УДК:
351.862.4-028.45(497.11)
Прегледни рад
ДОИ: 10.5937/DB2502139A

Дипломатија и безбедност
Година 8.
Број 2/2025.
Стр. 139-157.

Јасмина Андрић[1]

ПОТРЕБА И МОГУЋНОСТ КРЕИРАЊА ТЕОРИЈСКОГ МОДЕЛА БЕЗБЕДНОСНЕ АНАЛИТИКЕ[2]

Сажетак

Безбедност је одавно, заслугом Копенхашке школе безбедности, са чисто војног, проширена на политички, економски, социјетални и еколошки сектор. Тај теоријски приступ Копенхашке школе безбедности прихваћен је у научној теорији безбедности, али и у пракси, односно службеним стратешким документима бројних држава света. Полазећи од достигнућа Копенхашке школе, а на основу опсежног истраживања и теорије и праксе, у овом раду се истражује могућност креирања теоријског модела безбедносне аналитике у Србији. Основни циљ истраживања примарно је утврђивање потреба и могућности креирања јединственог теоријског модела безбедносне аналитике, који сада функционише засебно, под називима обавештајна аналитика, криминалистичка аналитика и другим. Основна претпоставка у истраживању јесте: Постоји потреба и могућност да се обавештајна аналитика креира као јединствен теоријски модел, који би могао да се примени у пракси. У долажењу до циља и потврђивању хипотезе коришћене су научне методе, пре свега: анализа садржаја, компаративна метода и испитивање. Применом усмереног интервјуа обухваћено је око 50 експерата предметне проблематике. Основни закључак рада јесте: Теоријски модел безбедносне аналитике је могућ и треба га научно верификовати и проверити у пракси.

Кључне речи: *безбедност, безбедносна аналитика, теоријски модел безбедносне аналитике.*

---

[1] Јасмина Андрић, Војна академија, Универзитет одбране, Београд. andric.jasmina@yahoo.com

[2] Рад је настао у току истраживања за израду докторске дисертације ауторке овог рада на тему „Креирање теоријског модела безбедносне аналитике на примеру супротстављања тероризму“.

УВОД

Теорија и пракса безбедности усмеравају нас на сталну потребу за усавршавањем начина на који, пре свега, субјекти система националне безбедности треба да дођу до максимално поузданих и истинитих сазнања о свим појавама које ту безбедност угрожавају. Чињеница је да је безбедност заслугом Копенхашке школе безбедности (The Copenhagen School of Security Studies) одавно проширена са чисто војног на политички, економски, социјетални и еколошки сектор (Buzan et al., 1998; Wæver et al., 1993; Wæver, 2008). У овом раду, постављено је основно истраживачко питање: Да ли постојећи начин информисања стратешког нивоа управљања системом националне безбедности задовољава захтев за потпуним информацијама о безбедносним претњама у свим секторима безбедности?

Основно питање је централни проблем истраживања усмерило на безбедносну аналитику као практичну делатност у раду свих субјеката система безбедности Републике Србије. Суштину проблема истраживања чини потреба и могућност да се садашњи сепаратни модели аналитике (обавештајна, криминалистичка и друге) организационо и функционално групишу у јединствен модел безбедносне аналитике на стратешком нивоу управљања системом националне безбедности. Наиме, безбедносна аналитика код нас појављује се само у теорији, а у пракси егзистира сепаратно (Forca & Anočić, 2018: 41).

Предмет истраживања јесте теоријски модел безбедносне аналитике. Наиме, потреба и могућност креирања јединственог модела безбедносне аналитике прво треба да се теоријски утврде, како би се касније проверила могућност примене у пракси. У том смислу, чиниоци предмета истраживања јесу три врсте знања: 1) о безбедности, 2) о процедурама рада аналитичара и 3) о стандардима који се примењују.

У складу с наведеним, методолошки и сазнајно је коректно да се постојећи модел безбедносне аналитике подвргне критици, а затим идентификује и опише теоријски модел као побољшање стања.

КРИТИКА ПОСТОЈЕЋЕГ МОДЕЛА БЕЗБЕДНОСНЕ АНАЛИТИКЕ

Аналитика, као основни појам у овом раду, дефинисана је на следећи начин: „Аналитика је првенствено интелектуална, организована, систематска и сврсисходна делатност усмерена ка стицању релативно истинитих, релативно тачних и употребљивих сазнања о претежно актуелним збивањима у разним областима људског и друштвеног живота" (Termiz & Milosavljević, 2008: 141).

У складу са тим општим појмом аналитике, логично су изведени сви остали појмови, па и безбедносна аналитика. Као изведени појмови, они треба да садрже битна својства општег појма (аналитика) и специфичности подручја у којима се та аналитика одвија. Међутим, појам безбедносна аналитика фигурира само теоријски, односно у пракси постоје његови делови, познати под називима „обавештајна аналитика", „криминалистичка (криминалистичко-обавештајна) аналитика" и други. Навешћемо неколико примера из различитих извора:

- Обавештајна аналитика је специјализовани облик знања, активности и организације. Као знање, обавештајни подаци информишу лидере, на јединствен начин помажући њиховом просуђивању и доношењу одлука. Као активност, то је средство којим се прикупљају подаци и информације, утврђује њихова релевантност за одређено питање, они се тумаче ради одређивања вероватних исхода и дистрибуирају појединцима и организацијама који их могу користити, а који су иначе познати као „потрошачи обавештајних података". Обавештајна организација усмерава и управља овим активностима, како би што ефикасније оформила такво знање (Moore, 2007: 2),
- У Приручнику „Полицијско-обавештајни модел" МУП-а Србије стоји: „Криминалистичка анализа (не користи се термин аналитика, прим.аутора) је процесно и методолошки најкомплекснија функција криминалистичко- обавештајних послова, којом се прикупљени и обрађени подаци и информације обједињавају, структурирају, процењују и тумаче, на основу чега се изводе релевантни закључци и дају препоруке неопходне за доношење одлука за предузимање оперативно-полицијских активности" (MUP Srbije, 2016: 56),
- У документима МУП-а Хрватске, криминалистичко-обавештајна аналитика је дефинисана на следећи начин: „Криминалистичко-обавештајна аналитика је делатност прикупљања, обједињавања, прегледавања и анализирања података у свези криминалних активности те изналажења кључних значајки тих криминалних активности" (Kralj, 2019: 25).

За дефинисање појма „безбедносна аналитика" користићемо правила дефинисања, раније наведену дефиницију „аналитике" и ставове о безбедности. Основно правило дефинисања гласи „виши род и специфична разлика" (*genus proximum – differentia specifica*). Дакле, сваки појам приликом дефинисања, као врсту, везујемо за виши род, а онда наводимо разлику тог појма као врсте на вишем роду, од других врста појомова које виши род обухвата. Друго, дефинисати неки појам значи одредити се према његовим најбитнијим карактеристикама, односно утврдити садржај појма (Forca & Anočić, 2018: 225).

Повезујући наведено и друга правила дефинисања, као и полазну дефиницију „аналитике" (Termiz & Milosavljević, 2008: 141), за утврђивање појма „безбедносна аналитика" користимо следеће премисе:

- Безбедносна аналитика је посебна врста аналитике као родног појма, на шта упућује реч „безбедносна";
- Све врсте аналитике на родном појму аналитика, имају нешто заједничко за све врсте (род као целину), и своје специфичности по којима се безбедносна аналитика од њих разликује;
- Оно што је заједничко за све врсте аналитике (род као целину) јесте да је то интелектуална, организована, систематска и сврсисходна делатност усмерена на стицање релативно истинитих и употребљивих сазнања о актуелним збивањима у свом домену;
- Специфична разлика безбедносне аналитике од других врста аналитике на родном појму аналитика, јесте што се испољава у сфери безбедности као друштвеној делатности;
- Безбедност као област друштвеног живота од других области разликујемо по томе што се бави: 1) појавама које угрожавају безбедност – субјекат угрожавања, 2) субјектом безбедности, односно системом који се супроставља угрожавању и 3) објектом безбедности, односно оним што се брани/штити. Дакле, тиме се не бави ниједна друга врста аналитике (Forca, 2021: 114);
- Информације (знања) до којих дође безбедносна аналитика користе сви субјекти система безбедности за своје потребе.

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

Иако не постоји јединствена безбедносна аналитика, њене врсте (обавештајна, криминалистичка) имају нешто заједничко, а то је процес у коме се одвијају. Тај процес именован је као обавештајни циклус.

Обавештајни циклус је структурисана, систематска серија операција које имају за циљ да се надлежни обавештајни органи упознају са расположивим информацијама, одлуче које од њих су битне за конкретну операцију, установе који подаци им недостају и наложе органима или агенцијама да их прибаве, а затим да процесуирају те податке у обавештајне информације, пре него што их доставе корисницима (Forca & Anočić, 2018: 102).

