Милошевић, 2021, стр. 132; Zupančič, 2011; Ivičević Karas, Kos, 2012). Код дела из чл. 141 КЗ се као извршилац, осим адвоката и лекара, помиње и друго лице које је сазнало за тајну у

вршењу свог позива. Дакле, предмет заштите је у оба случаја професионална тајна, а извршиоци могу да постану лица која су задужена за испуњавање законских обавеза руковаоца и обрађивача података о личности.

Закључак

Могућности за злоупотребу података су се последњих деценија значајно увећале. Дигитална ера је донела бројне погодности, али и ризике и изазове. Суочавање са новим безбедносним ризицима на плану заштите података захтева изградњу солидног и хармоничног правног оквира, усаглашеног са међународним изворима права, стандардима и добрим праксама.

Казненоправни оквир заштите података у Републици Србији јесте релативно развијен и обухватан, али не и у потпуности кохеренатан и непротивречан. У раду су изнете озбиљне критике поводом појединих законских решења, односно међусобне неусаглашености прописа и проблема који настају у практичној примени права, услед судара прекршајних и кривичних (негде и привреднопреступних) норми, нарочито у контексту процесне забране „не двапут о истом“.

Правни оквир се не може оценити као потпуно адекватан док се законодавном интервенцијом не отклоне примећени недостаци. Посматрајући казненоправне одредбе о тајним подацима, пословној тајни, подацима о личности и професионалној тајни, закључили смо да су потребне измене и допуне закона, првенствено ради међусобне хармонизације. Такође, знајући колико је област заштите података у дигитално доба динамична и развијена, сматрамо да субјекти криминалне политике морају да буду свесни потребе за честим мењањем односно ажурирањем прописа, како би правна реалност „ухватила корак“ са брзо растућим ризицима, првенствено у сајбер простору.

Коначно, правни прописи имају велику улогу на репресивном и превентивном плану. Мислимо да је изградња адекватног правног оквира од суштинског значаја и за јачање безбедносне културе, као и очување основних људских права и заштиту важних и легитимних личних, националних и корпорацијских интереса.

Библиографија

1. Делић, Н. (2021). *Кривично право – посебни део*. Београд: Универзитет у Београду, Правни факултет.
2. Дилигенски, А., Прља, Д., Церовић, Д. (2018). *Право заштите података GDPR*. Београд: Институт за упоредно право.
3. Директива 2016/943 Европског парламента и Савета од 8. јуна 2016. године о заштити неоткривених знања и искуства те пословних

информација (пословне тајне) од незаконитог прибављања, употребе и откривања, *Службени лист ЕУ* Л бр. 157/1.
4. Директива ЕУ о заштити грађана у вези са обрадом података о личности и о слободном кретању таквих података 1995/46.
5. Закон о заштити података о личности („Сл. гласник РС“, број 87/18).
6. Закон о заштити података о личности („Сл. гласник РС“, бр. 97/08, 104/09, 68/12 и 107/12).
7. Закон о заштити пословне тајне („Сл. гласник РС“, број 53/21).
8. Закон о заштити пословне тајне („Сл. гласник РС“, број 72/11).
9. Закон о тајности података („Сл. гласник РС“, број 104/09).
10. Zupančič, B. M. (2011). Ne bis in idem (zabrana ponovnog suđenja za isto delo): la belle dame sans merci, *Crimen: časopis za krivične nauke*, 2(2), pp. 171–178.
11. Ivičević Karas, E. & Kos, D. (2012). Primjena načela ne bis in idem u hrvatskom kaznenom pravu, *Hrvatski ljetopis za kazneno pravo i praksu* 19(2), pp. 555–584. URL: https://hrcak.srce.hr/110872.
12. Jovičić, K. (2018). Poslovne tajne: određenje i osnovi zaštite. *Strani pravni život*, 62(1), pp. 7–19.
13. Ковачевић, Н., Милошевић, М. (2022). Заштита тајних података у дигиталној форми – безбедносни и кривичноправни аспекти. *Безбедност*, 1/2022, стр. 93–108. doi: 10.5937/bezbednost2201093K
14. Кривични законик („Сл. гласник РС“, бр. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19).
15. Лазић, Р. (2017). Заштита тајности података – од правног основа до практичне примене. *Српска политичка мисао*, број 3/2017. год. 24. vol. 57. стр. 205–222.
16. Мандић, Г., Путник, Н., Милошевић, М. (2017). *Заштита података и социјални инжењеринг – правни, организациони и безбедносни аспекти*. Београд: Универзитет у Београду, Факултет безбедности.
17. Маркагић, М. (2018). Компромитујућа електромагнетна зрачења – изазови, претње и заштита. *Војнотехнички гласник*, вол. 66, бр. 1, стр. 143–153.
18. Матић, Г. (2012). *Систем заштите тајних података*. Београд: Организација за европску безбедност и сарадњу, Мисија ОЕБС у Србији: Канцеларија Савета за националну безбедност и заштиту тајних података.
19. Милошевић М. (2010). Кривична дела против уставног уређења и безбедности Републике Србије – историјски и позитивноправни приказ. У: Цветковић, В. (уредник). *Ризик, моћ и заштита – увођење у науке безбедности* (стр. 414–452). Београд: Службени гласник и Универзитет у Београду – Факултет безбедности.
20. Милошевић, М. (2021). Кривичноправна заштита података о личности. *Ревија за криминологију и кривично право*, 2/21, стр. 113–130.
21. Милошевић, М. (2022а). Кривичноправна заштита система националне безбедности: стратешке дилеме. Рад представљен на конференцији:

Михајло Копања и Владимир Ајзенхамер (ур). *Геополитички интереси великих сила и стратешка безбедност малих држава* (стр. 196–210). Београд: Факултет безбедности и ИМПП. 0.5 DOI: 10.18485/fb_givs_sbmd.2022.ch13.

22. Милошевић, М. *Кривично право – посебни део: изабране инкриминације за студије наука безбедности*. Београд: Универзитет у Београду, Факултет безбедности.
23. Milošević, M. (2021a). The Role of Criminal Law in Trade Secret Protection. „Archibald Reiss Days“. Paper presented at the 11th Thematic Conference Proceedings of International Significance, 9–10. November 2021 (pp. 53–63). Belgrade: University of Criminal Investigation and Police Studies.
24. Општа Уредба (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године о заштити физичких лица у односу на обраду података о личности и о слободном кретању таквих података и о стављању Директиве 95/46/ЕЗ ван снаге.
25. Пресуда Основног суда у Нишу, К 65/14 од 23.04.2014. године.
26. Prlja, S. (2018). Pravo na zaštitu ličnih podataka u EU. *Strani pravni život*, 62(1), str. 89–99.
27. Споразум о трговинским аспектима права интелектуалне својине (*The Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS), Светска трговинска организација, 1994 (ступио на снагу 1995. године). Приступљено 31.05.2021. године: https://www.zis.gov.rs/upload/documents/pdf_sr/pdf/trips.pdf
28. Срзентић, Н., Стајић, А., Краус, Б., Лазаревић, Љ., Ђорђевић, М. (1986). *Коментар кривичних закона СР Србије, САП Косова и САП Војводине.* Београд: Савремена администрација.
29. Стојановић, З. (2018). *Коментар Кривичног законика*. Београд: Службени гласник.

CRIMINAL DATA PROTECTION FRAMEWORK IN THE REPUBLIC OF SERBIA

Abstract

The collection, processing, analysis, evaluation and protection of data, as well as free public access to certain data, represent a challenging and complex matter for legislative regulation. In the legal system of the Republic of Serbia, there are four laws in force that directly regulate this matter, along with a number of by-laws and other regulations that, indirectly and/or partially, deal with issues of importance in the field of data protection.

Bearing in mind the complexity and scope of the regulations, the author decides to present and analyze the criminal law framework of data protection within the limits of the work. The aim of the paper is not to present in detail all crimes, economic offenses and misdemeanors related to unauthorized collection, processing and disclosure of all categories of data, but to critically review the legislative approach and indicate possible directions for further legislative development.

In the central part of the paper, the author takes a holistic view of the criminal law framework of data protection, showing the peculiarities of various categories of data. The author takes a critical look at the specifics, but also the shortcomings of criminal, misdemeanor (and sometimes economic offenses) norms: personal data, trade data, classified data, professional secrets and the right to access information of public importance. The relationship between different types of criminal liability for certain illegal behaviors was especially considered in the light of the principle of ne bis in idem. Systemic inconsistencies and lack of harmonization between different laws in this area are also observed.

In the concluding remarks, the author gives an assessment of the legislator's approach and suggests that changes and additions to certain regulations are necessary in order to harmonize them with each other and build a more solid legal framework. In particular, the merits of legislative solutions are considered, as a result of which there is a kind of "collision" between misdemeanor and criminal liability. The author strongly emphasizes the need for harmonization of secondary and main criminal legislation in the field of data protection and criticizes the approach that creates serious difficulties in the practical implementation of the law.

Keywords: *criminal law and protection of data; trade secrets, classified data, personal data, right to access information of public importance*.

