Универзитет у Београду

Тероризам, организовани криминал и безбедност

Мастер рад

КОНТРАОБАВЕШТАЈНА ДЕЛАТНОСТ КАО ФАКТОР СПРЕЧАВАЊА УГРОЖАВАЊА НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

Ментор:

др Радомир Милашиновић, редовни професор

Студент:

Жељко Стаменковић, 73/2013

Београд, јул 2015.

КОНТРАОБАВЕШТАЈНА ДЕЛАТНОСТ КАО ФАКТОР СПРЕЧАВАЊА УГРОЖАВАЊА НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

Сажетак

Рад се бави испитивањем улоге и значаја контраобавештајне делатности у заштити националне безбедности односно у спречавању њеног угрожавања од обавештајних, субверзивних и других делатности. Објашњен је начин заштите државних и других врста тајни од спољних носилаца обавештајне делатности, и наведене су адекватне мере које треба применити да би се успешно заштитили од таквих претњи. Анализиран је утицај тероризма и технолошког напретка, посебно појаве информационих технологија и интернета (које пружају нове могућности крађе виталних државних тајни и информација) на службе безбедности, односно на контраобавештајну делатност, која је између осталог проширила своју област деловања и на сајбер простор. Говори се о променама у области контраобавештајног рада, као и о разлозима за њихово спровођење. У закључку је истакнут значај контраобавештајне делатности за националну безбедност и дате су одређене смернице и препоруке за унапређење ове области.

Кључне речи: национална безбедност, угрожавање националне безбедности, обавештајне и контраобавештајне службе, контраобавештајна делатност

ABSTRACT

The thesis focuses on examining of the role and importance of counterintelligence activities in protection of the national security and in prevention of its endangerment from intelligence, subversive and other activities. An explanation is detailed in regards to protection of state and other types of secrets from foreign intelligence activities, and adequate measures were also listed which need to be applied for the purpose of successful protection against such threats. The influence of terrorism and technological advancement was analyzed, especially the appearance of information technologies and Internet (which provide completely new possibilities of theft of state secrets and information) on security services, and on the counterintelligence activity, which has, among other spheres, expanded its field of activities to the cyber space as well. The thesis speaks about changes in the sphere of counterintelligence work, as well as on reasons for their application. The conclusion stresses the importance of counterintelligence activities for the national security and provides guidelines and recommendations for improvements in this sphere.

Key words: national security, endangerment national security, intelligence and counter-intelligence services, counterintelligence activity

Биографија студента

Стаменковић Жељко рођен је у Зајечару 1989. године, где је завршио основну и средњу школу. Након тога уписује Факултет безбедности Универзитета у Београду, на коме је дипломирао 2013. године и стекао стручни назив „дипломирани менаџер безбедности“. Исте године уписао је мастер студије при Универзитету у Београду (Тероризам, организовани криминал и безбедност) и успешно положио све испите са просечном оценом 9.80.

САДРЖАЈ

Попис коришћених слика, шема, графика и табела

УВОД

Вековима уназад највећа безбедносна претња по сваку државу долазила је углавном од војних снага других држава, међутим, 21. век карактерише појава великог броја невојних претњи, државних или недржавних субјеката, од којих поред тероризма као глобалног безбедносног проблема, посебну опасност представљају обавештајне и субверзивне претње обавештајних служби. Технолошки напредак омогућио је и већу распрострањеност обавештајних и субверзивних активности, које су уз ослањање на савремене информационо-комуникационе технологије добиле нове могућности деловања и постале успешније него раније. Поред традиционалних начина крађе виталних државних информација, које обавештајне службе и друге организације примењују, јављају се нове могућности крађе података у сајбер простору, које представљају значајан контраобавештајни изазов, а самим тим и озбиљну опасност по систем националне безбедности свих држава.

Контраобавештајна делатност због своје специфичности није толико позната широј јавности, о њој се не пише често у медијима и ретко се воде јавне полемике као што је случај са обавештајном делатношћу. Можда је због тога неоправдано потцењена њена улога у спречавању угрожавања националне безбедности. Не сме се занемарити чињеница да би штете од крађа најбитнијих државних тајни или штете настале због индустријске шпијунаже биле катастрофалне за једну државу. Стога, систематско планирање развоја ове делатности мора бити препознато и спроведено од стране сваке власти.