Табела 1. *Различити погледи на садржаје обавештајног циклуса*

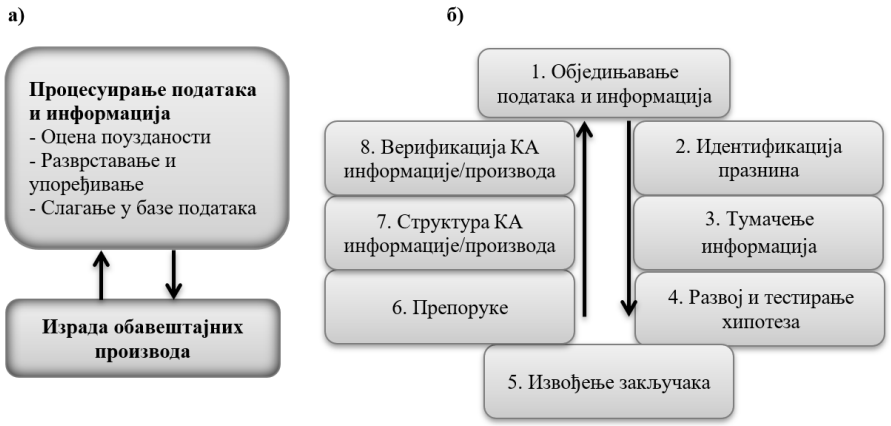
Аутор	Садржаји обавештајног циклуса
Шерман Кент (Sherman Kent)	1. Појава обавештајног проблема који заслужује пажњу стратегијских обавештајних служби
	2. Анализирање обавештајног проблема и детаљно сагледавање свих његових страна
	3. Разматрање расположивих и прикупљање нових података
	5. Критичко процењивање података
	5. Проучавање процењених података, као предуслов за одређивање хипотеза
	6. Прикупљање података у правцима који одређују постављене хипотезе
	7. Излагање – утврђивање веродостојности једне или више хипотеза
Лок Џонсон (Loch Johnson)	1. Планирање
	2. Прикупљање информација
	3. Обрада и анализирање информација
	4. Уступање информација
Лиза Кризан (Lisa Krizan)	1. Планирање и усмеравање
	2. Прикупљање информација
	3. Обрада информација
	4. Анализа информација и продукција
	5. Уступање (дисеминација) аналитичких производа
Вилијам Одом (William Odom)	1. Управљање обавештајним радом
	2. Прикупљање обавештајних информација
	3. Анализа
	4. Производња завршних обавештајних сазнања
	5. Уступање производа
	6. Повратна спрега
Младен Бајагић	1. Уочавање безбедносног проблема
	2. Утврђивање обавештајних потреба
	3. Преношење обавештајних захтева
	4. Иницијатива
	5. Планирање и организовање обавештајног истраживања
	6. Прикупљање сирових обавештајних информација
	7. Обрада информација
	8. Израда сирових обавештајних докумената
	9. Уступање завршних обавештајних докумената
	10. Техничка интерпретација завршних обавештајних сазнања
	11. Повратна спрега

Извор: Bajagić, 2009. (Допуњено од стране ауторке рада)

Иако је наведена дефиниција обавештајног циклуса јасна и прецизна, ипак, у пракси постоји мноштво приступа активностима (корацима) које тај циклкус чине (Табела 1).

Пажљивијим увидом у фазе обавештајног циклуса (Табела 1), уочавају се делови који се именују као: обрада и анализа информација, анализа, произвођење обавештајних сазнања, израда сирових обавештајних докумената и други. У пракси, ти називи су обједињени под појам аналитика, и они су на примеру војске и полиције приказани на Слици 1.

Слика 1. *Обавештајна (а) и Криминалистичка (б) аналитика*



Извор: Forca & Anočić, 2018.

На Слици 1 су приказана два приступа аналитици, која су суштински слична, а формално различита. Фрмална разлика је у броју и називу корака, а суштинска сличност јесте у крајњем производу – обавештајној информацији (производу).

Аналитиком се примарно баве аналитичари, било да је реч о војсци, полицији, службама безбедности или цивилном сектору (корпоративна безбедност). Процедуре рада аналитичара су сличне, а принципијелно могу се приказати као на Слици 2.

Слика 2. *ANACAPA метод криминалистичко-обавештајне аналитике*

Извор: Manojlović, 2008.

За општи приступ раду безбедносних аналитичара одабран је модел који се примењује у криминалистичко-обавештаној аналитици, али су сличне процедуре заступљене и у осталим врстама аналитике. Дакле, у бази података (стратегија) похрањено је мноштo информација, које се константно допуњују. Примењујући раније описан процес аналитике, аналитичари применом разноврсних метода (научних и практичних) развијају хипотезе (најмање две) за закључивање. У том процесу, највероватнија хипотеза се потврђује и доставља као закључак, односно обавештајни производ.

За ову прилику издвојићемо анализу рада оперативаца ЦИА (Централна информативна агенција САД), након терористичких напада Ал Каиде, 11. септембра 2001. године. Прво, извршена је компарација процедура рада оперативаца (аналитичара) и научног приступа и установљена готово подударност. Та подударност у даљој анализи показала је да оперативци (аналитичари) не познају довољно развијене научне методе (Colier, 2005: 7). Друго, дошло се до закључка да је амерички обавештајни систем изузетно разуђен (17.000 агенција само у полицији), те да га је потребно ефективније објединити (Racić, 2023: 231). У борби против тероризма морају се објединити подаци не само полиције, већ њих морају да достављају и службе безбедности и војска, и посебно цивилни сектор (Carter & Philips, 2015: 25).

Посебан аспект аналитике јесу стандарди који се примењују. У општем смислу посматрано, постоје међународни (ISO) и национални (СРБ) стандарди. Наравно, ти стандарди су развијени за одређене области безбедности, а не конкретно за безбедносну (обавештајну, криминалистичко-обавештајну) аналитику. Међу најпознатије ISO стандарде (Forca & Župac, 2025: 221) убрајају се:

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

На крају, како то истиче истраживач безбедности Марк Ловентал (Mark M. Lowenthal), поставља се питање: „Шта са обавештајном информацијом (производом)?" Ловентал даје и одговор, који гласи:

> Обавештајни аналитичари су људи стално ангажовани у својственој интелектуалној потрази за истином. Они покушавају да одгонетну загонетке, да разреше неизвесности, да открију природу и значење ствари које други желе да сакрију. Они морају имати читав интелектуални апарат који ће им помоћи да идентификују проблем, оцене делове које познају и установе шта не знају, да објасне оно што се дешава и да онда то искажу на начин да други – укључујући и оне који нису фамилијарни са њиховим техникама – могу разумети. (Lowenthal, 2022: 154)

Ако претходне ставове Ловентала применимо на домаћу праксу, доћи ћемо до следећих закључака: 1) Не постоји безбедносна аналитика, већ њене врсте, које дају сепаратне информације о појединим областима (одбрана-војска и криминал-полиција), 2) Поједини аспекти (сектори) безбедности уопште нису обухваћени безбедносном аналитиком, а то су, на пример, политичка безбедност, економска безбедност, еколошка безбедност.

Један од кључних критеријума за креирање теоријског модела безбедносне аналитике, управо, јесу и наведени закључци о функционисању безбедносне аналитике код нас.

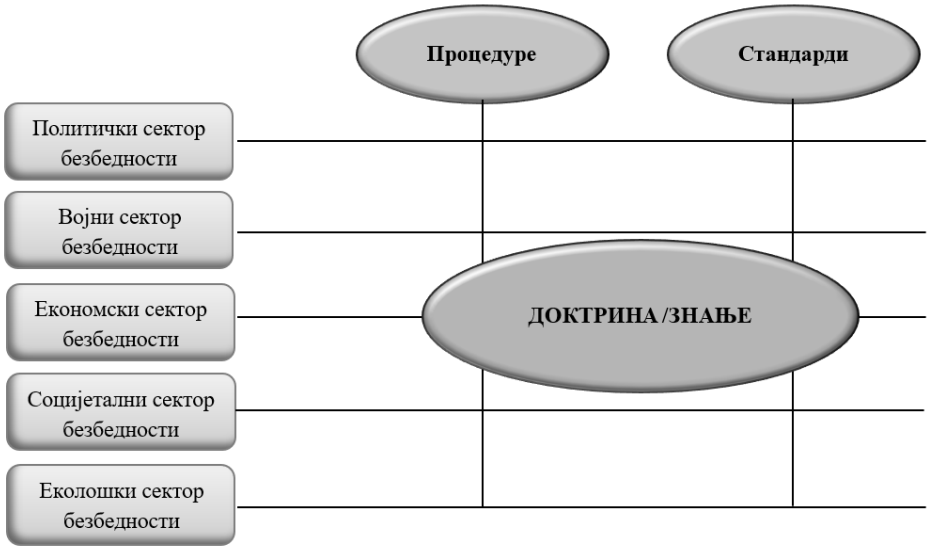
ТЕОРИЈСКИ МОДЕЛ БЕЗБЕДНОСНЕ АНАЛИТИКЕ

У класификацији модела, између осталих, разликујемо практичне, идеалне и идеализоване моделе. „Теоријски модел јесте идеализовани модел, који делом чине саставни делови праксе, а делом норме, захтеви, упутства и потребна знања усмерена ка пракси" (Miljević, 2007: 55).

У полазним активностима креирања теоријског модела безбедносне аналитике пошло се од става да је најприхватљивији превод енглеске речи

Intelligence, у суштини – знање. У том смислу, успостављен је теоријски модел безбедносне аналитике (Слика 3).

Слика 3. *Општа шема теоријског модела безбедносне аналитике*



Извор: Andrić & Tišma, 2021.

На слици 3 уочавамо да се ради о неколико врста (подручја) знања у моделу, као што су: безбедност, процедуре рада аналитичара и стандарди. На крају, говоримо о целокупном знању безбедносне аналитике, које се на националном нивоу успоставља као доктрина.

Знање о безбедности

С обзиром да су знања о процедурама рада аналитичара, као и знања о стандардима (у мањем обиму) позната, поставило се питање: Како формирати базу знања о безбедности? Уважавајући достигнућа домаће и стране теорије и праксе безбедности, била су могућа два приступа. Први приступ заступљен у домаћој теорији, кад је безбедност у питању, говори о компонентама безбедности које се именују као спољна, унутрашња и интегрална (Stajić, 2021: 44). Свакако да је то могући приступ анализи безбедности у држави (национална безбедност), али се, у крајњем, морају захватити сви сектори безбедности, што је приказано у другом приступу.

Други приступ јесте и у теорији и у пракси познати, признати и примењени у стратешким документима многих земаља, „секторски приступ без-

бедности" који је развила Копенхашка школа безбедности из састава Института за истраживање мира (The Copenhagen Peace Research Institute – COPRI). Наиме, истраживачи Копенхашке школе безбедности, у свом „секторском приступу", допринели су тзв. проширењу појма безбедност из чисто војног (агресија) у политички, економски, социјетални и еколошки сектор (Veljković, 2023: 71-83), Поред тога што су теоријски разрадили наведене секторе безбедности, истраживачи Копенхашке школе су посебно идентификовали кључне претње у тим секторима (Табела 2).