СПЕЦИФИЧНОСТИ УВИЂАЈА ПРИЛИКОМ ОТКРИВАЊА ИЛЕГАЛНИХ ЗАСАДА ЗА ПРОИЗВОДЊУ КАНАБИСА

Божидар Оташевић[1]

Апстракт

Једноставне процедуре производње, детаљне инструкције и упутства која се могу пронаћи на интернету, као и лако доступни потребни препарати и апаратуре, утицали су на пораст илегалне производње канабиса у Србији. Свакодневно откривање високопрофитабилних лабораторија и засада на отвореном указује на то да се домаћа потрошња све више снабдева из домаће производње. Међутим, због велике разноликости у начину култивације, као и због непостојања стандардизованих образаца за извештавање о заплењама на националном нивоу, није могуће извршити процену обима производње са прецизношћу која би била задовољавајућа за практичне потребе. Циљ овог рада је да укаже на законодавни оквир контроле канабиса у Србији и на криминалистичко-форензичку обраду места кривичног догађаја на ком се налази илегални засад канабиса, са посебним акцентом на значај материјалних доказа у сузбијању ове врсте криминалитета.

Стандардизација поступања, посебно у подручју трасологије, и познавање специфичних трагова у илегалној производњи канабиса на отвореном неопходни су за доношење релевантних закључака и за успешне криминалистичке истраге. Код илегалних засада канабиса могу се пронаћи трагови пнеуматика, трагови газеће површине стопала, трагови сечења, различити биолошки трагови људског порекла. Међутим, пажњу треба обратити на трагове биљног порекла, као што су саме биљке, полен и споре биљака, који су у криминалистичким истрагама неоправдано запостављени. Форензичка вредност полена и спора огледа се у

[1] Криминалистичко-полицијски универзитет, Београд, e-mail: bozidarotasevic@yahoo.com

Рад је настао у оквиру пројекта Фонда за науку Републике Србије „Идеје“ – Пројекат акцелерације иновација и подстицања раста предузетништва у Републици Србији – *Management of New Security Risks – Research and Simulation Development – NEWSIMR&D,* #7749151.

чињеници да су микроскопске величине, да се продукују у огромном броју, да се идентификују на нивоу токсина, да су високо резистентни и да се тешко распадају.

У раду су посебно описани трагови карактеристични за засад канабиса, њихово проналажење, фиксирање, узорковање, паковање и слање на различита лабораторијска вештачења.

Кључне речи: криминалистичке истраге, засади, биолошки трагови, биљке, полен и споре.

Увод

Канабис (лат. *Canabis sativa*) јесте биљка од које се производи индустријска конопља, али и психоактивне контролисане супстанце.[2] Индустријска конопља се добија од стабла или семена биљке (користи се за комерцијалну производњу хране, папира, (2022) детерџената, пластике, грађевинског материјала).

Међутим, без обзира на то што су све развијене земље у својим законодавствима уредиле систем производње и промета канабиса, он се у готово свим земљама гаји илегално и заузима прво место по популарности, што га чини најзаступљенијом дрогом у свету. Према подацима наведеним у Светском извештају о дрогама за 2016. годину, који је израдила Канцеларија УН за питања дроге и криминала (*United Nations Office on Drugs and Crime* – UNODC), канабис представља водећу илегалну супстанцу у свету што се тиче гајења, производње, препродаје и броја корисника (UNODC World Drug Report, 2016). Према најновијим статистичким подацима објављеним у њеном годишњем извештају о светској ситуацији са злоупотребом дрога, Канцеларија за сузбијање дрога и криминала УН констатује да је тренд повећаног конзумирања канабиса посебно изражен у време пандемије ковида 19. Фактори ризика попут економске кризе и повећаног осећаја социјалне изолације допринели су повећаној употреби свих психоактивних супстанци. Конзумација канабиса у појединим регионима у овом периоду порасла је за чак 42% (UNODC World Drug Report, 2016, p. 33). У периоду пандемије привремено су поремећена тржишта дрога у већини делова света, али су се она брзо консолидовала, уз изражено повећање бесконтактних метода за испоруку дрога потрошачима, посебно кроз поштанске доставе. Криминалне организације које делују на илегалном тржишту дрога служе се врло софистицираним методама рада када су у питању електронски трансфер новца и препродаја дроге путем интернета.

[2] Психоактивне контролисане супстанце су биљке и супстанце обухваћене важећим Правилником о утврђивању списка психоактивних контролисаних супстанци, „Службени гласник Републике Србије“, број 73 од 30. јуна 2022.

Марихуана, хашиш и хашишово уље јесу три производа биљке канабис који се због свог психоактивног дејства налазе на листи опојних дрога. Једна од битних разлика између ових психоактивних супстанци јесте концентрација ТХЦ-а. Тако марихуана садржи најмањи проценат ТХЦ-а (до 5%) и приликом конзумирања има најблаже дејство, хашиш садржи 5–12%, а уље хашиша 15–70% ТХЦ-а (Gazdek, 2014, p. 193). Последњих двадесет година производни процеси, обично у лабораторијски контролисаним условима, повећали су концентрацију ТХЦ-а у марихуани, те његова концентрација може бити 20%, па и више. Проценат ТХЦ-а у индијској конопљи зависи од тога који се део биљке користи за производњу дроге, али и од карактеристика саме биљке, врсте ђубрива, начина прераде, времена кад се бере, као и географске локације на којој расте (Оташевић, Атанасов и Лабовић, 2020, стр. 317). То значи да на канабиноидни садржај у канабису, укључујући и ТХЦ, утиче велики број фактора, као што су генетске разлике, услови узгоја, методе култивације, свежина производа и начин паковања, транспорта и складиштења. Најновија лабораторијска вештачења указују на то да постоје велике разлике у биохемијском саставу канабиса који циркулише на илегалном нарко-тржишту, што је свакако резултат промене генетске структуре биљака и услова гајења.

Законодавни оквир контроле канабиса у Србији

Недавна одлука Комисије УН за опојне дроге о брисању канабиса из Табеле IV Јединствене конвенције УН о опојним дрогама из 1961. године, на препоруку Светске здравствене организације, могла би имати утицај на промену политике многих земаља када је реч о медицинској и „рекреативној“ употреби канабиса (Васиљевић Продановић, Денчић, 2022, стр. 116). По нашем мишљењу, у Србији ће у будућности доћи до јачања иницијатива за измену законодавства у правцу депенализације, декриминализације и легализације канабиса. Према важећем закону о психоактивним контролисаним супстанцама Републике Србије[3], забрањени су поседовање, узгајање и промет варијетета канабиса који могу садржати више од 0,3% супстанци из групе ТХЦ-а (делта-9-тетрахидроканабинола) (члан 58). Истим законом је у члану 59 прописано да самоникла биљка из које се може добити психоактивна контролисана супстанца мора бити уништена. То значи да су у нашој земљи производња, промет и поседовање ове дроге у медицинске и „рекреативне“ сврхе забрањени.

У Србије је дозвољено гајење конопље (*Canabis*) правном, односно физичком лицу које има дозволу коју је издало министарство надлежно за послове пољопривреде. Гајење је дозвољено искључиво у циљу производње влакана,

[3] „Службени гласник Републике Србије“, бр. 99/2010, 57/2018.

производње семена за исхрану животиња, даљег размножавања, прераде, испитивања квалитета семена, као и његовог промета. Ради адекватне контроле, дозвола се може издати само ако је склопљен уговор о производњи и откупу конопље с правним лицем које је регистровано за обављање те делатности.

Правно или физичко лице које је добило дозволу за гајење канабиса дужно је да обавести министарство надлежно за унутрашње послове и министарство надлежно за послове пољопривреде о свакој околности која указује на могућност да су конопља или делови конопље употребљени или да могу бити употребљени за недозвољену производњу психоактивних контролисаних супстанци (члан 60).

У члану 60 став 4 Закона о психоактивним контролисаним супстанцама прописано је да министар надлежан за послове пољопривреде прописује: сорту конопље коју је дозвољено гајити, услове које мора испуњавати правно или физичко лице за добијање дозволе за гајење конопље, начине издавања и рок важења дозволе, трошкове давања дозволе и све друге услове за дозвољено гајење конопље.

Без обзира на то што у Србији постоје иницијативе за измену нашег законодавства у правцу легализације канабиса и у медицинске и у „рекреативне“ сврхе, мишљења смо да је законодавни оквир за контролу канабиса у Србији добар. У нашој земљи су поседовање и промет канабиса у медицинске сврхе забрањени. Став нашег законодавства је исправан, имајући у виду да досадашња научна истраживања не пружају довољно уверљиве доказе да су препарати канабиса лековити. Недостатак тих доказа може довести до непотребне примене канабиса у медицинске сврхе, која може имати штетне последице за пацијенте. Пилот-пројекти, научна истраживања и контролисане клиничке студије којима би се испитивало евентуално лековито дејство канабиса, мада нужни, тренутно су на самом почетку. У прилог томе да је легализација канабиса у медицинске сврхе преурањена говоре и налази једног истраживања спроведеног у Израелу у којем је испитивана повезаност између медицинске примене канабиса и његове злоупотребе. Резултати овог истраживања показали су да изложеност наративним садржајима о позитивним ефектима канабиса на ублажавање здравствених тегоба индиректно учвршћује уверење о потреби легализације и употребе канабиса у „рекреативне“ сврхе (Sznitman, Lewis, 2018).

У складу са наведеним сматрамо да је измена законодавног оквира којим би се дозволила употреба канабиса у „рекреативне“ сврхе апсолутно непотребна, јер би то могло имати многобројне штетне последице по здравље становништва (ризик

од стварања зависности,[4] негативан утицај на концентрацију, памћење и координацију покрета; изазива анксиозност, нападе панике, халуцинације, доводи до когнитивне дисфункције, респираторних проблема и поремећаја у понашању) (Васиљевић Продановић, Денчић, 2022, стр. 118). Такође, може имати негативне последице по безбедност учесника у саобраћају и отежавати рад државних органа на превенцији злоупотребе дрога.