Шпијунажа, тероризам, саботажа и друге претње у сајбер простору нису утицале на промену функција контраобавештајне делатности, али јесу на промену њених метода рада и мера супротстављања. Период глобализације донео је бржи проток и размену информација, што доприноси стварању нових рањивости у систему националне безбедности. Ово се посебно односи на област тајних података и њихове заштите од страних обавештајних служби и других субјеката, који њиховим откривањем могу угрозити безбедност виталних државних вредности и интереса. У тим измењеним околностима, функционисање савремених националних и обавештајно-безбедносних система прилагођава се новом безбедносном контексту, у коме

безбедносне и обавештајне службе проширују овлашћења, добијају нове улоге и задатке, а контраобавештајна делатност као саставни елемент националних безбедносних потенцијала представља све значајнији фактор у заштити националне безбедности. Узимајући то у обзир, државе морају јачати и капацитете за демократски и цивилни надзор обавештајних и безбедносних служби, у циљу спречавања разних злоупотреба и смањења могућности за кршење људских и грађанских права. Контраобавештајне службе данас се суочавају са бројнијим и већим изазовима него икад пре на пољу заштите тајних података и заштите од шпијунаже, која се проширила и на сајбер простор.

Који су конкретни бенефити од контраобавештајне делатности у заштити националне безбедности, на који начин контраобавештајна делатност доприноси заштити националне безбедности и које су препоруке за повећање ефикасности контраобавештајног рада су нека од питања на која је одговорено у овом раду.

Контраобавештајна делатност треба да заштити државне и друге врсте тајни од спољних носилаца обавештајне делатности и најчешће подразумева спровођење активности на територији матичне државе. Поред техничко-технолошке модернизације рада и усвајања нових метода деловања, развој контраобавештајне делатности је подразумевао све учесталије офанзивне активности у циљу задржавања поузданости и ефикасности заштите система националне безбедности. Успостављање контраобавештајних мера имало је дуг пут развоја и усавршавања, а свака служба која обавља контраобавештајну делатност развија активне и пасивне мере прилагођене својим могућностима и потребама.

Државе данас усвајају нове стратегије националне безбедности, стратегије контраобавештајног и контратерористичког рада и тако чине одређене кораке ка реорганизацији система националне безбедности. Неке од најразвијенијих светских безбедносних служби препознале су тренутак за унапређење контраобавештајне делатности и стратешки се окренуле борби против савремених претњи, рачунајући на већу и бољу материјалну, кадровску и технолошку подршку. У раду је описана америчка безбедносна служба FBI, као и промене које је спровела у циљу побољшања контраобавештајног рада.

Циљ рада је представљање и анализа контраобавештајне делатности из садашње перспективе и анализа неких савремених претњи, ради бољег разумевања њене улоге у

заштити националне безбедности. Прикупљене чињенице је потребно адекватно обрадити и критички протумачити, и у складу са тим у раду ће бити коришћене основне методе истраживања, као што су: анализа, синтеза, апстракција, генерализација, индукција и дедукција.

1. ОПШТИ ПОЈАМ БЕЗБЕДНОСТИ И НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

Безбедност је одувек заокупљала пажњу човека, од самог настанка људског друштва па до данас, појединци, људске групе, организације и институције имале су потребу да се брину о својој безбедности. У складу са тим, предузимане су одређене активности на постизању, одржавању и развијању одређеног нивоа безбедности, које су се временом мењале и проширивале. Основна преокупација друштвених група у прошлости била је везана за бригу о њиховом опстанку, која произилази из урођеног нагона за самоодржањем.[1] Међутим, још је Томас Хобс писао да нагон за самоодржањем производи у човеку тежњу за стицањем добара и личне моћи, што за собом повлачи антагонизме и непријатељства, односно стање општег сукоба у коме влада осећај несигурности, небезбедности. Чињеница је да је људско биће у својој суштини противречно и подељено на две целине: егоистичну и разумску, из чијег сукоба и настаје држава као творевина која треба да спречава негативне последице човекове зле природе унутар државе.[2] Да је безбедност једна од основних људских потреба потврђује и пирамидална хијерархија људских потреба америчког психолога Абрахама Маслова, која се састоји из пет група. Поређане су по важности од најниже до највише и обухватају: физиолошке потребе; потребе за сигурношћу; потребе за припрадношћу, потреба за уважавањем и потреба за самоостварењем. (слика 1)