Табела 2. *Безбедносне претње у секторима безбедности*

Сектор	**Безбедносне претње**
Политички	Намерне, ненамерене, тероризам
Војни	Агресија, трка у наоружавању, војни притисци, војна интервенција
Економски	Бојкот, санкције, криминал, корупција
Социјетални	Страни утицај, губљење суверенитета, сецесионизам, депопулација, миграције
Еколошки	Природне претње, претње изазване деловањем човека са мањим последицама и претње изазване деловањем човека са значајним последицама

Извор: Forca, 2024.

Секторски приступ безбедности је широко прихваћен у научној теорији безбедности код нас и у свету (Vilijams, 2012: 45). С друге стране, увидом у бројна стратешка документа, пре свега у стратегије националне безбедности које, као документ, усваја већина држава света, евидентно је да се изазови, ризици и претње безбедности, углавном, класификују у складу са секторским приступом безбедности, како га је утврдила Копенхашка школа. Наведено је доказао професор Форца у својој монографији анализом 33 стратегије националне безбедности страних држава (Forca, 2022).

У анализи сектора безбедности мора се истаћи једна чињеница. Наиме, Копенхашка школа безбедности је као посебан сектор утврдила социјеталну безбедност. Дакле, у питању је однос према безбедности друштва (*societet*). Међутим, професор Форца истиче да је за теоријски модел битно шире утврдити тај сектор, именовати га као „друштвени", односно, осим друштва, фокусирати се и на појединца, чиме ће сектор бити комплетан (Forca, 2024: 16). Истини за вољу, треба истаћи да је и код самих истраживача Копенхашке школе безбедности постојало неслагање око детерминисања овог сектора. Тако, разликују се ставови водећег истраживача Бери Бузана

(Barry Buzan) и његових сарадника, као што су Оле Вивер (Ole Wæver) и Јап де Вилде (Jaap de Wilde) (Wæver et.al., 1993; Wæver, 2008).

Знање о процедурама рада аналитичара

Други аспект теоријског модела јесте знање о процедурама рада аналитичара. У оквиру овог аспекта, неопходно је утврдити: 1) Поступак рада, 2) Методе и технике које се користе у раду, као и 3) Потребна својства аналитичара.

Чињеница је да је овај део модела најпознатији у пракси, посебно по питању поступака рада аналитичара и метода и техника које примењују (Heuer & Pherson, 2016). Стога, пажњу заслужују ставови који се односе на карактер (квалитет) безбедносних аналитичара.

У теорији и пракси разних врста аналитике, као и општем приступу, наводи се мноштво карактеристика које треба да поседује квалитетан безбедносни аналитичар; оне се крећу у распону од неколико, до преко педесет (Forca & Anočić, 2018; Manojlović, 2008). Стога, у овом раду приказаћемо обједињен приступ који је дала група теоретичара (Табела 3).

Табела 3. *Компарација особина безбедносних аналитичара по различитим ауторима*

Аутор	Способности, вештине, атрибути и карактеристике	Окружење
Клозер, Клозер и Вир (Clauser, 2008; Clauser & Weir, 1976)	**Карактеристике**: способност расуђивања, тачност, интелектуална искреност, отвореност, скептицизам, дистанцираност, стрпљење, марљивост, истрајност, машта.	Национална безбедност
Катер и остали (Katter et al., 1979)	**Карактеристике**: разумевање сложених концептуалних модела, генерисање концептуалних модела, знање, памћење, ментална флексибилност.	Војска
Фишл и Гилберт (Fischl & Gilbert, 1983)	**Атрибути**: способност расуђивања на високом нивоу, индуктивно резоновање, интелектуална флексибилност, вештина писања, памћење, интелектуална радозналост, промишљеност, међуљудске вештине, мотивација за постигнућима, самодисциплина, истрајност.	Одбрана

Шнајдер (Schneider, 1995)	**Атрибути**: интелектуална радозналост, памћење, брза асимилација информација, упорност, расуђивање. **Карактеристике**: широк спектар интересовања, развијена истраживачка способност, искуство, иницијатива, самостално усмеравање, дисциплина, интелектуална храброст. **Вештине**: писање, вештина усмене комуникације.	Спровођење закона
Винг (Wing, 2000)	**Карактеристике**: знање, предвиђање, радозналост, иновација, одлучност, интуиција, логика, машта, надахнуће.	Војска
Мур, Кризан и Мур (Moore, Krizan, & Moore, 2005)	**Способности**: комуникација, сарадња, размишљање.	Национална безбедност
	Карактеристике: незасито радознао, самомотивисан, фасциниран енигмама, склоност ка АХА размишљању, радознало посматра, чита незасито, продуктивно опседнут, заузима различите перспективе, ствара креативне везе, разигран, смисао за хумор, способност чуђења, интензивно се концентрише, преиспитује конвенције.	
	Знање: циљ, заједница, политика, клијент, ресурси. **Вештине**: критичко резоновање, писменост, рачунарска писменост, изражавање, страни језик, истраживање, манипулација прикупљањем информација, пројектно управљање, визуелизација.	
Ален Д.М. (Allen, D. M. 2008).	**Атрибути**: редослед информација, препознавање образаца, резоновање.	Одбрана
	Вештине: техничка стручност, циљно знање, аналитичке технике, претраживачке и организационе способности, способност синтезе података, индуктивно резоновање, изражавање идеја.	
Куормби и Јанг (Quarmby & Young, 2010)	**Атрибути**: комуникација, сарадња, критичко размишљање, креативност.	Усаглашавање и управљање
	Вештине: Стручност, процесна експертиза, стручност у домену дисциплина, генеричко знање.	
Ричардс (Richards, 2010)	**Вештине**: критичко размишљање, креативност, расуђивање, комуникација.	Национална безбедност

Извор: Corkill, Cunow, Ashton & East, 2015

Знање о стандардима

Драгишић и Радивојевић на следећи начин дефинишу стандард:

> Стандард се, уопште, у документима међународних организација одређује као документ којим се утврђују захтеви, спецификације, правила, смернице или карактеристике које треба конзистентно следити и испунити да би се обезбедило да материјал, производи, процеси, услуге, заиста могу служити за њихову основну намену. Стандарди треба да се заснивају на провереним резултатима науке, технологије и искуства, а ради постизања оптималне користи за друштво. Стандардизација процеса описује успостављање скупа правила која регулишу начин на који људи у организацији треба да испуне одређени задатак или низ задатака. Тако, најпознатији вид стандарда су ISO (International Organization for Standardization) стандарди. У том смислу, стандардизација је оквир споразума кога се морају придржавати све стране у организацији (компанији) како би осигурале да се сви процеси који су повезани са стварањем (призводња, услуге и др) одвијају у складу са постављеним смерницама. (Dragišić & Radivojević, 2014: 12)

У складу с наведеним, а и општим стандардима у домену опште безбедности наведеним у претходном питању, чињеница је да се у свим секторима безбедности примењују ти општи и развијају посебни стандарди, које је готово немогуће све набројати. Разлог за ово је што је, на пример, за ISO стандард 27001 (безбедност информација), у Србији донето 25 националних (СРБ) стандарда (Forca & Župac, 2025: 234).

Уместо навођења мноштва стандарда у свим секторима безбедности, навешћемо пример Обавештајне заједнице САД.

Обавештајна заједница САД чини један шири концепт обавештајног рада, обухватајући различите специјализоване агенције које деле информације и сарађују са јасним циљем заштите националне безбедности САД. Она обухвата различите аспекте обавештајног рада, попут националне и војне безбедности, борбе против тероризма, контраобавештајне делатности и друге значајне области. Управо наведено представља пример безбедносне аналитике који покрива различите секторе безбедности, уз координацију рада различитих служби, организација и агенција са циљем заштите укупне безбедности на стратешком нивоу, поштујући њихове различите процедуре, али уз уважавање одређених стандарда (The Intelligence Comunity, 2024). На основу Закона о националној безбедности из 1947. године, са изменама Закона о реформи обавештајних служби и превенцији тероризма из 2004. го-

дине, као и других регулатива, Канцеларија директора националне обавештајне службе (ODNI) је даље кодификовала ове стандарде у Директиви обавештајних заједница (ICD) 203, Аналитички Стандарди. IC аналитички стандарди су установљени 2007. године, а ревидирани, ревалидирани и одобрени од стране DNI у јануару 2015. године. У овом документу наводи се следеће: Сви IC аналитички производи треба да буду у складу са следећих пет аналитичких стандарда, укључујући девет стандарда аналитичког заната:

а. Објективност: Аналитичари морају обављати своје функције са објективношћу и са свешћу о сопственим претпоставкама и размишљањима. Они морају користити технике размишљања и практичне механизме који откривају и ублажавају пристрасност. Аналитичари треба да буду опрезни у погледу утицаја постојећих аналитичких ставова или одлука и морају размотрити алтернативне перспективе и супротне информације. Анализа не треба да буде превише ограничена претходним закључцима када нови развој догађаја указују на потребу за изменама.

б. Независност од политичких разматрања: Аналитичке процене не смеју бити изобличене нити обликоване за промоцију одређеног циља, публике или политичког става. Аналитички судови не смеју бити под утицајем преференција за одређену политику.

в. Правовременост: Анализа мора бити достављена на време како би била корисна за кориснике. Аналитички елементи имају одговорност да буду стално свесни догађања од обавештајног интереса, активности и распореда корисника, као и обавештајних захтева и приоритета, како би пружили корисну анализу у правом тренутку.