Спољни и унутрашњи узгој канабиса

Канабис се узгаја напољу, на земљиштима различитог квалитета и у готово свим деловима света осим у поларним регионима. Могућ је и унутрашњи узгој у лабораторијским условима, на свим локацијама где је доступан извор струје и воде (Оташевић, Коларевић, 2020, стр. 7).

На подручју југоисточне Европе и западног Балкана канабис се узгаја и на отвореном и у затвореном простору. Када се узгаја напољу, може бити засађен као засебна култура или у комбинацији са неком другом биљном културом, као што су кукуруз, малина, сунцокрет и томе слично. Илегални произвођачи се најчешће одлучују да на рубним деловима парцеле засаде неку другу биљну културу (као што су кукуруз, сунцокрет, малина, зависно од поднебља), док се у унутрашњости парцеле узгаја канабис који је „сакривен од очију јавности“. Засади се формирају у природно погодним условима, обично на падини са доста сунчаних дана у току године и доста сунчаних сати у току дана. Најчешће је то далеко од градских средина, по сеоским атарима, забаченим парцелама са лошим прилазним путевима, поред тешко приступачних обала река и потока, често у жбуњу и на зараслим плацевима. Иако спољни узгој у принципу даје један принос годишње, постоје непотврђени извештаји према којима је могуће добити и три приноса годишње (Bloomer, 2008).

Веома су чести засади у кућним условима, некада и у најурбанијим деловима града. Такви засади су обично замаскирани на терасама станова, крововима зграда или заклоњеним двориштима кућа. Биљке су засађене у саксијама које су позициониране тако да добијају сунчеву светлост. У њиховој близини налазимо разну амбалажу и хемијске препарате за узгој који су карактеристични за засаде на отвореном.

Постоји и комбинована варијанта узгоја биљне културе *Cannabis sativa*, која има карактеристике и засада и лабораторије – то је заправо узгој канабиса у пластеницима. Реч је о затвореном простору у коме је инсталирана опрема као у

[4] Примера ради, марихуана је раније имала релативно мали проценат ТХЦ-а, до 3%. Примена савремених технологија у илегалном узгоју канабиса је напредовала, тако да данас проценат ТХЦ-а у марихуани може бити и преко 20%.

лабораторији, али се за узгој користи дневна сунчева светлост. Дакле, основна разлика између пластеника и лабораторије јесте то што се у лабораторијама канабис гаји у вештачки створеним условима, укључујући вештачко осветљење које је замена за дневну сунчеву светлост. У лабораторијама су такође и сви други климатски услови строго контролисани, што свакако утиче на количину и квалитет производа.

У последњој деценији готово у свим европским државама, а самим тим и у Србији, забележена је константна производња канабиса у затвореним просторима, и то због смањеног ризика од откривања (Bouchard, 2007, стр. 35), могућности контроле услова гајења, као и могућности добијања већих приноса и добијања финалног производа са већим процентом ТХЦ-а (Leggett, Pietschmann, 2008). Гајење канабиса у затвореним просторима омогућава контролу климатских услова, чиме се заобилазе све тешкоће које се могу јавити током гајења канабиса на отвореном простору, а то су најчешће: дневни природни циклуси, унакрсно опрашивање, мраз и томе слично. Унутрашњи узгој канабиса је могућ на свим местима где је доступан извор струје и воде. Резултати истраживања спроведених у Европи показују да укупна количина електричне енергије која се користи у производњи канабиса, од дана садње до дана жетве, износи отприлике 1 kw по граму произведеног сувог цветног материјала. Тамо где су доступни, подаци о потрошњи енергије могу бити корисни показатељи могуће производње незаконитог канабиса, а у криминалистичким истрагама они су индиција да се ради о илегалној производњи марихуане.[5] Како би избегле неконтролисану потрошњу електричне енергије, која је неопходна због производње вештачког светла за узгој канабиса у затвореном, а самим тим и високе рачуне за струју, криминалне групе се често одлучују за крађу електричне енергије. Управо због тога, као и због нестручног рада и лоших инсталација, у таквим лабораторијама неретко се дешавају пожари.

Унутрашњи узгој канабиса, за разлику од узгоја на отвореном, може имати шест приноса годишње. Сматра се да су технике гајења канабиса у лабораторијама напредовале у готово свим земљама Европе, због смањене могућности откривања од стране полиције, као и због могућности контролисања климатских услова који директно утичу на количину и квалитет производа. Неоспорно је да лоши климатски услови ограничавају илегалне произвођаче на отвореном да производе сталну и „сигурну“ количину током читаве године (Оташевић и Коларевић, 2020, стр. 18).

[5] Види шире: *EMCDDA Insights:* (2012). *Canabis Production and Markets in Europe*. Lisbon: European Monitoring Centre for Drugs and Drug Addiction, p. 32–36.

У Србији је у периоду од 1. јануара 2013. до 30. јуна 2019. године откривено 138 илегалних лабораторија за производњу канабиса (унутрашњи узгој). Највећи број њих откривен је у градским срединама (80,9%), док је у сеоским или приградским срединама откривено 19,1%. Највише лабораторија је откривено у Београду (37) (Оташевић et al., 2020, стр. 68). Резултат је очекиван и у складу је са Стратешком проценом јавне безбедности коју је израдило Министарство унутрашњих послова 2017. године. У поменутој процени наведено је: „Највише организованих криминалних група делује у Београду, доминантна криминална активност ових група је илегална производња и трговина опојним дрогама, којом се бави 86,2% регистрованих организованих криминалних група“ (Документ Министарства унутрашњих послова, Стратешка процена јавне безбедности, Београд 2017. године).

Међутим, обим илегалне производње канабиса у нашој земљи тренутно није могуће проценити. Доступни подаци о запленама канабиса су издељени, нестандардизовани и углавном научно неутемељени. Један од проблема у вези са процењивањем обима производње јесте велика разноликост у методама култивације, као и одсуство стандардизованих образаца за извештавање на националном нивоу. Међутим, треба напоменути да Србија није изузетак по овом питању, јер је због различитих метода гајења готово немогуће проценити глобалну производњу канабиса са прецизношћу која би била задовољавајућа за практичне потребе. Свакако, број откривених засада и лабораторија за производњу канабиса у Србији, који је у последњих пет година постао видљив пре свега захваљујући медијском извештавању, указује на то да заплењене количине канабиса више нису занемарљив део националне потражње.

Поступање приликом уласка и лабораторију или засад за производњу канабиса

Када полиција дође до сазнања о постојању илегалног засада или лабораторије за производњу канабиса, нужно је предузети мере у правцу откривања и лишења слободе лица која су учествовала у илегалној производњи, заустављања процеса производње и демонтирања и чишћења локације, ако су у питању лабораторије. Улазак у лабораторију или засад требало би реализовати у тренутку када се основано очекује да ће се у њима затећи и лица укључена у илегалну производњу. Ако се оперативним радом дође до сазнања о постојању илегалне лабораторије или засада, локацију је неко време могуће тајно осматрати и у погодном тренутку планирати упад и лишење слободе лица која су учествовала у илегалној производњи. Упад у празну (без људи) лабораторију, а посебно засад, касније може отежати доказивање шта се тачно на тој локацији производило и која су све лица учествовала у илегалној производњи. Упад треба да буде брз и ефикасан. У

случају сазнања да се поједине фазе процеса производње (гајење, сушење, дробљење, паковање и др.) одвијају на више локација, или да постоји више мањих лабораторија или засада, на све локације и објекте треба упасти истовремено. Све просторије треба ставити под контролу за најкраће могуће време како би се спречила паника међу затеченим лицима.

Након овладавања илегалном лабораторијом или засадом, полиција треба да изврши општи преглед локације и одреди и обезбеди шире место догађаја, како би се обухватили потенцијални путеви доласка и одласка учинилаца кривичних дела који су учествовали у илегалној производњи. Наведени поступци се предузимају с циљем спречавања трасолошког дефицита (недостатка трагова) и проналажења релевантних материјалних доказа.

Простор се мора пажљиво погледати и притом се треба кретати искључиво по чврстим површинама, односно избегавати ходање по влажним површинама, теписима и отирачима, као и по електричним, водоводним, гасним и другим инсталацијама.

Специфични трагови код засада канабиса

Засади биљне културе *Cannabis sativa* формирају се у природним условима погодним за развој биљака. За све варијанте засада карактеристично је што могу постојати само у одређено доба године, то јест само док траје вегетација. Могућност проналаска трагова током увиђаја зависи од много фактора, а вероватно је најважнија величина засада, јер већа површина подразумева већи број стабљика, више времена за саму садњу и узгој, а самим тим и веће шансе да лица која учествују у илегалној производњи оставе трагове.

Трагови остају од самог почетка неовлашћене производње, од првог крчења и припреме локације, па све до бербе, и касније сушења, дробљења и паковања психоактивних супстанци ради продаје. Имајући у виду да је тек засађеним садницама на отвореном простору потребно око десет недеља да би биле спремне за бербу, са сваким поновним доласком на парцелу остају нови трагови. На поједине трагове утичу атмосферске прилике, неке оштећује проток времена, неке нови трагови који настају у дуготрајном процесу производње, док поједини остају дуго нетакнути и на њих атмосферске прилике уопште не могу утицати.