Слика 1- *Хијерархијска структура потреба*[3]

[1] Ивановић, А., *Теорије безбедности*, Универзитетска мисао, 11/2012, 55-82, стр. 55.
[2] Хобс, Т., *Левијатан*, Култура, Београд, 1961; преузето из: Милашиновић, Р., Милашиновић, С., *Основи теорије конфликата*, Факултет безбедности, Београд, 2007, стр. 50, 51.
[3] Станић, М., *Дефинисање садржаја појма безбедности*, Војно дело, 2014, 93-113, стр. 101.

Потребе се задовољавају од најнижег ка највишем нивоу, а када се једна потреба са нижег нивоа задовољи тада опада значај њене мотивационе улоге, и њено место заузима потреба са вишег нивоа. Задовољавањем основних физиолошких потреба прелази се на наредну групу потреба која се тиче безбедности. Потреба за безбедношћу као једне од најважнијих потреба човека заснива се „на тежњи ка предвидљивости, извесности у погледу судбине најважнијих добара и вредности којима личност и ужа или шира заједница располажу или им стреме.“[4]

Држава, коју многи сматрају најстаријим типом организација, настала је и из потребе за ефикаснијим организовањем послова, подразумевајући ту и бољу и ефикаснију заштиту људи, односно повећање осећаја безбедности.[5] У прошлости, готово до краја XX века, безбедност се најчешће посматрала са аспекта спољног угрожавања безбедности државе и везивала се за војску и њену функцију заштите безбедности државе. Иако није прошло много година од тада, то гледиште је значајно промењено. Разлози који су утицали на промену гледишта су бројни бројни, од појаве савремених невојних облика угрожавања безбедности, чије последице превазилазе могућности појединачних држава на супротстављању, и доводе у питање не само егзистенцију појединаца и државе већ и целог човечанства, до промена у међународним односима.[6]

Данас је пажња са државе као референтног објекта безбедности преусмерена на појединце, друштвене групе, економски систем, животну средину итд. што је неминовно довело до развоја концепта индивидуалне, социјеталне, глобалне, економске, еколошке и осталих видова безбедности.[7] До данашњих дана није донета општеприхваћена дефиниција безбедности, па је у језику друштвених наука „безбедност“ и даље контроверзан појам. У зависности од људских идеја, култура и перцепција стварности, појам безбедности добија другачију вредност, што доказују бројне дефиниције које су се појавиле после Хладног рата. Држава је на неки начин представљала модел безбедности, јер је била одговорна у заштити својих грађана, тако да је безбедност грађана зависила од безбедности саме државе, односно од њених

[4] Димитријевић, В., *Појам безбедности у међународним односима*, Савез удружења правника Југославије, Београд, 1973, 7-38, стр. 10.
[5] Станић, М., *Дефинисање садржаја појма безбедности*, Војно дело, 2014, 93-113, стр. 93.
[6] Ивановић, А., *Теорије безбедности*, Универзитетска мисао, 11/2012, 55-82, стр. 55.
[7] Исто, стр. 55, 56.