г. Засновано на свим доступним изворима обавештајних информација: Анализа треба да буде снабдевена свим релевантним информацијама које су доступне. Аналитички елементи треба да идентификују и решавају кључне празнине у информацијама и сарађују са онима који прикупљају и достављају податке, како би развили стратегије приступа и прикупљања.

д. Спроводи и показује стандарде аналитичког заната, специфично: Исправно описује квалитет и кредибилитет основних извора, података и методологија: Аналитички производи треба да идентификују основне изворе и методологије на основу којих су закључци засновани, и користе дескрипторе извора у складу са lCD 206, Захтевима за изворе за објављене аналитичке производе, како би описали факторе који утичу на квалитет и кредибилитет извора. Ови фактори

могу укључивати тачност и потпуност, могуће порицање и обману, старост и актуелност информација, као и техничке елементе прикупљања, као и приступ изворима, валидацију, мотивацију, могућу пристрасност или стручност. Препоручује се коришћење резимеа извора, како је описано у lCD 206, како би се пружила свеобухватна процена снага и слабости извора и објаснило који су извори најважнији за кључне аналитичке закључке.

Исправно изражава и објашњава несигурности повезане са главним аналитичким закључцима: Аналитички производи треба да означе и објасне основу несигурности повезаних са главним аналитичким закључцима, специфично вероватноћу настанка догађаја или развоја, и поверење аналитичара у основу овог закључка. Степени вероватноће обухватају читав спектар, од слабих до готово извесних. Поверење аналитичара у процену или закључак може бити засновано на логици и доказима који их подржавају, укључујући количину и квалитет изворног материјала, и њихово разумевање теме. Аналитички производи треба да напомену узроке несигурности (нпр. тип, актуелност и количину информација, празнине у знању и природу проблема) и објасне како несигурности утичу на анализу (нпр. до ког степена и како закључак зависи од претпоставки). (The Intelligence Community, 2024)

Знање као доктрина

Целокупно знање о одређеној области, подразумевајући и практично поступање, у западној литератури се именује као доктрина (Forca, 2021: 164). У том смислу, Доктрина безбедносне аналитике јесте целовит национални приступ опису, објашњењу и предвиђању угрожавања безбедности државе и грађана Републике Србије. Представља скуп знања о секторимаа безбедности, као и скуп знања и вештина потребан за аналитику о процедурама, методима и техникама, као и стандардима. Доктрина је динамична и мења се у складу са променом теорије и праксе изазова, ризика и претњи, као и усавршавањем процедура и стандарда у аналитици.

Овако утврђена дефиниција Доктрине безбедносне аналитике, као знања, заслужује мало шире појашњење:

Прво, доктрина безбедносне аналитике је целовит национални приступ угрожавању безбедности државе и грађана, што подразумева аналитику на стратегијском (стратешком) нивоу у систему националне безбедности. Принциијелно посматрано, такве приступе имају савремене државе и интеграције.

На пример NIM (the National Intelligence Model) у Великој Британији (National Criminal Intelligence Service, 2000), или ECIM (the European Criminal Intelligence Model) у Европској унији, преко пројекта SOCTA (Andrić & Terzić, 2023). У складу са карактером аналитике у било којој области, тај приступ у доктрини безбедносне аналитике описује, објашњава и предвиђа изазове, ризике и претње (изворе, облике и носиоце) угрожавања националне безбедности. Описивање подразумева информације о томе шта се и када догодило. Објашњење подразумева виши ниво аналитике, тражењем разлога – како и зашто се нешто догодило или догађа. Највиши ниво доктрине безбедносне аналитике јесте предвиђање како и зашто ће се нешто (угрожавање) догађати у будућности. Такав целовит национални приступ доктрине треба да стратегијском нивоу управљања системом националне безбедности испоручи релевантан скуп информација о угрожавању државе и грађана, потребних за њихов рад, односно предузимање мера за супротстављање угрожавању безбедности.

Друго, да би стратегијском нивоу управљања системом националне безбедности испоручила релевантан скуп информација о угрожавању националне безбедности, доктрина безбедносне аналитике мора да обухвати изузетно широк и дубок скуп знања (сазнања), како научних (теоријских), тако и стручних (искуствених), којима располажу безбедносни аналитичари. Та знања (сазнања) примарно се односе на секторе безбедности, процедуре рада и примену стандарда (стандардизације) у раду аналитичара. Процедуре и стандарди најшире су познати у војној (обавештајној) и криминалистичкој аналитици. Стога, тежиште треба да се помера ка економској, социјеталној (Ilić-Krstić, 2016) и еколошкој безбедности (Office of EU, 2014; Forca, 2020: 75-101). Као таква, доктрина безбедносне аналитике је теорија струке, заснована на науци, што подразумева да се уобличава у скуп за одређено време релевантних упутстава, правила и процедура рада.

Треће, доктрина безбедносне аналитике није догма. Она је отворени систем знања и вештина, који се мења у складу са променом основних чинилаца на којима је заснована. Дакле, мења се у складу са теоријско-практичним променама у погледу сектора безбедности, процедура рада аналитичара и усвршавања и коришћења стандарда у том раду. У том смислу, поред развоја теорије и праксе на националном нивоу, доктрина безбедносне аналитике користи и најбоља страна искуства и решења.

ДЕЛИМИЧАН ПРИКАЗ РЕЗУЛТАТА ЕМПИРИЈСКОГ ИСТРАЖИВАЊА[3]

Истраживање за потребе креирања теоријског модела безбедносне аналитике имало је теоријски и емпиријски део. Теоријски део истраживања, применом компаративне методе и анализе садржаја, био је усмерен на критику постојеће праксе безбедносне аналитике. Такође, поједини аспекти теоријског истраживања, а пре свега национални и међународни модели аналитике, дали су импут за емпиријско истраживање. Емиријско истраживање реализовано је пре свега применом усмереног интервјуа. Критеријум за избор лица за усмерени интервју био је да се дуже време баве безбедношћу, посебно безбедносном аналитиком. Интервјуу је подвргнуто око 50 лица, која су се професионално бавила безбедношћу и безбедносном аналитиком (Табела 3).

Табела 4. *Структура испитаника који су учествовали у истраживању*

Категорија	**Подкатегорија**	**Проценат**
Пол	Мушки	96,43%
	Женски	3,57%
Старосна доб	До 40 година	7,14%
	Од 40 до 55 година	39,29%
	Преко 55 година	53,57%
Професионални статус	Активни припадници служби безбедности	21,43%
	Пензионисани припадници служби безбедности	46,43%
	Академска заједница	14%
	Корпоративна безбедност и менаџмент	14%
	Пословне/владине канцеларије	4,14%
Искуство у безбедносној аналитици	До 5 година	7,14%
	Од 5 до10 година	39,29%
	Преко 10 година	53,57%

[3] Истраживање је спроводено за потребе наведене докторске дисертације ауторке овог рада. С обзиром да докторска дисертација још није званично одбрањена, у овом раду се приказују само неки сегменти истраживања.

Образовање	Високо образовање/мастер	14,81%
	Докторске студије	85,19%
Институција у којој су се бавили безбедносном аналитиком	Војне институције (ВОА, ВБА, Генералштаб, Команде војске)	36,84%
	Полицијске/државне институције (МУП, БИА, РДБ Р. Српске)	31,58%
	Образовне/истраживачке институције (институт, факултет)	15,79%
	Остало (приватни сектор, канцеларија савета, кроз наставу)	15,79%
Период бављења аналитиком	Између 1992-1999.	12,50%
	Између 1999-2009.	25%
	Након 2009.	29,17%
	Комбиновано (више периода)	33,33%

Извор: Обрада ауторке

Усмерени интервју, поред основних података о испитаницима, обухватао је три сегмента предмета истраживања: 1) Безбедност, 2) Безбедносна аналитика и 3) Теоријски модел безбедносне аналитике. Из наведених разлога (види: фуснота 3), у овом раду ће се приказати само по један од кључних резултата.

- На питање да ли прихвата секторски приступ безбедности који је утврдила Копенхашка школа, већина од 69% испитаника је одговорила са „да". У постотку од 31%, испитаници сматрају да секторском приступу могу да се додају и: информациони, културолошки и технолошки сектор;
- Сви испитаници (100%) су става да у пракси не функционише безбедносна аналитика, већ обавештајна, криминалситичка и друге;
- На питање: Да ли сматрате да је потребно и могуће креирати јединствен теоријски модел безбедносне аналитике, испитаници су одговорили са: 1) Да, 82,12%, и 2) Не, или нисам сигуран, 17,8%.

ЗАКЉУЧАК

Безбедност је предуслов опстанка и развоја човечанства. Тако је записано у теорији, али и бројним службеним документима (стратегијама) држава света. Безбедност је давно из чисто војног (рат) проширена у друге секторе безбедности, као што су политички, економски, друштвени и еколошки. Чињеница је да угрожавање безбедности држава (национална безбедност) никада не долази само из једног сектора.

Спознаја о појавама угрожавања безбедности, код нас и у свету, дуго се исцрпљивала у домену обавештајне и криминалистичко-обавештајне аналитике, занемарујући остале секторе безбедности. Међутим, управо карактер угрожавања безбедности јесте вишеструко деловање претњи у истом тренутку, што захтева целовит приступ.

Безбедносна аналитика, као појам, појављује се само у теорији. Међутим, управо тренд поимања те аналитике у савременим државама света и њено целовито испољавање у пракси, намеће потребу да се стање те аналитике и код нас унапреди. Могуће унапређење стања у домену безбедносне аналитике, логично, креће од теоријског модела, преко његове научне верификације и примене у пракси. О томе недвосмислено говори и овај рад.

UDK:
351.862.4-028.45(497.11)

Review paper
DOI: 10.5937/DB2502139A

Diplomacy and Security
Volume VIII
Number 2/2025.
Page: 159-178.