Трагови на широј локацији места кривичног догађаја

Свакако да је најтеже доћи до сазнања где се засад налази. Када полиција дође до тог сазнања, у склопу криминалистичко-форензичке обраде лица места може се наћи велики број различитих трагова. Имајући у виду да се засади обично налазе на скривеним падинама, далеко од очију јавности, илегални произвођачи се обично одлуче да до парцеле исеку ниско и високо растиње и направе „прилазни

тунел“ кроз густо жбуње. На таквим местима треба прво тражити трагове сечења, а истовремено са њима и трагове газеће површине стопала. Хронолошки гледано, ако је подлога погодна за трагове газеће површине стопала, они ће настати истовремено са траговима сечења.

Трагови стопала могу бити видљиви и невидљиви (латентни) трагови. Када су у питању засади канабиса на отвореном, на лицу места ће се најчешће наћи видљиви трагови стопала, који у зависности од влажности подлоге могу бити површински или рељефни. Са криминалистичког становишта њихова вредност је подједнака, јер разлика између површинских и рељефних трагова постоји само у погледу треће димензије, у овом случају дубине. Трагови стопала, у овом случају трагови обуће, представљају елиминациону карактеристику, индивидуалне карактеристике јављају се услед хабања само код ношене обуће, јер том приликом долази до разних оштећења која имају индивидуални карактер. На основу таквих идентификационих карактеристика могуће је извршити идентификацију трагова обуће, али под условом да постоји неспорна обућа за упоређивање. Треба имати у виду да се у овом случају идентификује обућа која је оставила траг, а не особа која је носила обућу (Максимовић, Тодорић, 1995, стр. 312). Али без обзира на наведено, ови трагови су значајни са криминалистичког становишта јер могу да укажу на број лица која су боравила на засаду, што се одређује на основу различитих трагова стопала нађених на лицу места. Такође, они указују на правац кретања, висину особе и евентуално постојање патолошких карактеристика у ходу. Када су у питању засади канабиса, настајање трагова газеће површине стопала могу ометати трава и друго ниско растиње. Ипак, како су ти путеви изложени честим дејствима кретања, долази до огољавања земље и после извесног времена стварања погодних услова за настанак ових трагова.

Ако је коришћено возило, на прилазном путу према засаду настали су и трагови газеће површине пнеуматика, те приликом криминалистичко-форензичке обраде места догађаја треба обратити пажњу и на њих. Трагови газеће површине пнеуматика на оваквим локацијама су рељефни, у виду утиснућа у блату, земљи и прашини, али могу бити и површински, у виду отисака на некој равној површини попут папира, картона, стакла или тканине коју је пнеуматик прегазио. Трагови пнеуматика ће у близини засада увек бити бројни, јер се засад мора често обилазити. Они пружају довољно материјала за оперативни рад на трагању за возилом које их је оставило. На основу њих се може одредити врста возила, а самим тим и елиминисати велика група возила. Трагови газеће површине пнеуматика настају у широј зони места догађаја, а на њих се надовезују трагови газеће површине обуће ближе засаду.

Код засада канабиса постоји велика могућност проналаска трагова сечења. Употреба секире, мачете или другог сечива ради крчења пролаза прави „тунел“ који води до самих биљака, а оставља трагове сечења у виду микробразди на

дебљим гранама или стаблима жбуња и дрвенастог густиша. Ти трагови настају на самом почетку, при формирању засада, и дуго остају нетакнути. На њих не утичу други нови трагови јер је „тунел“ већ направљен, а незнатно утичу атмосферске прилике и донекле проток времена.

Задатак сваког сечива је да раздвоји један део на две целине. То раздвајање може бити потпуно, па се у том случају од једне целине добијају две, или непотпуно, када сечиво само засече предмет, али га не одвоји на два дела (на пример, засечена грана). Као резултат дејства сечива на пресечени или засечени предмет јављају се одрази микрорељефа, у виду великог броја паралелних бразди које служе као основа за идентификацију сечива (Максимовић, Тодорић, 1995, стр. 335). Идентификација се може извршити само када се пронађе инкриминисано сечиво, јер сами за себе трагови сечива не говоре ништа о идентитету учиниоца кривичног дела. Идентификација се заснива на три особине сечива које се преносе на спорни траг: опште карактеристике настале током производње, случајна обележја на оштрици настала током производње и случајна обележја на оштрици настала током употребе (Максимовић, Тодорић, 1995, стр. 405). Идентификацију сечива врши искључиво вештак трасолог на основу индивидуалних обележја сечива насталих током израде и употребе сечива. Ти трагови се након откривања морају означити и констатовати у записнику, а место налажења треба унети у скицу и фиксирати размерном фотографијом.

Тунел који се прави чишћењем високог и ниског растиња обично је узан, и лица која обилазе илегални засад морају се кроз њега провлачити. У тако узаном пролазу, где вире неправилно пресечени и оштри врхови грана (често са трњем), долази до трења и гребања, а самим тим и до директног контакта са кожом и гардеробом, услед чега на гранама, трњу и лишћу остаје биолошки материјал (крв, длаке, кожа, зној и излучевине), који је погодан за идентификацију оставиоца трага. Тродимензионалност посматрања лица места долази до изражаја управо овде у пролазу, односно тунелу. Траг крви на врховима огуљених грана може бити лако уочљив, и у оваквој средини обично ће бити сасушен. Молекуларно-генетичком анализом може се одредити ДНК профил и идентификовати оставилац трага. Међутим, ако не постоје неспорни узорци[6] за упоређивање, трагови крви пронађени на месту извршења кривичног дела могу послужити за елиминацију, у циљу сужавања круга осумњичених лица. Ако је крв људског порекла, лабораторијским испитивањима се свакако може одредити да ли припада мушкарцу, жени или детету, и о којој крвној групи се ради. За идентификацију учиниоца довољне су изузетно мале количине биолошког материјала. Примера ради, савременим методама за типизацију молекула ДНК могу се анализирати

[6] Неспорни узорак је биолошки материјал особе чији нам је идентитет познат.

узорци у којима се налази само сто пикограма материјала. За изузимање трага крви са места извршења кривичног дела довољна је крвна мрља величине једног квадратног милиметра.

Такође, на оштрим крајевима грана сасвим се лако уочавају влакна гардеробе, а где има влакана, врло често буде и тешко уочљива длака. Форензичком анализом косе или длаке можемо доказати постоји ли веза између осумњиченог и места догађаја. Неретко се деси да се приликом вршења увиђаја нађе и део тканине који је заглављен у расцепаној грани, или део откинуте гајке или алке, што може бити од изузетне користи за механоскопска уклапања и идентификовања предмета као што су торба, ранац, каиш и томе слично.

Трагови пронађени у пролазу готово увек потичу од лица која су активно учествовала у формирању засада. Карактеристике свих трагова који се могу наћи на прилазним путевима према парцели јесте да су они веома уочљиви и снажно међусобно повезани – ако пронађемо један од њих, пронаћи ћемо и све друге трагове који следе.

Трагови на парцели где је засад формиран

Након обраде шире локације места кривичног догађаја, за криминалистичко-форензичку обраду остаје парцела на којој су засађене биљке. Тај простор се мора пажљиво прегледати, при чему се треба кретати искључиво по чврстим површинама и избегавати ходање по водоводним и евентуално електричним инсталацијама. Потребно је измерити површину засада, број биљака, групације биљака (висина и друге уочене карактеристике), као и остале специфичности простора и опреме која је затечена на парцели. Важно је да биљке приближно исте висине и изгледа припадају истој групацији. Након тога, потребно је утврдити укупан број биљака у свакој од групација и укупан број биљака на целом засаду. Посебно се обележава и фотографише свака групација. Проналазак биљака различитих висина на једној парцели упућује на закључак да се ради о комерцијалним произвођачима чији је циљ неовлашћена продаја и остваривање профита по том основу. Они имају биљке различитих висина, које за сетву стижу у различито време, чиме се обезбеђује да увек постоји одређена количина готовог производа за илегално нарко-тржиште.

На самом засаду посебно треба обратити пажњу на све трагове биљног порекла, који су у криминалистичкој пракси, за разлику од других врста трагова, прилично запостављени. Трагови биљног порекла јављају се у виду трагова целих очуваних биљака, делова биљака и микротрагова биљног порекла. Данас многа истраживања у свету указују на значај палинологије[7] за откривање и доказивање

[7] Палинологија је наука која проучава полен и споре биљака (грч. *paline* – ситна прашина).

кривичних дела. Уопште, палинологија може се применити да би се (Mildenhall, 1990; Coyle, 2004; Szibor et al., 1998):

- повезао осумњичени са местом извршења кривичног дела или местом откривања кривичног дела;
- повезао предмет пронађен на месту извршења кривичног дела или месту откривања кривичног дела са осумњиченим;
- повезао предмет са места откривања кривичног дела са местом извршења кривичног дела;
- доказао или поништио алиби;
- сузио круг осумњичених лица;
- одредила промена локације предмета, укључујући дрогу;
- пружила информација о окружењу из ког је предмет дошао;
- пружила информација о географском пореклу предмета;
- пружила помоћ полицији при њиховим испитивањима.

Вредност форензичке палинологије огледа се у четири карактеристике полена и спора:

- микроскопске су величине;
- продукују се у огромном броју;
- могу се идентификовати на нивоу таксона;
- високо су резистентни и тешко се распадају.