способности да се одбрани од непријатеља.[8] Безбедност се као рационална делатност организује у систем који треба да задовољи потребе заштите виталних вредности друштва. Његова основна функција је превентивна, јер својим постојањем представља инструмент одвраћања од свих облика и извора угрожавања.[9]

„Етимолошки посматрано, израз безбедност потиче од латинске речи **securutas-atis**, што значи безбедност, одсуство опасности, извесност, самопоуздање, неустрашивост, заштићеност (**securus** лат. – сигура, безбедан, поуздан, неустрашив, уверен, сталан, чврст, одан, истинит итд.).“[10] Безбедност се у српском језику дословно преводи као одсуство беде, стање без беде, где беда означава бригу или невољу. Према С. Мијалковићу: „Бити безбедан значи бити заштићен од утицаја нежељених појава, и осећати се заштићеним (сигурним, без страха) у предвидивом и контролисаном амбијенту. Безбедност је резултанта односа-баланса између стварне и потенцијалне угрожености референтних вредности и интереса и постојећих капацитета (људских, материјалних, организационих и функционалних) који их штите.“ [11]

За појам безбедности се везују различита мишљења и тумачења, а неретко има и више значења, међутим, уобичајено гледиште је да се под тим појмом подразумева одређено стање, организација, функција или систем, или све то заједно.[12] „Према савременом схватању, безбедност је својство неког реалног друштвеног, природног или техничког субјекта (бића, творевине или ствари) испољено као успостављено, одржано и унапређено стање и (ли) вредност, а која се изражава кроз испуњеност минимума одређених безбедносних стандарда својствених том субјекту, а што му омогућава реалну основу за опстанак, рад, раст и развој без обзира на носиоце, облике, време и место угрожавања.“[13]

Уважавајући научни приступ, безбедност се дели на:[14]

- унутрашњу (индивидуална, социјетална и национална) и

[8] Iglesias, M., Ministrio de Defensa, 2011, *The Evolution of the concept of Security*, Instituto Español de Estudios Estratégicos, str. 1.
[9] Кековић, З., Системи безбедности, Факултет безбедности, Београд, 2009, стр. 81, 86.
[10] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 21.
[11] Мијалковић С., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009, стр. 40.
[12] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 24.
[13] Исто, стр. 28.
[14] Стајић, Љ., Гаћиновић, Р., *Увод у студије безбедности*; Драслар партнер, Београд, 2007, стр. 35; цитирано према: Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 32.

– међународну (регионална, глобална, заједничка, колективна и кооперативна) безбедност.

У наредном потпоглављу пажња ће бити посвећена националној безбедности, (дистинкцији термина националне и државне безбедности).

1.1. Државна и(ли) национална безбедност

Посматрано из угла традиционалног приступа безбедности, концепт државне безбедности је подразумевао заштиту суверенитета и територијалног интегритета као виталних државних вредности, док су питања свакодневне безбедности људи углавном била маргинализована. Поред тога, јачањем војних капацитета требало је заштитити основне државне интересе, који се углавном нису поклапали са интересима других држава (осим ако није реч о савезништву). Страх од оружаног напада и спремност за одбрану земље од различитих врста претњи, као и превентивно јачање војних потенцијала, који би били средство одвраћања од напада, обележили су готово читав период Хладног рата. У том периоду, када је средиште свих безбедносних питања заузимала готово искључиво држава, односно очување њених виталних вредности и интереса, све чешће долази до употребе термина национална безбедност, иако је термин државна безбедност био одговарајући. Може се рећи да се носиоци власти нису устручавали да у својој реторици (зло)употребљавају придев национални као средство којим би се придобило друштво и тиме прикупила легитимност за потенцијално контроверзну политику.[15] Чињеница да су појмови држава и нација потпуно различити не представља носиоцима власти држава препреку да уместо државне безбедности (зло)употребљавају синтагму национална безбедност у „сврсисходним моментима“.

Национална безбедност као појам је после Другог светског рата ушао у ширу употребу, а сматра се да га је први употребио Волтер Липман у својој књизи Спољна политика САД-а (U.S. Foreign Policy 1943), иако је он пре тога коришћен у Француској и у Краљевини Југославији. У Министарству унутрашњих дела 1940. године постојала

[15] Кековић, З., *Системи безбедности*, Факултет безбедности, Београд, 2009, стр. 110.