Jasmina Andrić[1]

THE NEED AND POSSIBILITY OF DEVELOPING A THEORETICAL MODEL OF SECURITY ANALYTICS[2]

Abstract

Security, largely owing to the Copenhagen School of Security Studies, has long been expanded beyond its traditional military focus to encompass political, economic, societal, and environmental sectors. This theoretical approach has been widely accepted both in scientific security theory and in practice, that is, in the strategic documents of numerous states. Building upon the achievements of the Copenhagen School, and on the basis of extensive research into both theory and practice, this paper examines the possibility of developing a theoretical model of security analytics in Serbia. The primary aim of the research is to determine the need and feasibility of creating a unified theoretical model of security analytics, which currently functions in a fragmented manner under the designations of intelligence analytics, criminal analytics, and others. The central assumption of the study is that there exists both a need and a possibility to conceptualize intelligence analytics as a unified theoretical model applicable in practice. To achieve the research objective and verify the hypothesis, several scientific methods were employed, primarily content analysis, comparative method and empirical inquiry. Through directed interviews, approximately 50 experts in the relevant field were consulted. The main conclusion of the paper is that a theoretical model of security analytics is feasible and should be scientifically validated and empirically tested.

Keywords: *security, security analytics, theoretical model of security analytics.*

[1] Military Academy of the University of Defense, Belgrade. andric.jasmina@yahoo.com

[2] The paper was created during the research for the doctoral dissertation of the author of this paper on the topic "Creating a theoretical model of security analytics using the example of countering terrorism".

INTRODUCTION

Security theory and practice consistently point to the need for improving the methods by which actors within the national security system obtain the most reliable and accurate insights into phenomena that threaten security. It is a well-established fact that, owing to the Copenhagen School of Security Studies, the notion of security has expanded from a purely military domain to political, economic, societal, and environmental sectors (Buzan et al., 1998; Wæver et al., 1993; Wæver, 2008). This paper poses the core research question: Does the existing system of informing the strategic level of national security management adequately satisfy the need for comprehensive information on security threats across all sectors of security?

This central question directs the focus of the research toward security analytics as a practical activity performed by all actors within the security system of the Republic of Serbia. The essence of the research problem lies in examining the need and feasibility of consolidating the currently separate analytical models (intelligence, criminal, and others) into a unified model of security analytics at the strategic level of national security management. At present, security analytics appears only in theoretical discussions, whereas in practice it exists in a fragmented form (Forca & Anočić, 2018: 41).

The subject of the research is the theoretical model of security analytics. Specifically, the need and feasibility of creating a unified model of security analytics must first be established at the theoretical level, after which its practical applicability may be examined. In this respect, the key components of the research subject include three bodies of knowledge: (1) knowledge of security, (2) knowledge of analytical procedures, and (3) knowledge of applicable standards.

In line with the above, it is methodologically and epistemologically justified to subject the existing model of security analytics to critical examination, and subsequently to identify and describe a theoretical model that would improve the current state of affairs.

CRITIQUE OF THE EXISTING MODEL OF SECURITY ANALYTICS

Analytics, as the key concept in this paper, is defined as follows: "Analytics is primarily an intellectual, organized, systematic, and purposeful activity aimed at acquiring relatively truthful, relatively accurate, and usable knowledge about predominantly current developments in various spheres of human and social life" (Termiz & Milosavljević, 2008: 141).

In accordance with this general concept of analytics, all derivative concepts, including security analytics, are logically derived. As derivative concepts, they should contain the essential properties of the general notion of analytics, as well as the specific features of the domain in which the analytic activity is carried out. However, the term security analytics appears only at the theoretical level; in practice, it exists only in the form of its constituent parts, commonly referred to as "intelligence analytics," "criminal (or criminal-intelligence) analytics," and others. A few examples from various sources illustrate this point:

> • Intelligence is a specialized form of knowledge, an activity, and an organization. As knowledge, intelligence informs leaders, uniquely aiding their judgment and decision-making. As an activity, it is the means by which data and information are collected, their relevance to an issue established, interpreted to determine likely outcomes, and disseminated to individuals and organizations who can make use of it, otherwise known as "consumers of intelligence." An intelligence organization directs and manages these activities to create such knowledge as effectively as possible (Moore, 2007:2),
> • In the *Police Intelligence Model* handbook of the Ministry of the Interior (MUP) of Serbia, it is stated: "Criminal analysis (the term analytics is not used, author's note) is the most procedurally and methodologically complex function within criminal-intelligence work. It is a process through which collected and processed data and information are consolidated, structured, evaluated, and interpreted, on the basis of which relevant conclusions are drawn and recommendations are provided that are necessary for decision-making related to operational police activities" (MUP Srbije, 2016: 56),
> • In the documents of the Croatian Ministry of the Interior, criminal-intelligence analytics is defined as follows: "Criminal-intelligence analytics is an activity involving the collection, consolidation, review, and analysis of data related to criminal activities, and the identification of key features of such criminal activities" (Kralj, 2019: 25).

To define the concept of security analytics, we rely on the standard rules of definition, the previously cited definition of analytics, and established understandings of security. The fundamental rule of definition is the principle of "proximate genus and specific difference" (*genus proximum – differentia specifica*). Thus, in defining any concept as a species, we first connect it to a higher-order genus and then specify the characteristics that distinguish it from other species encompassed by that genus. Moreover, defining a concept requires identifying its essential characteristics, that is, determining its conceptual content (Forca & Anočić, 2018: 225).

By connecting these definitional rules with the initial definition of "analytics" (Termiz & Milosavljević, 2008: 141), we employ the following premises in determining the concept of "security analytics":

- Security analytics is a specific type of analytics as a higher-order concept, which is indicated by the qualifier security;
- All types of analytics share certain common characteristics derived from the genus analytics, as well as their own specificities that distinguish them from one another; security analytics is differentiated by its domain;
- What is common to all forms of analytics (as a genus) is that they constitute an intellectual, organized, systematic, and purposeful activity aimed at acquiring relatively truthful and usable knowledge about current developments within their respective domains;
- The specific difference that sets security analytics apart from other forms of analytics is that it operates within the sphere of security as a social activity;
- Security, as a domain of social life, differs from other domains in that it concerns: (1) phenomena that threaten security – the subject of threat; (2) the subject of security, that is, the system that counters threats; and (3) the object of security, meaning that which is defended or protected. No other analytic field addresses all three of these dimensions (Forca, 2021: 114);
- The information (knowledge) generated by security analytics is used by all entities within the security system for their respective needs.

In line with the above, the nominal definition of the concept (syntagm) security analytics is as follows: Security analytics is a distinct type of analytics manifested as an intellectual, organized, systematic, goal-oriented, and purposeful activity aimed at acquiring relatively truthful and usable knowledge about the subject of threat, the subject of security, and the referent object of security – knowledge necessary for the functioning of the actors within the security system.

Although a unified form of security analytics does not currently exist, its constituent branches (such as intelligence and criminal analytics) share common features, the most important of which is the process through which they unfold. This process is traditionally referred to as the intelligence cycle.

The intelligence cycle is a structured, systematic series of operations aimed at enabling the competent intelligence bodies to familiarize themselves with the available information, determine which of these are relevant to a specific operation, identify which data are lacking and instruct the competent bodies or agencies to obtain them, and subsequently process these data into intelligence information before delivering them to end users. (Forca & Anočić, 2018: 102)

Although the above definition of the intelligence cycle is clear and precise, in practice there exists a wide range of approaches to the activities (steps) that constitute the cycle (Table 1).

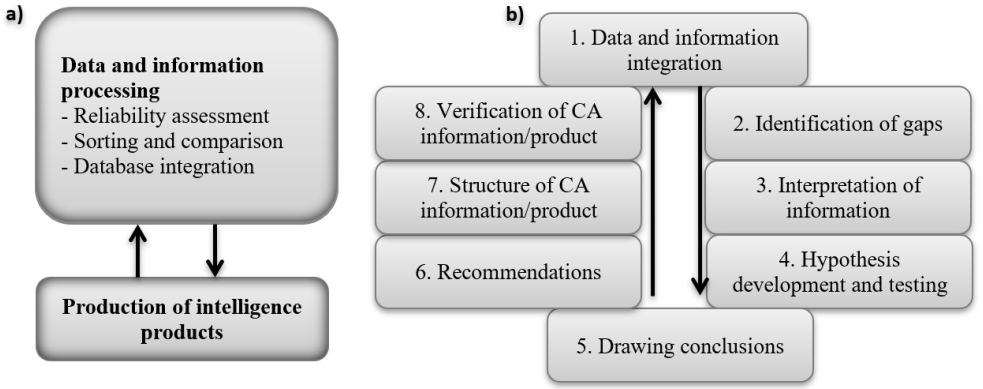
Table 1. *Different Perspectives on the Components of the Intelligence Cycle*

Author	Components of the Intelligence Cycle
Sherman Kent	1.Emergence of an intelligence problem warranting the attention of strategic intelligence services 2.Analysis of the intelligence problem and detailed examination of all its aspects 3.Consideration of available data and collection of new data 4.Critical evaluation of data 5.Study of evaluated data as the basis for formulating hypotheses 6.Collection of data directed by established hypotheses 7.Presentation – determining the credibility of one or more hypotheses
Loch Johnson	1. Planning 2. Information collection 3. Information processing and analysis 4. Information sharing
Lisa Krizan	1. Planning and direction 2. Information collection 3. Information processing 4. Information analysis and production 5. Dissemination of analytical products
William Odom	1. Intelligence Management 2. Intelligence Collection 3. Analysis 4. Production of Final Intelligence Findings 5. Product Release 6. Feedback
Mladen Bajagić	1. Identifying a security problem 2. Determining intelligence needs 3. Communicating intelligence requirements 4. Initiative 5. Planning and organizing intelligence research 6. Collecting raw intelligence 7. Processing information 8. Producing raw intelligence documents 9. Providing final intelligence documents 10. Technical interpretation of final intelligence findings 11. Feedback

Source: M. Bajagić, 2009 (expanded by the author of this paper).