Форензичка палинологија, дакле, користи микроскопске доказе који су резистентни на спољне утицаје и измештање са места догађаја. Неко ко је починио кривично дело врло лако може да, не знајући, са места догађаја понесе велики број спора и поленових зрна, који нису видљиви голим оком. Неке биљке које се опрашују помоћу ветра, као што је *Canabis sativa*, производе и до 70.000 поленових зрна по антери. Ако се ова биљка узгаја на великој површини, током периода цветања дневна количина ослобођених поленових зрна мери се у милионима (Faegri, 1989, p. 328). Током лета 1995. године на европској обали Медитерана регистрована је висока концентрација полена канабиса који је, ношен ветром, стигао из Марока (Dobrescu et al., 2011, p. 90).

Canabis sativa је двополна биљка и мушке јединке продукују полен. Да не би долазило до нежељене оплодње женских цветова и да би се наставила/повећала производња канабиноида, мушке биљке су у одгајалиштима ретке и чувају се у контролисаним условима (најчешће одвојено од женских јединки). Пошто се полен канабиса преноси ветром, он је лаган, малих димензија (око 15–20 μm) и без великих неравнина на површини (Wizenberg et al., 2020). Полен се идентификује микроскопским анализом помоћу светлосне и СЕМ микроскопије и помоћу њега се осумњичени може недвосмислено повезати са илегалним засадом канабиса, ако је засад у затвореном, док то ипак није случај са засадима који се налазе на отвореном. Трагове полена ћемо најчешће пронаћи на одећи, обући (везицама) и коси особа које су боравиле на илегалном засаду. У нашим условима

траговима полена се не придаје велика важност, па се самим тим не може стећи велико искуство у препознавању, изузимању и повезивању ових трагова са кривичним делом.

Свакако најзначајнији трагови биљног порекла јесу саме биљке пронађене у засаду. Оне се узоркују исецањем вршних делова биљака. Додатно је неопходно извршити исецање малог броја целих биљака (исецањем надземног дела биљке) како би се прорачунала нето маса сирове биљне материје у засаду. Сваки од изузетих узорака пакује се посебно у папирне кесе које се прописно обележавају одговарајућим идентификационим бројем.

Осталим биљкама нађеним у илегалном засаду потребно је одсећи надземне делове и потом их сушити на адекватно обезбеђеном простору. Осушени узорци се пакују у сигурносне кесе обележене налепницом са идентификационим бројем. Приликом паковања треба водити рачуна да остаци осушених биљака припадају изворној групацији. Уколико је изводљиво, остатке из једне групације треба паковати у једну кесу. Ако због пронађене количине то није могуће, те је за паковање остатка једне групације потребно више сигурносних кеса, на свакој кеси се мора означити којој групацији дати остаци припадају.

Поред побројаних трагова, у засаду на обрађеној земљи могу се наћи и трагови газеће површине стопала, али и идентификациони трагови, као што су трагови биолошког порекла и трагови папиларних линија. Без обзира на то што су биолошки трагови изложени дејству атмосферских прилика, они се могу наћи на дршкама ручног алата, а нарочито на храпавим, назубљеним деловима пластичних затварача или на храпавим дршкама амбалаже за воду. Трагови папиларних линија могу се веома успешно изазвати са глатких делова амбалаже за воду којом су биљке заливане. Такође, често се могу пронаћи и на бочицама разних других препарата за заштиту биљака, које су одбачене у непосредној близини засада. Отисци папиларних линија узимају се са свих делова опреме и алата. Уз остале методе фиксирања затечене ситуације на месту кривичног догађаја, обезбеђивање видео-записа требало би да буде део стандардне процедуре, посебно приликом узимања отисака папиларних линија, како би се могло доказати које лице је радило са којим алатом и апаратуром, а и ради лакшег давања исказа на суду. Није добро да касније, приликом давања исказа, лице које је пронашло и изузело отисак папиларних линија не може да се сети где је тачно отисак пронађен.

Поред пронађених биљака, потребно је одузети и комплетну документацију, белешке, нотесе, телефонске именике, мобилне телефоне, упутства за гајење, дневнике гајења, рачуне, поруџбине опреме, компјутере и томе слично.

Закључак

У позитивном законодавству Србије су производња, промет и поседовање канабиса у медицинске и „рекреативне“ сврхе забрањени. Имајући у виду да су научна истраживања у овој области на самом почетку и да она не пружају довољно уверљиве доказе да су препарати канабиса лековити, сматрамо да би легализација ове психоактивне супстанце у медицинске сврхе била преурањена, док би легализација у рекреативне сврхе имала последице по безбедност и здравље становништва.

У криминалистичкој пракси постоје три варијанте илегалног узгоја канабиса на отвореном: засади на отвореном, где се канабис узгаја самостално или у комбинацији са неком другом биљном културом, затим гајење у саксијама и гајење у пластеницима. Заједничка карактеристика све три варијанте засада јесте да се за узгој биљака искључиво користи дневна сунчева светлост, и биљке се могу гајити само у периоду вегетације. За разлику од плантажног гајења канабиса, лабораторијски узгој подразумева гајење у строго контролисаним условима, у којима се користи искључиво вештачко осветљење као замена за дневну сунчеву светлост, и гајење може да траје током целе године, независно од периода вегетације. Број откривених лабораторија и засада на нивоу целе Србије указује на пораст домаће производње. За успешно откривање и доказивање ове врсте криминалитета, као императив времена намеће се специјализација у раду полиције и правосудних органа, посебно у области трасологије. Наиме, у склопу криминалистичко-форензичке обраде на широј локацији места кривичног догађаја могу се пронаћи различити трагови који могу указивати на идентитет учесника илегалне производње. У пролазу према засаду најчешће се откривају трагови пнеуматика, на које се надовезују трагови газеће површине стопала и трагови сечења. У узаном пролазу према засаду обично се на врховима неправилно исечених грана могу пронаћи трагови влакана и различити биолошки трагови. На самом засаду посебну пажњу треба обратити на трагове биљног порекла, као што су саме биљке, трагови полена и спора биљака. Вредност полена и спора огледа се у чињеници да су микроскопске величине, да се продукују у огромном броју, да се идентификују на нивоу токсина, да су високо резистентни и да се тешко распадају. Веома су чести и трагови папиларних линија, који се могу пронаћи на деловима амбалаже за воду, бочицама од препарата који су коришћени за заштиту биљака, на деловима опреме и алату. Све ове трагове након откривања треба означити и правилно фиксирати.

Библиографија

1. Bloomer, J. (2008). *A political ecology approach to extra-legal rural livelihoods: a Lesotho-based case study of cultivation of and trade in cannabis*. PhD diss., Trinity College Dublin.
2. Васиљевић Продановић, Д. и Денчић, М. (2021). Друштвена реакција на употребу канабиса. *Безбедност* 63(3): 113–130.
3. Bouchard, M. (2008). Towards a realistic method to estimate cannabis production in industrialized countries. *Contemporary drug problems* 35(2–3): 291–320.
4. Gazdek, D. (2014). Marihuana u medicinske svrhe–javnozdravstveni aspekt. *Liječnički vjesnik* 136 (7–8): 192–199.
5. Dobrescu, E. M., Olteanu, I. G. and Sima, E. (2011). DEFINING THE ELEMENTS OF NEW SCIENTIFIC DISCIPLINES-PALYNOFORENSICS. *Int J Criminal Investig* 1: 87–94.
6. Insights, E. M. C. D. D. A. (2012). Cannabis production and markets in Europe. *Luxembourg: Office for Official Publications of the European Communities* .
7. Закон о психоактивним контролисаним супстанцама, „Службени гласник Републике Србије“, бр, 99/2010, 57/2018.
8. Leggett, T. and Pietschmann, T. (2008). Global cannabis cultivation and trafficking. *EMCDDA MONOGRAPHS* 189.
9. Максимовић, Р., Тодорић, У. (1995). *Криминалистчка техника*. Београд: Полицијска академија.
10. Mildenhall, D. C. (1990). Forensic palynology in New Zealand. *Review of palaeobotany and palynology* 64(1–4): 227–234.
11. Министарство унутрашњих послова. (2017). *Стратешка процена јавне безбедности*, Београд.
12. Otašević, B., Kolarević, D. and Radovanović, I. (2020). Clandestine drug production laboratories in Serbia. *Teme* (2020): 1125–1140.
13. Оташевиќ, Б., Атанасов, С. и Лабовиќ, Д. (2020). Распространетоста на илегалните лаборатории за производство на марихуана во Србија. *У седма меѓународна конференција, Општествените промени во глобалниот свет*, (ур. Кире Зафиров), (стр. 315–330). Штип: Правни факултет, Универзитет „Гоце Делчев“.
14. Оташевић, Б. и Коларевић, Д. Карактеристике илегалних лабораторија за производњу марихуане у Србији. *Безбедност* 62(2): 5–27.
15. Otasevic, B., Kolarevic, D., Cvorovic, D. and Atanasov, S. ILLEGAL CANNABIS GROWERS IN SERBIA. *Human Research in Rehabilitation*, 12(1): 66–73.
16. Правилник о о утврђивању списка психоактивних контролисаних супстанци, „Службени гласник Републике Србије“, бр. 73/2022.
17. Sznitman, S. R. and Lewis, N. (2018). Examining effects of medical cannabis narratives on beliefs, attitudes, and intentions related to recreational cannabis:

a web-based randomized experiment. *Drug and alcohol dependence* 185(2018): 219–225.
18. Szibor, R., Schubert, C., Schöning, R., Krause, D. and Wendt, U. (1998). Pollen analysis reveals murder season. *Nature* 395(6701): 449–450.
19. UNODC World Drug Report 2016. (2016). Приступљено 15.08.2022.: https://www.unodc.org/doc/wdr2016/WORLD_DRUG_REPORT_2016_web. pdf. 19.
20. UNODC World drug report 2021. (2021). Executive summary police implications, C Research.
21. Faegri, K., Kaland, E. P. and Krzywinski, K. (1989). Textbook of pollen analysis. No. Ed. 4. *John Wiley & Sons Ltd*.
22. Coyle, H. M. (2004). *Forensic botany: principles and applications to criminal casework*. crc press.
23. Wizenberg, S. B., Weis, E. A. and Campbell, G. L. (2020). Comparing methods for controlled capture and quantification of pollen in Cannabis sativa. *Applications in plant sciences* 8(9): e11389.