је „Дирекција националне безбедности“ по угледу на сличну дирекцију у француском Министарству унутрашњих послова.[16]

Безбедност државе обухвата заштиту државних вредности, пре свега: суверенитета, територијалног интегритета, уставног и правног поретка. У том смислу, појам државне безбедности имао је знатно ужи обим и садржај од савременог поимања националне безбедности, јер није обухватао категорије безбедности појединца и друштвених група, њихових слобода и људских права, живота и имовине, демократских институција, али ни недржавни сектор безбедности, који су сматрани сфером тзв. јавне безбедности.[17]Међутим, погрешно је закључити да је безбедност појединаца и група искључена из тог концепта. Она наравно спада у круг вредности које држава треба заштитити, у прошлости често обухваћена називом друштво. Можда је исправно рећи да је заштита људских права у прошлости била маргинализована, нарочито до краја Хладног рата, када су се државе константно наоружавале, не водећи превише рачуна о човеку. Међутим, данас се људска безбедност као концепт потпуно афирмисао, тако да проширује области деловања система националне безбедности и не представља концепт супротан националној безбедности, већ његову допуну и надоградњу.

Данас је уобичајено да се у савременим политичким и правним наукама државна безбедност третира само као једна од компоненти националне безбедности.[18] Вредности које се штите код једне и код друге категорије су мање више исте, али се додавањем придева „национални“ више пажње усмерава ка човеку, становништву (људским правима) и њиховој заштити. Такође, важно је рећи и да су различите државе на различите начине употребљавале једну од ове две синтагме. Ако се говори о безбедносној пракси земаља, чињеница је да су у источним земљама претежно користили синтагму *државна безбедност*, а у западним *национална безбедност*.[19] На западу се генерално националност изједначава са држављанством, јер се под нацијом обично подразумева скуп грађана неке државе, док се у другим деловима света,

[16] Илић, П., *О дефинисању и дефиницијама националне безбедности*, Војно дело, 2012, 123-138, стр. 128, 129. ; Мијалковић, С., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009, стр. 79. ; Драгишић, З., *Систем националне безбедности: Покушај дефинисања појма*, Војно дело 3/2009., стр. 164.
[17] Мијалковић, С., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009, стр. 82.
[18] Илић, П., *О дефинисању и дефиницијама националне безбедности*, Војно дело, 2012, 123-138, стр. 129.
[19] Мијалковић, С., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009, стр. 187, 188.

рачунајући ту и Србију придев „националан“ често везивао за нацију као велику етничку групу, која се својим специфичним карактеристикама разликује од других таквих група.[20] Важно је истаћи и да је феномен нације најчешће ширег (географског) обима од државе, а државе и не морају да буду националне, односно да се територијално подударају са простирањем нација.[21]

Највећи број аутора у својим дефиницијама националну безбедност одређује као одређено стање државе, што је свакако један од кључних услова за њено успешно дефинисање. Тако је према С. Мијалковићу, национална безбедност „*стање несметаног остваривања, развоја, уживања и оптималне заштићености националних и државних вредности и интереса које се достиже, одржава и унапређује функцијом безбедности грађана, националног система безбедности и наднационалним безбедносним механизмима, као и одсуство (појединачног, групног и колективног) страха од њиховог угрожавања, те колективни осећај спокојства, извесност и контрола над развојем будућих појава и догађаја од значаја за живот друштва и државе*“.[22]

Национална безбедност према Војину Димитријевићу обухвата следеће вредности које треба заштити:[23]

- опстанак државе, нације и становништва;
- територијални интегритет;
- политичку самосталност; и
- квалитет живота.

Данас се национална безбедност генерално доживљава као безбедност грађана и државе, али и свих сфера државног и друштвеног живота.[24] Код доносиоца политичких одлука често постоји тенденција да се класни, групни па и лични интереси представе као национални, међутим, ово не би требало да доведе до његовог избацивања из употребе, јер је овај појам „уврежен у државној и националној посебности и

[20] Илић, П., *О дефинисању и дефиницијама националне безбедности*, Војно дело, 2012, 123-138, стр. 128.
[21] Мијалковић, С., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009, стр. 80.
[22] Исто, стр. 181.
[23] Димитријевић, В., *Појам безбедности у међународним односима*, Савез удружења правника Југославије, Београд, 1973, 7-38, стр. 18-24.
[24] Мијалковић, С., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009, стр. 83.