A more detailed examination of the stages of the intelligence cycle (Table 1) reveals components designated as information processing and analysis, analysis, production of intelligence knowledge, preparation of raw intelligence documents, and others. In practice, these terms are consolidated under the concept of analytics, demonstrated in the context of the military and the police in Figure 1.

Figure 1. *Intelligence (a) and Criminal (b) Analytics*

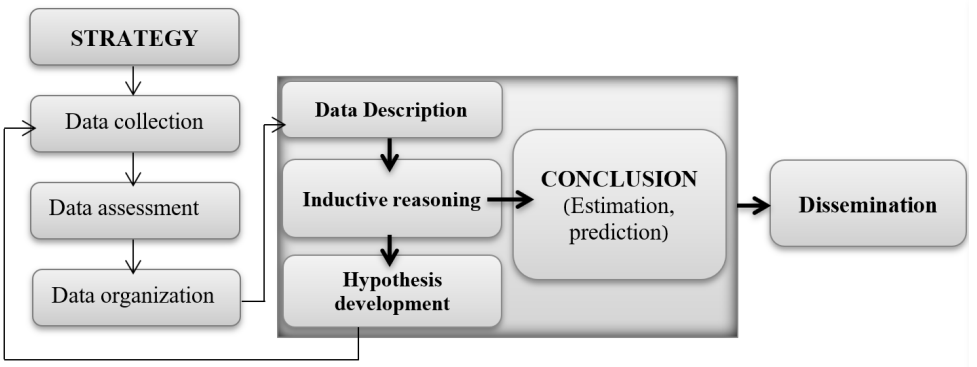


Source: Forca & Anočić, 2018

Figure 1 presents two approaches to analytics that are substantively similar but formally different. Their formal difference lies in the number and naming of steps, while their substantive similarity lies in the nature of the final outcome – an intelligence product.

Analytics is primarily carried out by analysts, whether within the military, police, security services, or the civilian (corporate security) sector. The work procedures of analysts are similar and can, in principle, be illustrated as shown in Figure 2.

Figure 2. *The ANACAPA Method of Criminal-Intelligence Analytics*



Source: Manojlović, 2008

For a general approach to the work of security analysts, the model used in criminal-intelligence analytics has been selected, although similar procedures are present in other types of analytics. Databases (strategic repositories) contain large volumes of information that are continuously updated. Applying the previously described analytic process, analysts employ various methods (scientific and practical) to develop hypotheses (at least two) as a basis for inference. In this process, the most probable hypothesis is confirmed and submitted as a conclusion, that is, as an intelligence product.

For the purposes of this discussion, we highlight the analysis of the work of CIA operatives following the al-Qaeda terrorist attacks of 11 September 2001. First, a comparison of operative (analyst) procedures and scientific methodology revealed an almost complete correspondence. However, further analysis showed that operatives (analysts) were insufficiently familiar with well-developed scientific methods (Collier, 2005: 7). Second, it was concluded that the U.S. intelligence system is extremely fragmented (17,000 agencies in the police alone), requiring more effective integration (Racić, 2023: 231). The fight against terrorism requires the integration not only of police data, but also data provided by security services, the military, and especially the civilian sector (Carter & Phillips, 2015: 25).

An important aspect of analytics is the set of standards applied in practice. Generally speaking, there are international (ISO) and national (SRB) standards. These standards have been developed for particular domains of security, though not specifically for security (intelligence or criminal-intelligence) analytics. Among the most well-known ISO standards (Forca & Župac, 2025: 221) are:

- Quality management: ISO 9001
- Environmental protection: ISO 14001
- Energy management: ISO 50001
- Occupational health and safety: ISO 45001, SCC
- Information security: ISO 27001
- Crisis and emergency management: ISO 22301
- Risk management: ISO 31000, and numerous others.

Ultimately, as security researcher Mark M. Lowenthal points out, the question arises: "What about the intelligence (product)?" Lowenthal provides an answer, which reads:

> Intelligence analysts are people constantly engaged in an inherent intellectual pursuit for the truth. They try to unravel puzzles, resolve uncertainties, and discover the nature and meaning of things that others want to hide. They must have an entire intellectual apparatus to help them identify the problem, evaluate the pieces they know and determine what they don't know, explain what is happening, and then express it in a way that others - including those not familiar with their techniques - can understand. (Lowenthal, 2022: 154)

If Lowenthal's positions are applied to the domestic context, several conclusions emerge:

1. Security analytics, as such, does not exist; instead, only its constituent types operate separately, providing fragmented information (e.g., defense–military and crime–police sectors).
2. Several sectors of security are not included in any analytic framework, such as political security, economic security, and environmental security.

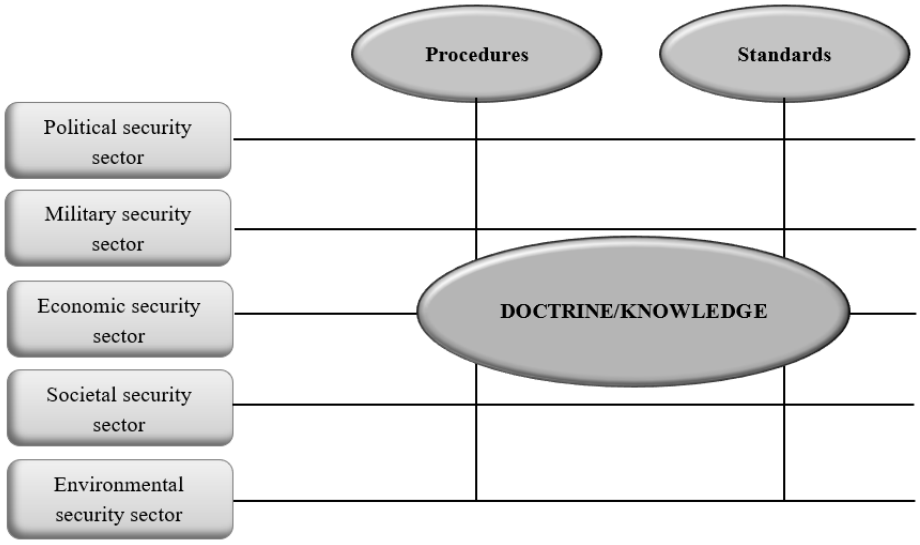
These conclusions regarding the functioning of security analytics in Serbia constitute one of the key criteria for developing a theoretical model of security analytics.

THEORETICAL MODEL OF SECURITY ANALYTICS

In model classification, among others, practical, ideal, and idealized models are distinguished. "A theoretical model is an idealized model, partially composed of elements drawn from practice, and partially of norms, requirements, instructions, and the knowledge necessary to guide practice" (Miljević, 2007: 55).

In the initial phase of developing a theoretical model of security analytics, the starting point was the premise that the most appropriate translation of the English term intelligence is, in essence, knowledge. Based on this understanding, a theoretical model of security analytics was established (Figure 3).

Figure 3. *General scheme of the Theoretical Model of Security Analytics*



Source: Andrić&Tišma, 2021

In Figure 3, we see that there are several types (areas) of knowledge in the model, such as: security, analyst work procedures and standards. Finally, we are talking about the overall knowledge of security analytics, which is established at the national level as a doctrine.

Knowledge About Security

Given that knowledge about analyst work procedures, as well as knowledge about standards (to a lesser extent) are known, the question arose: How to form a knowledge base about security? Taking into account the achievements of domestic and foreign security theory and practice, two approaches were possible. The first approach represented in domestic theory, when it comes to security, talks about the components of security that are named as external, internal and integral (Stajić, 2021: 44). This is certainly a possible approach to analyzing security in a state (national security), but ultimately, all security sectors must be covered, as shown in the second approach.

The second approach is known in theory and practice, recognized and applied in the strategic documents of many countries, the "sectoral approach to security" developed by the Copenhagen School of Security within the Copenhagen Peace Research Institute (COPRI). Namely, the researchers of the Copenhagen School of Security, in their "sectoral approach", contributed to the so-called expansion of the concept of security from a purely military (aggression) to the political, economic, societal and environmental sectors (Veljković, 2023: 71-83). In addition to theoretically developing the aforementioned security sectors, the researchers of the Copenhagen School specifically identified key threats in these sectors (Table 2).

Table 2. *Security Threats in Security Sectors*

Sector	Security threats
Political	Intentional, unintentional, terrorism
Military	Aggression, arms race, military pressure, military intervention
Economic	Boycott, sanctions, crime, corruption
Societal	Foreign influence, loss of sovereignty, secessionism, depopulation, migration
Ecological	Natural threats, threats caused by human activities with minor consequences and threats caused by human activities with significant consequences

Source: Forca, 2024

The sectoral approach to security is widely accepted in the scientific theory of security in our country and in the world (Williams, 2012: 45). On the other hand, by looking at numerous strategic documents, primarily national security strategies that are adopted as documents by most countries in the world, it is evident that security challenges, risks and threats are generally classified in accordance with the sectoral approach to security, as established by the Copenhagen School. This was proven by Professor Forca in his monograph analyzing 33 national security strategies of foreign countries (Forca, 2022).

In analyzing the security sector, one fact must be emphasized. Namely, the Copenhagen School of Security has established societal security as a separate sector. Therefore, it is a matter of attitude towards the security of society. However, Professor Forca points out that for the theoretical model it is important to define this sector more broadly, to name it as "social", that is, in addition to society, to focus on the individual, which will make the sector complete (Forca, 2024: 16). Truth be told, it should be noted that even among the researchers of the Copenhagen Security School there was disagreement about the determination of this sector. Thus, the views of the leading researcher Barry Buzan and his associates, such as Ole Wæver and Jaap de Wilde, differ (Wæver et.al., 1993; Wæver, 2008).