SPECIFIC INSIGHTS DURING THE DETECTION OF ILLEGAL PLANTATIONS FOR THE PRODUCTION OF CANNABIS

Abstract

Simple production procedures, detailed instructions and instructions that can be found on the Internet, as well as easily available necessary preparations and equipment, have influenced the increase of illegal cannabis production in Serbia. The daily discovery of highly profitable laboratories and open-air plantations point to the conclusion that domestic consumption is increasingly supplied from domestic production. However, due to the great diversity in cultivation methods, as well as the lack of standardized forms for reporting confiscation at the national level, it is not possible to estimate the volume of production with a precision that would be satisfactory for practical purposes. The aim of this work is to point out the importance of criminal-forensic processing of the scene of a criminal event where an illegal cannabis plant is located and the importance of material evidence in suppressing this type of crime.

Standardization of procedures, especially in the field of traceology and knowledge of specific traces in the illegal production of cannabis in the open, are necessary for making relevant conclusions and for successful criminal investigations. Tire tracks, footprints, cutting marks, various biological traces of human origin can be found in illegal cannabis plantations. However, attention should be paid to traces of plant origin such as the plants themselves, pollen and plant spores, which are unjustifiably neglected in criminal investigations. The forensic value of pollen and spores is reflected in the fact that they are microscopic in size, that they are produced in huge numbers, that they can be identified at the level of toxins, that they are highly resistant and that they are difficult to decompose.

The paper specifically describes traces characteristic of cannabis plants, their finding, fixing, sampling, packaging and sending to various laboratory expertise..

Keywords: *criminal investigations, plantation, biological traces, plants, pollen and spores*.

ПРИМЕНА СИМУЛАЦИЈА У КРИЗНИМ СИТУАЦИЈАМА

Александра Вуловић [1]

Апстракт

Технолошки развој претходних деценија имао је позитиван и негативан утицај на људско друштво. Позитиван утицај се пре свега огледа кроз значајан развој компоненти за рачунаре, што је утицало на могућност анализирања и симулирања сложених проблема, као што су симулације лета, биомеханика итд. Једна од области где су симулације пронашле примену јесте анализа различитих типова кризних ситуација. Кризне ситуације имају значајан утицај на квалитет живота људи и често остављају велику материјалну штету. Без обзира на тип кризне ситуације (природне катастрофе, вируси, климатске промене...), одлуке се доносе веома брзо и веома често без довољно улазних информација. Могућност симулације кризних ситуација омогућава припрему за боље реаговање кроз развој неопходних способности, како би се донеле што боље одлуке у стресним ситуацијама. Симулације кризних ситуација имитирају процесе стварног света и захтевају учешће свих страна које имају улогу у кризним ситуацијама, како би се на што реалнији начин дизајнирали и имплементирали одговарајући модели и на тај начин створили што реалнији симулациони модели. Поред теоријских информација о применама симулација у кризним ситуацијама, посебан осврт је дат на њихову тренутну примену у кризним ситуацијама које су изазване природним непогодама – земљотресима и поплавама. Ове кризне ситуације су изабране због учесталости последњих година на нашим просторима као и због чињенице да представљају веома велики ризик, како за јавну инфраструктуру, тако и за живот људи.

---

[1] Факултет инжењерских наука Универзитета у Крагујевцу, Сестре Јањић 6, 34000 Крагујевац, e-mail: aleksandra.vulovic@kg.ac.rs

Рад је настао у оквиру пројекта Фонда за науку Републике Србије „Идеје“ – Пројекат акцелерације иновација и подстицања раста предузетништва у Републици Србији – Management of New Security Risks – Research and Simulation Development – NEWSIMR&D, #7749151.

Кључне речи: безбедност, виртуелна реалност, земљотрес, поплаве, ризици, симулације.

Увод

Кризне ситуације настају као последице различитих фактора и могу утицати на здравље људи, као и на квалитет живота. Такође, ове ситуације често као последицу остављају велику материјалну штету. У циљу спречавања кризних ситуација, али и отклањања последица, неопходно је преузети превентивне мере. У кризне ситуације спадају: климатске промене, уништења изазвана природним катастрофама, избијање оружаних сукоба, ширења смртносних вируса итд. (Milić, Ranđelović and Devetak, 2019).

Оно што је карактеристично за све кризне ситуације јесте то што све захтевају да се одлуке доносе веома брзо, са ограниченим улазним информацијама и под знатно већим притиском него у нормалним околностима. Припрема за боље реаговање у кризним ситуацијама може се обавити коришћењем симулација које су, са развојем технологије, постале све сложеније. Последњих деценија, са развојем рачунара, симулације су пронашле примену у великом броју различитих области, међу којима су: аутомобилска индустрија (Weyer et al., 2016; Imran et al., 2017), здравствени сектор (So et al., 2019; Currie et al., 2020), биомеханика (Bulat et al., 2019; El Bojairami, El-Monajjed and Driscoll, 2020), симулације лета (Dehais et al., 2018), спорт (Wood et al., 2021), као и за симулације кризних ситуација.

Симулације се заснивају на примени математичких модела. Разликујемо детерминистичке и стохастичке моделе. Ова два типа модела се разликују по улазним и излазним параметрима. Код детерминистичких модела, улазни и излазни параметри су фиксни, док код стохастичких модела бар један од улазних или излазних параметара јесте непредвидљив и дефинише се преко вероватноће догађаја. И детерминистички и стохастички модели се даље деле на статичке и динамичке моделе. Код статичких модела, време се не разматра као параметар, док код динамичких модела веза између параметара, током времена, улази у обзир. Динамички модели се даље могу поделити на дискретне и континуалне моделе. Дискретни модел се тренутно мења, као одговор на одређене дискретне догађаје. Континуални модел се заснива на диференцијалним једначинама и покушава да квантификује промене у систему, током времена, док дискретни модел се тренутно мења као одговор на одређене дискретне догађаје (Soleymani Shishvan and Benndorf, 2017).

Симулација имитира процесе или системе у стварном свету, уз употребу модела, и омогућава анализу утицаја промена улазних информација на крајњи исход и помаже у процесу доношења одлука, кроз могућност да се примени за тестирање различитих сценарија (Jánošíková and Lacinák, 2019). У последње време, у циљу

још бољих резултата, симулације се комбинују са виртуелном реалношћу како би се пружило још боље искуство (Pfandler et al., 2017; Makransky et al., 2019).

Главне предости и недостаци симулација су приказани у табели испод (табела 1).

Предности симулација	Недостаци симулација
Симулација омогућава анализирање „шта ако“ сценарија.	Квалитет симулације зависи од квалитета модела и улазних информација.
Симулације су јефтиније у односу на реалне експерименте.	Захтева доста времена и труда да се постави одговарајућа симулација.
Омогућавају да се уоче најзначанији параметри одговора на кризне ситуације.	Људи могу другачије реаговати када се суоче са кризним ситуацијама у стварном свету у односу на кризне ситуације у симулацијама.
Помаже да се идентификују уска грла и укажу на сегменте где је потребно унапредити одговор на кризну ситуацију	Веома је тешко дефинисати потпуно реалистичну симулацију јер се правила дефинишу на основу претходних догађаја и доступних резултата истраживања.