Knowledge of Analyst Work Procedures

Another aspect of the theoretical model is knowledge of analyst work procedures. Within this aspect, it is necessary to determine: 1) Work procedure, 2) Methods and techniques used in the work, and 3) Required analyst characteristics.

The fact is that this part of the model is the most well-known in practice, especially regarding analysts' work procedures and the methods and techniques they apply (Heuer & Pherson, 2016). Therefore, attention is paid to the views related to the character (quality) of security analysts.

In the theory and practice of various types of analytics, as well as the general approach, a multitude of characteristics are listed that a quality security analyst should possess; they range from a few to over fifty (Forca & Anočić, 2018; Manojlović, 2008). Therefore, in this paper we will present a unified approach provided by a group of theorists (Table 3).

Table 3. *Comparison of Security Analyst Characteristics by Different Authors*

Authors	Abilities, Skills, Attributes and Characteristics	Environment
(Clauser, 2008; Clauser & Weir, 1976)	**Characteristics**: Reasoning ability, Accuracy, Intellectual honesty, Open-mindedness, Scepticism, Detachment, Patience, Diligence, Perseverance, Imagination	National Security
(Katter et al., 1979)	**Characteristics** : Comprehend complex conceptual models, Generate conceptual models, Knowledge, Memory, Mental flexibility	Military
(Fischl & Gilbert, 1983)	**Attributes**: High level reasoning ability, Inductive reasoning, Intellectual flexibility, Writing skill, Memory, Intellectual curiosity, Deliberateness, Interpersonal skill, Achievement motivation, Self-discipline, Perseverance	Defence
(Schneider, 1995)	**Attributes** : Intellectual curiosity, Memory, Rapid assimilation of information, Tenacity, Make judgements **Characteristics**: Broad range of interests, Developed research ability, Experience, Initiative self-direction, Disciplined, Intellectual courage Skills: Writing skills, Oral communication skills	Law Enforcement
(Wing, 2000)	**Characteristics**: Knowledge, Foresight, Curiosity, Innovation, Determination, Intuition, Logic, Imagination, Inspiration	Military
(Moore, Krizan, & Moore, 2005)	**Abilities**: Communication, Collaboration, Thinking **Characteristics**: Insatiably curious, Self-motivated, Fascinated by puzzles, Exhibit AHA thinking, Observes voraciously, Reads voraciously, Fruitfully obsessed, Takes variable perspectives, Makes creative connections, Playful, Sense of humour, Sense of wonder, Concentrates intensely, Questions convention **Knowledge**: Target, Community, Policy, Customer, Resource **Skills**: Critical reasoning, Literacy, Computer literacy, Expression, Foreign Language, Research, Information gathering manipulation, Project management, Visualization	National Security
(Allen, 2008)	**Attributes** : Information ordering, Pattern recognition, Reasoning **Skills**: Technical expertise, Target knowledge, Analytic techniques, Search and organisational abilities, Ability to synthesise data, Inductive reasoning, Express ideas	Defence
(Quarmby & Young, 2010)	**Attributes** : Communication, Collaboration, Critical thinking, Creativity **Skills**: Subject expertise, Procedural expertise, Disciplinary expertise, Generic knowledge	Compliance& Governance
(Richards, 2010)	**Skills**: Critical thinking, Creativity, Judgement, Communication	National Security

Source: Corkill, Cunow, Ashton, & East, 2015

Knowledge of Standards

Dragišić and Radivojević define a standard as follows:

> A standard is generally defined in documents of international organizations as a document that establishes requirements, specifications, rules, guidelines or characteristics that should be consistently followed and fulfilled to ensure that materials, products, processes, services can truly serve their primary purpose. Standards should be based on proven results of science, technology and experience, in order to achieve optimal benefits for society. Process standardization describes the establishment of a set of rules that regulate the way in which people in an organization should complete a certain task or series of tasks. Thus, the most well-known type of standard is the ISO (International Organization for Standardization) standards. In this sense, standardization is a framework of agreement that all parties in an organization (company) must adhere to in order to ensure that all processes related to creation (production, services, etc.) take place in accordance with the established guidelines. (Dragišić & Radivojević, 2014: 12)

In accordance with the above, as well as the general standards in the domain of general security mentioned in the previous question, the fact is that in all security sectors these general and specific standards are applied and developed, which are almost impossible to list. The reason for this is that, for example, for the ISO standard 27001 (information security), 25 national (SRB) standards have been adopted in Serbia (Forca & Župac, 2025: 234).

Instead of listing a multitude of standards in all security sectors, we will cite the example of the US Intelligence Community.

The United States Intelligence Community constitutes a broader concept of intelligence activity, encompassing various specialized agencies that share information and cooperate with the explicit objective of safeguarding U.S. national security. It covers multiple dimensions of intelligence work, including national and military security, counterterrorism, counterintelligence activities, and other areas of critical importance. This framework represents a clear example of security analytics that spans different security sectors, involving the coordinated efforts of diverse services, organizations, and agencies aimed at protecting overall security at the strategic level, while respecting their distinct procedures and simultaneously adhering to established standards (The Intelligence Community, 2024).

Pursuant to the National Security Act of 1947, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004, as well as other relevant regulations, the Office of the Director of National Intelligence (ODNI) further

codified these standards in Intelligence Community Directive (ICD) 203, Analytic Standards. The IC Analytic Standards were originally established in 2007 and subsequently revised, revalidated, and approved by the Director of National Intelligence in January 2015. This document stipulates the following: all IC analytic products must comply with five analytic standards, which incorporate nine standards of analytic tradecraft:

a. Objective: Analysts must perform their functions with objectivity and with awareness of their own assumptions and reasoning. They must employ reasoning techniques and practical mechanisms that reveal and mitigate bias. Analysts should be alert to influence by existing analytic positions or judgments and must consider alternative perspectives and contrary information. Analysis should not be unduly constrained by previous judgments when new developments indicate a modification is necessary.

b. Independent of political consideration: Analytic assessments must not be distorted by, nor shaped for, advocacy of a particular audience, agenda, or policy viewpoint. Analytic judgments must not be influenced by the force of preference for a particular policy.

c. Timely: Analysis must be disseminated in time for it to be actionable by customers. Analytic elements have the responsibility to be continually aware of events of intelligence interest, of customer activities and schedules, and of intelligence requirements and priorities, in order to provide useful analysis at the right time.

d. Based on all available sources of intelligence information: Analysis should be informed by all relevant information available. Analytic elements should identify and address critical information gaps and work with collection activities and data providers to develop access and collection strategies.

e. Implements and exhibits Analytic Tradecraft Standards, specifically:

(1) Properly describes quality and credibility of underlying sources, data, and methodologies: Analytic products should identify underlying sources and methodologies upon which judgments are based, and use source descriptors in accordance with ICD 206, Sourcing Requirements for Disseminated Analytic Products, to describe factors affecting source quality and credibility. Such factors can include accuracy and completeness, possible denial and deception, age and continued currency of information, and technical elements of collection as well as source access, validation, motivation, possible bias, or expertise.

> Source summary statements, described in ICD 206, are strongly encouraged and should be used to provide a holistic assessment of the strengths or weaknesses in the source base and explain which sources are most important to key analytic judgments.
> (2) Properly expresses and explains uncertainties associated with major analytic judgments: Analytic products should indicate and explain the basis for the uncertainties associated with major analytic judgments, specifically the likelihood of occurrence of an event or development, and the analyst's confidence in the basis for this judgment. Degrees of likelihood encompass a full spectrum from remote to nearly certain. Analysts' confidence in an assessment or judgment may be based on the logic and evidentiary base that underpin it, including the quantity and quality of source material, and their understanding of the topic. Analytic products should note causes of uncertainty (e.g., type, currency, and amount of information, knowledge gaps, and the nature of the issue) and explain how uncertainties affect analysis (e.g., to what degree and how a judgment depends on assumptions). (The Intelligence Community, 2024)

Knowledge as Doctrine

The totality of knowledge relating to a specific field, including practical action, is referred to in Western literature as doctrine (Forca, 2021: 164). In this sense, the Doctrine of Security Analytics constitutes a comprehensive national approach to describing, explaining, and forecasting threats to the security of the state and the citizens of the Republic of Serbia. It represents a body of knowledge concerning security sectors, as well as a set of knowledge and skills required for analytics related to procedures, methods, techniques, and standards. Doctrine is dynamic in nature and evolves in accordance with changes in both theory and practice concerning challenges, risks, and threats, as well as through the continuous refinement of analytical procedures and standards.

The definition of the Doctrine of Security Analytics thus established, understood as knowledge, deserves a more detailed clarification.

First, the Doctrine of Security Analytics represents a comprehensive national approach to threats to the security of the state and its citizens, which implies analytics conducted at the strategic level within the national security system. In principle, such approaches are characteristic of contemporary states and supranational integrations. Examples include the National Intelligence Model (NIM) in the United

Kingdom (National Criminal Intelligence Service, 2000), or the European Criminal Intelligence Model (ECIM) within the European Union, implemented through the SOCTA (Serious and Organised Crime Threat Assessment) project (Andrić & Terzić, 2023). In line with the nature of analytics in any field, this doctrinal approach to security analytics describes, explains, and forecasts challenges, risks, and threats to national security, including their sources, forms, and actors.

Description entails information about what occurred and when it occurred. Explanation involves a higher level of analysis, seeking to identify the reasons: how and why something occurred or is occurring. The highest level of the Doctrine of Security Analytics is forecasting how and why security threats will occur in the future. Such a comprehensive national doctrinal approach should provide the strategic level of governance of the national security system with a relevant set of information on threats to the state and its citizens, necessary for decision-making and for undertaking measures aimed at countering security threats.