Табела 1: Предности и недостаци симулација

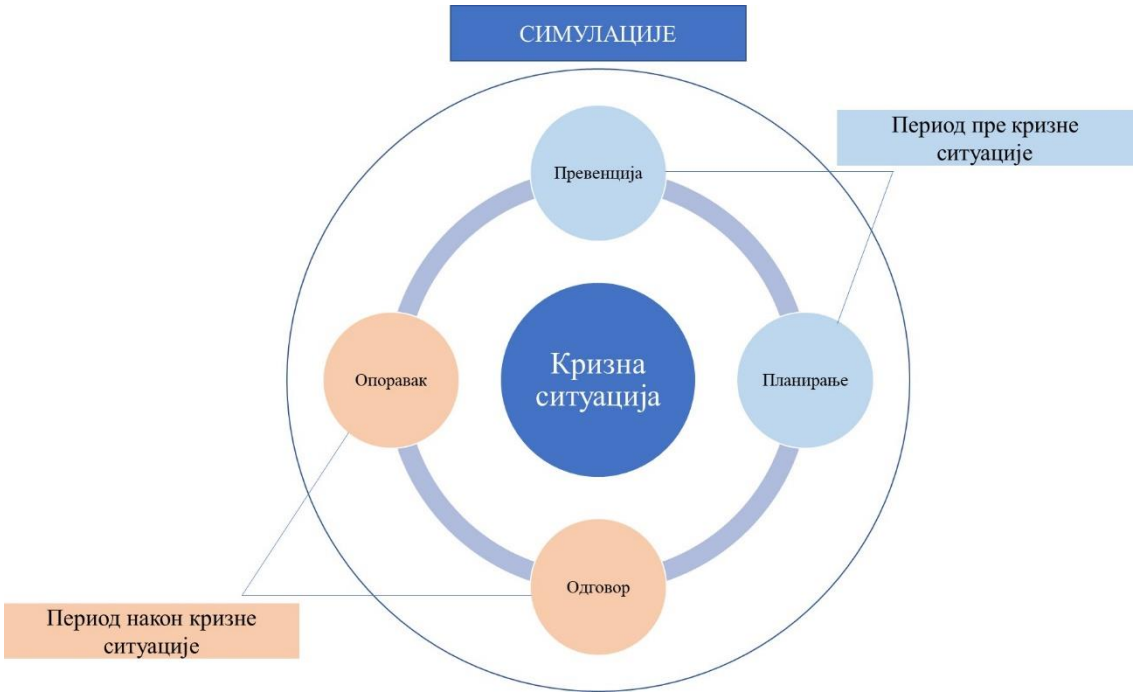
Симулације за кризне ситуације

Главни значај симулација је то што омогућавају да се искуси нека кризна ситуација пре него што она настане, и на тај начин пружају припрему и помажу у стварним кризним ситуацијама. Такође, сматра се да учење из неуспелих симулација позитивно утиче на спремност у будућности (Cesta, Cortellessa and Benedictis, 2014).

Сврха симулације у области кризних ситуација јесте да побољша спремност, планове реаговања, процедуре и системе за различите врсте опасности. Циљ симулације је да тестира применљивост дефинисаног плана за одређену кризну ситуацију и из тог разлога симулација треба да што реалније репрезентује физичку стварност. Симулације се могу користити за све фазе управљања кризним ситуацијама, што укључује обуку и осмишљавање одговора на догађаје, као што су природне катастрофе. Одговори се могу анализирати кроз симулацију указујући на потенцијалне проблеме, али и области у којима је потребна додатна

обука. На овај начин се обезбеђује да се грешке направе у безбедном окружењу и да се анализира њихов утицај пре кризног догађаја у стварном животу.

Један од постојећих предлога је да се модел који се користи за симулације састоји из четири фазе, које су подељене у две целине – период пре кризне ситуације и период након кризне ситуације (дијаграм 1). Период пре настанка кризног догађаја састоји се од фазе превенције и фазе планирања кризе. У овим фазама, симулације омогућавају: предвиђање тока кризе, анализу нових одговора на различите врсте догађаја, планирање ресурса, креирање сценарија, обуку особља за управљање кризним ситуацијама.



Дијаграм 1: Фазе кризних ситуација (извор: аутор)

Након појаве кризне ситуације прелази се на фазу одговора, а затим и на фазу опоравка. Симулације омогућавају да се боље предвиди развој кризних ситуација, јер развијени модел омогућава убрзану симулацију развоја ситуације. У оквиру фазе опоравка, симулације се могу користити за проналажење најефикаснијег решења, за опоравак од кризне ситуације, као што је реконструкција јавних простора и инфраструктуре (Jánošíková and Lacinák, 2019).

Приликом креирања симулација за кризне ситуације неопходно је водити рачуна о многим аспектима, као што су:

- Како побољшати вредности коју симулације кризних ситуација пружају за доношење одлука?
- У којим ће фазама управљања кризним ситуацијама симулације дати највећи допринос?
- Које методе треба изабрати за симулације одређених кризних ситуација?
- Како потврдити резултате симулација?
- Како повећати поверење у симулације и добијене резултате?

Примена симулација за кризне ситуације изазване природним непогодама

У овом делу рада биће приказане методе симулација које су нашле примену за анализу кризних ситуација, а које су изазване земљотресом или поплавом, као и симулацијама које се користе за обуку, у циљу боље реакције на ове кризне ситуације.

Земљотрес

Понашање људи током земљотреса и евакуације од великог је значаја за њихову безбедност, јер људи имају различите реакције на земљотресе.

Имерзивна виртуелна реалност је иновативна техника, која је успешно примењена за анализу људског понашања у условима као што је земљотрес. Применом ове методе могуће је извршити реалнију вежбу евакуације у случају земљотреса. Ово знатно смањује разлику која постоји између вежбе и реалне ситуације, јер виртуелна реалност омогућава учесницима да имају приступ реалнијим окружењима које рачунари креирају, укључујући и могуће опасности, које су реалне током земљотреса (Lovreglio et al., 2017; Feng et al., 2018).

Имерзивна виртуелна реалност је коришћена како за визуализацију земљотреса, тако и за саму обуку учесника. Када се користи само за визуализацију, циљ је направити што реалнији 3Д модел и искористити симулације да се укаже на пожељне начине понашања током земљотреса и тада нема интеракције између корисника и објеката у симулацији (Tarnanas and Manos, 2001; Sinha et al., 2012).

Уколико се користи за обуку учесника, циљ је креирати симулацију у којој ће се корисник кретати у виртуелним окружењима и манипулисати њима тако да избегне да буде повређен и на тај начин се припреми за земљотрес, који се може десити у будућности. Истраживање је показало да испитаници који су тренирали у виртуелном окружењу имају већу спремност приликом тестирања у новим ситуацијама. Испитаници су тренирани у просторијама које представљају

канцеларије, дневне собе и трпезарије, а затим су тестирани у просторијама истог типа, али са различитим распоредом намештаја (Li et al., 2017).

Имерзивна виртуелна реалност се може комбиновати са другим приступима, као што је анализа вербалног протокола, у циљу истраживања процеса доношења одлука у зградама током земљотреса и евакуације после земљотреса. Истраживање је спроведено на 87 људи у болници у Окланду (Нови Зеланд). Резултати овог истраживања су показали да се већина учесника, приликом доношења одлука, угледала на понашање других људи. Такође, резултати указују да ће већина људи препустити доношење одлука људима на лидерским позицијама (Feng et al., 2020). Поред комбиновања са анализом вербалног протокола, виртуелна реалност је последњих година комбинована и са игрицама и то тренутно представља један од најпопуларнијих приступа. Главни проблем са овим приступом јесте недостатак флексибилности како би се покрили корисници који имају различите циљеве обуке. Истраживање је показало да примена концепта учења на адаптивним играма може помоћи како би се прилагодила обука различитим типовима учесника (Feng et al., 2020).

Пружање интерактивне обуке, кроз игру, пружа знатно боље резултате у односу на традиционалне приступе обуке, који подразумевају читање безбедносних правилника или гледање видео-снимака. Иако је тешко закључити о реалном учинку ова два приступа у околностима које су симулиране, може се закључити да интерактивна обука треба да пружи боље резултате у случају стварног земљотреса, јер омогућава да учесник учи директно кроз вежбу.

Поплаве

Поплаве у урбаним подручјима представљају веома велики ризик, како за јавну инфраструктуру, тако и за живот људи. За планирање превенције поплаве и адаптације инфраструктуре неопходни су алати који могу да предвиде поплаву, као и количину воде која ће је изазвати.

Топографски подаци су кључни за моделирање поплава. Најчешћи приступи за моделирање су нумеричке симулације, процена података о падавинама, као и симулација поплава која се заснива на географском информационом систему (Wu et al., 2019, Samantaray et al., 2022). Неколико студија је развило методологије за конструисање 3Д виртуелне реалности за визуализацију опасности од поплава (Macchione et al., 2019; Wang et al., 2019).

Један од приступа за симулацију кретања воде јесте примена рачунске динамике флуида за тродимензионалну нумеричку симулацију. Главни недостатак овог приступа јесте време које је потребно за добијање резултата, уколико се симулира кретање воде на веома великој површини, као што је насеље или цео град. Једна од могућности да се убрза симулација јесте да се користи метода рачунске

динамике флуида која се заснива на честицама. Овај приступ омогућава ефикасан прорачун тока воде у урбаном окружењу (Winkler, Zischg and Rauch, 2018).

Једна од највећих природних катастрофа су бујичне поплаве, које захтевају брзу евакуацију и доводе до веома велике штете. У Јапану је спроведено истраживање, у коме је учествовало 103 студента, са циљем да се испитају два приступа за подстицање раних одлука о евакуацији из бујичних поплава. Први приступ се заснивао на пројектовању сигнализације ризика од бујичних поплава, док се други приступ заснивао на идеји да унапред одређени чланови заједнице започну евакуацију у препоручено време. За испитивање ефеката ових приступа коришћена је виртуелна реалност. Резултати су показали да су учесници истраживања добро реаговали на оба приступа и да се виртуелна реалност може користити за дизајнирање ефикасних приступа подстицања за рану евакуацију током различитих природних катастрофа (Fujimi and Fujimura, 2020).

Закључак

Симулација представља еволуцију модела и описује одређене феномене, процесе или системе у дефинисаном временском периоду. Рачунари новијих генерација пружају прилику за њихову примену у веома комплексним ситуацијама, које раније није било могуће анализирати. Симулације су пронашле примену у различитим индустријама где су омогућиле да се уштеди време приликом анализе „шта ако“ ситуација и анализе могућих решења. Једна од тих области је и област кризних ситуација, где је циљ да се што више смањи њихов утицај кроз њихово боље управљање. Симулације у области кризних ситуација могу да помогну у припреми за одговор приликом различитих катастрофа. Симулације криза и кризних ситуација захтевају окупљање великог броја заинтересованих страна, како би се на што реалнији начин дизајнирали и имплементирали одговарајући модели у различитим фазама кризних ситуација и на тај начин побољшали њихову поузданост, употребљивост и валидност. Такође, симулације су све више прихваћене у пракси, јер су резултати показали да имају практичну примену. На основу свега претходно поменутог, јасно се може закључити да коришћење симулација, у склопу припрема за одговор у кризним ситуацијама, може омогућити бољи одговор, а на тај начин и боље управљање кризама и кризним ситуацијама.

Поред теоријског описа симулација кризних ситуација, у раду је приказан и преглед примене симулација у кризним ситуацијама које се односе на земљотресе и поплаве, као и симулације које се користе за обуку, у циљу да се људи боље припреме на ове кризне ситуације. Описане методологије и добијени резултати отварају простор за развој и примену методологија како би се пружила адекватна обука људима како у Србији, тако и шире.

Библиографија

1. Bulat, M., Nuray, K. C., Yunus, Z. A. and Walter, H. (2019). Musculoskeletal simulation tools for understanding mechanisms of lower-limb sports injuries. *Current Sports Medicine Reports* 18(6): 210–216.
2. Cesta, A., Cortellessa, G. and De Benedictis, R. (2014). Training for crisis decision making – An approach based on plan adaptation. *Knowledge-Based Systems* 58: 98–112.
3. Currie, C. S., Fowler, J. W., Kotiadis, K., Monks, T., Onggo, B. S., Robertson, D. A. and Tako, A. A. (2020). How simulation modelling can help reduce the impact of COVID-19. *Journal of Simulation* 14(2): 83–97.
4. Dehais, F., Dupres, A., Di Flumeri, G., Verdiere, K., Borghini, G., Babiloni, F. and Roy, R. (2018). Monitoring pilot's cognitive fatigue with engagement features in simulated and actual flight conditions using an hybrid fNIRS-EEG passive BCI. 2*018 IEEE international conference on systems, man, and cybernetics (SMC)*. 544–549.
5. El Bojairami, I., El-Monajjed, K. and Driscoll, M. (2020). Development and validation of a timely and representative finite element human spine model for biomechanical simulations. *Scientific Reports* 10 (1): 1–15.
6. Feng, Z., González, V. A., Amor, R., Lovreglio, R. and Cabrera-Guerrero, G. (2018). Immersive virtual reality serious games for evacuation training and research: A systematic literature review. *Computers & Education* 127: 252–266.
7. Feng, Z., González, V. A., Mutch, C., Amor, R., Rahouti, A., Baghouz, A., Li, N. and Cabrera-Guerrero, G. (2020). Towards a customizable immersive virtual reality serious game for earthquake emergency training. *Advanced Engineering Informatics* 46: 101134.
8. Feng, Z., González, V. A., Trotter, M., Spearpoint, M., Thomas, J., Ellis, D. and Lovreglio, R. (2020). How people make decisions during earthquakes and post-earthquake evacuation: Using verbal protocol analysis in immersive virtual reality. *Safety science* 129: 104837.
9. Fujimi, T. and Fujimura, K. (2020). Testing public interventions for flash flood evacuation through environmental and social cues: The merit of virtual reality experiments. *International Journal of Disaster Risk Reduction* 50: 101690.
10. Imran, M., Kang, C., Hae Lee, Y., Jahanzaib, M. and Aziz, H. (2017). Cell formation in a cellular manufacturing system using simulation integrated hybrid genetic algorithm. *Computers & Industrial Engineering* 105: 123–135.
11. Jánošíková, M. and Lacinák, M. (2019). The Use Of Simulation In The Model Of Crisis Management. *CBU International Conference Proceedings*. 928–932.
12. Changyang, L., Liang, W., Quigley, C., Zhao, Y. and Yu, L. (2017). Earthquake safety training through virtual drills. *IEEE transactions on visualization and computer graphics* 23(4): 1275–1284.
13. Lovreglio, R., Gonzalez, V., Amor, R., Spearpoint, M., Thomas, J., Trotter, M. and Sacks, R. (2017). The need for enhancing earthquake evacuee safety by

using virtual reality serious games. *Lean & Computing in Construction Congress*.
14. Macchione, F,, Costabile, P., Costanzo, C. and De Santis, R. (2019). Moving to 3-D flood hazard maps for enhancing risk communication. *Environmental modelling & software* 111: 510–522.
15. Makransky, G., Mayer, E. R., Veitch, N., Hood, M., Christensen, B. K. and Gadegaard, H. (2019). Equivalence of using a desktop virtual reality science simulation at home and in class. *Plos one* 14(4): e0214944.
16. Milić, A., Ranđelović, A. and Devetak, M. S. (2019). Training of command staff for the use of units in crisis situations based on the application of modern technology. *Vojno delo* 71(5): 26–40.
17. Pfandler, M., Lazarovici, M., Stefan, P. and P., Weigl, Wucherer, M. (2017). Virtual reality-based simulators for spine surgery: a systematic review. *The Spine Journal* 17(9): 1352–1363.
18. Samantaray, S., Das, S. S., Sahoo, A. and Satapathy, D. P. (2022). Evaluating the application of metaheuristic approaches for flood simulation using GIS: A case study of Baitarani river Basin, India. *Materials Today: Proceedings* 61: 452–465.
19. Sinha, R., Sapre, A., Patil, A., Singhvi, A., Sathe, M. and Rathi, V. (2012). Earthquake disaster simulation in immersive 3d environment. *15th World conference on earthquake engineering*. 24–28.
20. So, H. Y., Chen, P. P., Kwok Chu Wong, G. and Tung Ning Chan, T. (2019). Simulation in medical education. *Journal of the Royal College of Physicians of Edinburgh* 49(1): 52–57.
21. Soleymani S., Masoud and Benndorf, J. (2017). Operational decision support for material management in continuous mining systems: from simulation concept to practical full-scale implementations. *Minerals* 7(7): 116.
22. Tarnanas, I. and Manos, C. G. (2001). Using virtual reality to teach special populations how to cope in crisis: the case of a virtual earthquake. *Studies in health technology and informatic*s 81: 495–501.
23. Wang, C., Hou, J., Miller, D., Brown, I. and Jiang, Y. (2019). Flood risk management in sponge cities: The role of integrated simulation and 3D visualization. *International Journal of Disaster Risk Reduction* 39: 101139.
24. Weyer, S., Meyer, T., Ohmer, M., Gorecky, D. and Zühlke, D. (2016). Future modeling and simulation of CPS-based factories: an example from the automotive industry. *Ifac-Papersonline* 49(31): 97–102.
25. Winkler, D., Zischg, J. and Rauch. W. (2018). Virtual reality in urban water management: communicating urban flooding with particle-based CFD simulations. *Water Science and Technology* 77(2): 518–524.
26. Wood, G., Wright, J. D., Harris, D., Pal, A., Franklin, C. Z. and Vine, J. S. (2021). Testing the construct validity of a soccer-specific virtual reality simulator using novice, academy, and professional soccer players. *Virtual Reality* 25(1): 43–51.

27. Wu, Y., Peng, F., Peng, Y., Kong, X., Liang, H. and Li, Q. (2019). Dynamic 3D simulation of flood risk based on the integration of spatio-temporal GIS and hydrodynamic models. *ISPRS International Journal of Geo-Information* 8(11): 520.

APPLICATION OF SIMULATIONS IN CRISIS SITUATIONS

Abstract

The technological development that happened in previous decades had positive and negative impacts on human society. The positive impact is primarily related to the development in the area of components for computers, which allowed for the possibility to analyze and simulate complex problems, such as flight simulations, biomechanics, etc. Simulations have found applications in many areas, such as for the analysis of crisis situations. Crisis situations arise due to various factors and significantly impact people's quality of life. Regardless of the type of crisis situation, decisions have to be made very quickly and very often without sufficient input information. The possibility of simulating crisis situations enables development of the necessary skills for adequate preparation, in order to make the best decisions in stressful situations. Simulations of crisis situations require inputs from all parties, that have a role in a crisis situation, in order to design and implement appropriate models as realistically as possible and thus create simulation models as realistic as possible. A particular focus is given to the current application of simulations in crisis situations, which are caused by natural disasters - earthquakes and floods.

Keywords: safety, virtual reality, earthquake, floods, risks, simulations.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

351.861(082)(0.034.2)
351.861:32(082)(0.034.2)
323.2(082)(0.034.2)

КОНФЕРЕНЦИЈА Стратешки и нормативни оквир Републике Србије за реаговање на савремене безбедносне ризике (2022 ; Београд)
Зборник радова са конференције Стратешки и нормативни оквир Републике Србије за реаговање на савремене безбедносне ризике [Електронски извор] / Божидар Бановић, Ненад Стекић (ур.). - Београд : Универзитет, Факултет безбедности, 2023 (Београд : Факултет безбедности). - 1 електронски оптички диск (CD-ROM) : текст ; 12 cm

Системски захтеви: Нису наведени. - Тираж 100. - Насл. са насловног екрана

ISBN 978-86-80144-60-3

1. Гл. ств. насл.
а) Национална безбедност -- Зборници б) Безбедносни сектор -- Зборници

COBISS.SR-ID 112749321

NEWSIMR&D

Funded by Science Fund of the Republic of Serbia

[ФБ]
УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ
UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

Подржао:

Фонд за науку
Републике Србије

ISBN: 978-86-80144-60-3