Second, in order to provide the strategic level of governance of the national security system with a relevant body of information on threats to national security, the Doctrine of Security Analytics must encompass an exceptionally broad and in-depth body of knowledge, both scientific (theoretical) and professional (experiential), possessed by security analysts. This knowledge primarily relates to security sectors, operational procedures, and the application of standards (standardization) in analytical work. Procedures and standards are most widely developed and recognized in military (intelligence) and criminal intelligence analysis. Accordingly, the analytical focus should increasingly shift toward economic, societal (Ilić-Krstić, 2016), and environmental security (Office of the EU, 2014; Forca, 2020: 75–101). As such, the Doctrine of Security Analytics constitutes a theory of professional practice grounded in science, which implies that it is articulated as a set of, for a given period, relevant guidelines, rules, and operational procedures.

Third, the Doctrine of Security Analytics is not a dogma. It is an open system of knowledge and skills that evolves in accordance with changes in the fundamental factors upon which it is based. Consequently, it adapts to theoretical and practical developments concerning security sectors, analysts' working procedures, and the refinement and application of standards in analytical practice. In this context, alongside the development of theory and practice at the national level, the Doctrine of Security Analytics also draws upon best practices and solutions from international experience.

PARTIAL PRESENTATION OF EMPIRICAL RESEARCH RESULTS

The research conducted for the purpose of developing a theoretical model of security analytics comprised both a theoretical and an empirical component. The theoretical component of the study, employing the comparative method and content analysis, was focused on critically examining existing practices in security analytics. In addition, certain aspects of the theoretical inquiry, most notably national and international analytical models, provided the impetus for the empirical research.

The empirical research was conducted primarily through the use of directed interviews. The criterion for selecting participants for the interviews was their long-term professional engagement in the field of security, with particular emphasis on security analytics. Approximately 50 individuals were interviewed, all of whom were professionally involved in security and security analytics (Table 3).

Table 4. *Structure of Respondents who Participated in the Survey*

Category	Subcategory	Percentage
Gender	Male	96,43%
	Female	3,57%
Age	Up to 40 years	7,14%
	From 40 to 55 years	39,29%
	Over 55 years	53,57%
Professional status	Active security service members	21,43%
	Retired security service members	46,43%
	Academia	14%
	Corporate security and management	14%
	Business/government offices	4,14%
Experience in security analytics	Up to 5 years	7,14%
	From 5 to 10 years	39,29%
	Over 10 years	53,57%
Education	Higher education/Masters	14,81%
	Doctoral studies	85,19%

Institution where they worked as security analysts	Military institutions (VOA, VBA, General Staff, Army Commands)	36,84%
	Police/state institutions (MUP, BIA, RDB R. Srpska)	31,58%
	Educational/research institutions (institute, faculty)	15,79%
	Other (private sector, council office, teaching)	15,79%
Period of working as an analyst	Between 1992-1999	12,50%
	Between 1999-2009	25%
	After 2009	29,17%
	Combined (multiple periods)	33,33%

Source: Editing by the author

The directed interview, in addition to collecting basic demographic and professional data on the respondents, encompassed three segments of the research subject: (1) Security, (2) Security Analytics, and (3) the Theoretical Model of Security Analytics. For the reasons stated above (see footnote 3), this paper presents only one key result from each segment.

- In response to the question of whether they accept the sectoral approach to security as established by the Copenhagen School, a majority of respondents (69%) answered in the affirmative. By contrast, 31% of respondents believe that the sectoral approach could be expanded to include additional sectors, such as information, cultural, and technological security.
- All respondents (100%) expressed the view that, in practice, security analytics as such does not function, whereas intelligence analytics, criminal intelligence analytics, and other forms do.
- In response to the question of whether it is necessary and possible to develop a unified theoretical model of security analytics, respondents answered as follows: (1) Yes, 82.12%; and (2) No, or unsure, 17.8%.

CONCLUSION

Security is a prerequisite for the survival and development of humanity. This premise is firmly established both in theoretical discourse and in numerous official state documents and strategies worldwide. Security has long since expanded beyond a purely military (wartime) concept to encompass other security sectors, such as political, economic, societal, and environmental security. It is a well-established fact that threats to state security (national security) never originate from a single sector alone.

For a considerable period, understanding security threats, both domestically and internationally, was largely confined to the domains of intelligence and criminal intelligence analytics, while other security sectors were neglected. However, the very nature of contemporary security threats involves the simultaneous operation of multiple threats across different sectors, which necessitates a comprehensive and integrated approach.

As a concept, security analytics appears primarily in theory. Nevertheless, prevailing trends in how this form of analytics is understood and comprehensively applied in practice by contemporary states underscore the need to improve the state of security analytics in the domestic context as well. Logically, such improvement in the field of security analytics must begin with the development of a theoretical model, followed by its scientific validation and practical application. This paper provides clear and unequivocal support for that proposition.

REFERENCE LIST

Andrić, J., (2024). *Usmereni intervju za istraživanje po temi doktorske disertacije* „Kreiranje teorijskog modela bezbednosne analitike na primeru suprotstavljanja terorizmu", Vojna akademija, Beograd.

Andrić, J., Tišma, M. (2021). New models of security analytics, *International journal of economic and law, Volume 11, No. 33 (Online), Belgrade, page 27-40.*

Andrić, J., Terzić, M. (2023). Intelligence cycle in the fight against terrorism with usage of osint data, *Journal of Information Systems & Operations Management, Vol. 17.1, May 2023:1-17.*

Bajagić, M. (2009). *Međunarodna bezbednost*, Kriminalističko-policijska akademija, Beograd.

Buzan B., Waever, O., and De Wilde, J. (1988). *Security: A New Framework for Analysis*, Linne Reinner Publishers.

Carter, J. G. & Phillips, S. W. (2015). *Intelligence-led policing and forces of organisational change in the USA*, Policing and Society, 25:4, 333-357, DOI: 10.1080/10439463.2013.865738.

Collier, M. W., (2005). "A Pragmatic Approach to Developing Intelligence Analysts", *Defence Intelligence Journal: 14-2, November, 2005.*

Corkill, J. D., Cunow, T. K., Ashton, E., & East, A. (2015). *Attributes of an analyst: What we can learn from the intelligence analysts job description.*

DOI:https://doi.org/10.4225/75/57a83ad2d2cf7.

Digest of EEA indicators (2014). Luxembourg: Publications Office of the European Union.

Dragišić, Z., Radojević, K. (2014). *Bezbednosni menadžment*. Beograd: Službeni glasnik.

Forca, B., Anočić, B., (2018). *Bezbednosna analitika*, Fakultet za poslovne studije i pravo, Beograd.

Forca, B., (2020). Teorijski i praktični aspekti ekološke bezbednosti, *Diplomatija i bezbednost, Broj 1/2020, Godina III, vol. 3, Str. 75-101.*

Forca, B., (2021). *Sistemi bezbednosti*, Fakultet za poslovne studije i pravo, Beograd.

Forca, B., (2022). *Teorijski i uporedni aspekt analize strategije nacionalne bezbednosti Republike Srbije*, Monografija, Fakultet za poslovne studije i pravo, Beograd.

Forca, B., (2024). *Evropski bezbednosni čvor*, Tematski zbornik radova sa međunarodnog naučnog skupa „Evropa na raskrsnici – Bezbednosna analitika", str. 53-88; Originalan naučni rad, Fakultet za poslovne studije i pravo, Beograd.

Forca, B., Župac, G., (2025). *Krizni menadžment u sistemu bezbednosti*, Monografija, Fakultet za poslovne studije i pravo, Beograd.

Heuer, J.R, Pherson, R.H., (2016). *Structured Analytics Techniques, for Intelligence Analyisis;* Department of Political Science, University of Copenhagen.

Ilić-Krstić, I.,(2016). *Socijalno-ekološka bezbednost, održivi razvoj i kvalitet života*, Doktorska disertacija, Fakultet zaštite na radu, Niš.

Kralj, R., (2019). *Kriminalističko-obaveštajna delatnost*, Univerzitet, Rijeka.

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy* (9. izd.). CQ Press.

Manojlović, D., (2008). *Kriminalisitička analitika*, Službeni glasnik, Beograd.

Miljević, M., (2007). *Metodologija naučnog rada*, Filozofski fakultet, Sarajevo.

Moore D.T., (2007). *Critical Thinking and Intelligence Analysis, Second Printing (with revisions*), Occasional Paper Number Fourteen, National Defense Intelligence College Washington, DC March, 2007.

NCIS (National Criminal Intelligence Service), (2000). *The National Intelligence Model*. London, NCIS.

Policijsko-obaveštajni model – Priručnik (2016). MUP Republike Srbije.

Racić, I., (2023). *Policijsko-obaveštajni model u Republici Srbiji, preduslovi za organizaciono prilagođavanje,* Monografija, Institut za kriminološka i sociološka istraživanja, Beograd.

Stajić, Lj., (2021). *Osnovi sistema bezbednosti*, Pravni fakultet, Novi Sad.

Strategija nacionalne bezbednosti Republike Srbije (2019). *„Službeni glasnik RS", br. 94/2019.*

Termiz, Dž., Milosavljević, S., (2008). *Analitika I tom*, Lukavac.

The Intelligence Community, (2024). Retrieved October 20, 2025, from URL.

Vilijams, D.P., (2012). *Uvod u studije bezbednosti*, Službeni glasnik, Beograd.

Veljković, S., (2023). Sektorski pristup bezbednosti i prelivanje pretnji na primeru oružanog sukoba u Makedoniji 2001; *Diplomatija i bezbednost,* Godina 6 Broj 2/2023, Strana 71-83.

Wæver, O., Buzan, B., Kelstrup, M., (1993). *Identity, Migration and the New Security Agenda in Europe,* London: Pinter.

Wæver, O., (2008). "The Changing Agenda of Societal Security": 581-593 in *Globalization and Environmental Challenges, Reconceptualizing Security in the 21st Century* ed. Giinter Brauch,Hans et. al., eds. Globalization and Environmental Challenges, Reconceptualizing.Security in the 21st Century, Heidelberg: Springer.