идентитету, у припадању човековој политичкој заједници, коју осећа као своју и онда када хоће да је мења и побољшава и од које очекује и личну безбедност.“[25]

2. ОБАВЕШТАЈНО-БЕЗБЕДНОСНИ СИСТЕМ

Држава као заједница која синтетизује и тежи остварењу интереса својих грађана (терминолошки означени као државни, витални или национални интереси), мора успоставити одређене механизме или системе, како би их заштитила од унутрашњих и спољних опасности. Приоритетни интереси сваке државе треба да буду усмерени на очување територијалног интегритета, неповредивост граница, заштиту грађана и материјалних добара. Способност организованог отклањања опасности се често истиче као важан услов постојања и развоја сваке државе, и у складу са тим, а узимајући у обзир схватање безбедности као функције државе и уставне категорије, држава мора поседовати одговарајуће организован и уређен систем, који основни задатак остварује кроз две функције: безбедносну и обавештајну.[26] Схватањем државе као макросистема можемо разумети логику успостављања великих система, подсистема и микросистема (као што су: политички, економски, социјални, безбедносни, одбрамбени и др.) који су испреплетени вертикалним и хоризонталним везама, посредством којих функционишу као глобални државни и друштвени систем, остварујући тиме друштвене и државне интересе, односно испуњавајући сврху свог постојања. [27]

Унутрашње правне норме које регулишу безбедност државе морају бити усаглашене са општим нормама међународног права. Истовремено, држава усклађује своје обавезе према склопљеним војним и безбедносним уговорима, тако да свој систем безбедности прилагођава уговорним обавезама. Може се рећи да систем националне безбедности представља подстистем ширих друштвених система (пре свега политичког), а истовремено представља веома сложен систем сачињен од одређених

[25] Димитријевић, В., *Појам безбедности у међународним односима*, Савез удружења правника Југославије, Београд, 1973, 7-38, стр. 31, 33.
[26] Мијалковски, М., *Обавештајне и безбедносне службе*, Факултет безбедности, Службени гласник, Београд, 2009, стр. 32, 33. ; Драгишић, З., *Систем националне безбедности: Покушај дефинисања појма*, Војно дело 3/2009, 162-176, стр. 162.
[27] Мијалковски, М., *Обавештајне и безбедносне службе*, Факултет безбедности, Службени гласник, Београд, 2009., стр. 32.

подсистема и елемената, који су функционално повезани и усклађени. [28] „Систем безбедности као целовита и јединствена делатност сваког конкретног друштва укључује скуп чинилаца и њихових акција у миру, ванредним приликама и рату. Сви чиниоци безбедности међусобно су повезани на основу јединствених начела политичког система и правног поретка земље.“ [29]

Обавештајно-безбедносни систем се уобичајено формулише као подсистем система безбедности који: „*представља прописима дефинисан делокруг надлежности и међусобних права свих обавештајних и безбедносних служби и других установа државе или другог одговарајућег ентитета које су ангажоване да прикупљају, процењују и дистрибуирају обавештајне податке, као и да извршавају друге захтеве који им се ставе у надлежност*.“[30] У стратегији националне безбедности Републике Србије из 2009. године, обавештајно-безбедносни систем такође је представљен као подсистем националне безбедности сачињен од три агенције: Безбедносно-информативне агенције, Војнобезбедносне агенције и Војнообавештајне агенције. Њихове надлежности, делокруг рада, овлашћења, задаци, цивилна и демократска контрола, регулишу се законом.[31]

Делатност свих чиниоца система у оквиру њихових надлежности је синхронизована и подразумева висок степен формализованости. У организационом смислу не постоји тип обавештајно-безбедносног система који би одговарао свакој држави. У пракси међутим постоје два доминантна начина организовања овог система, то су: *централизовани систем*, у коме постоји једна централна обавештајна установа, која је главни обавештајни и аналитички орган; и *децентрализовани систем*, који има одвојене обавештајне службе, које су истовремено и обавештајни и главни аналитички орган (свака у оквиру свог ресора).[32] Свака држава, узимајући у обзир предности и недостатке ових система, се опредељује за онај систем који највише одговара њеним условима и државним интересима и прилагођава га конретним околностима.

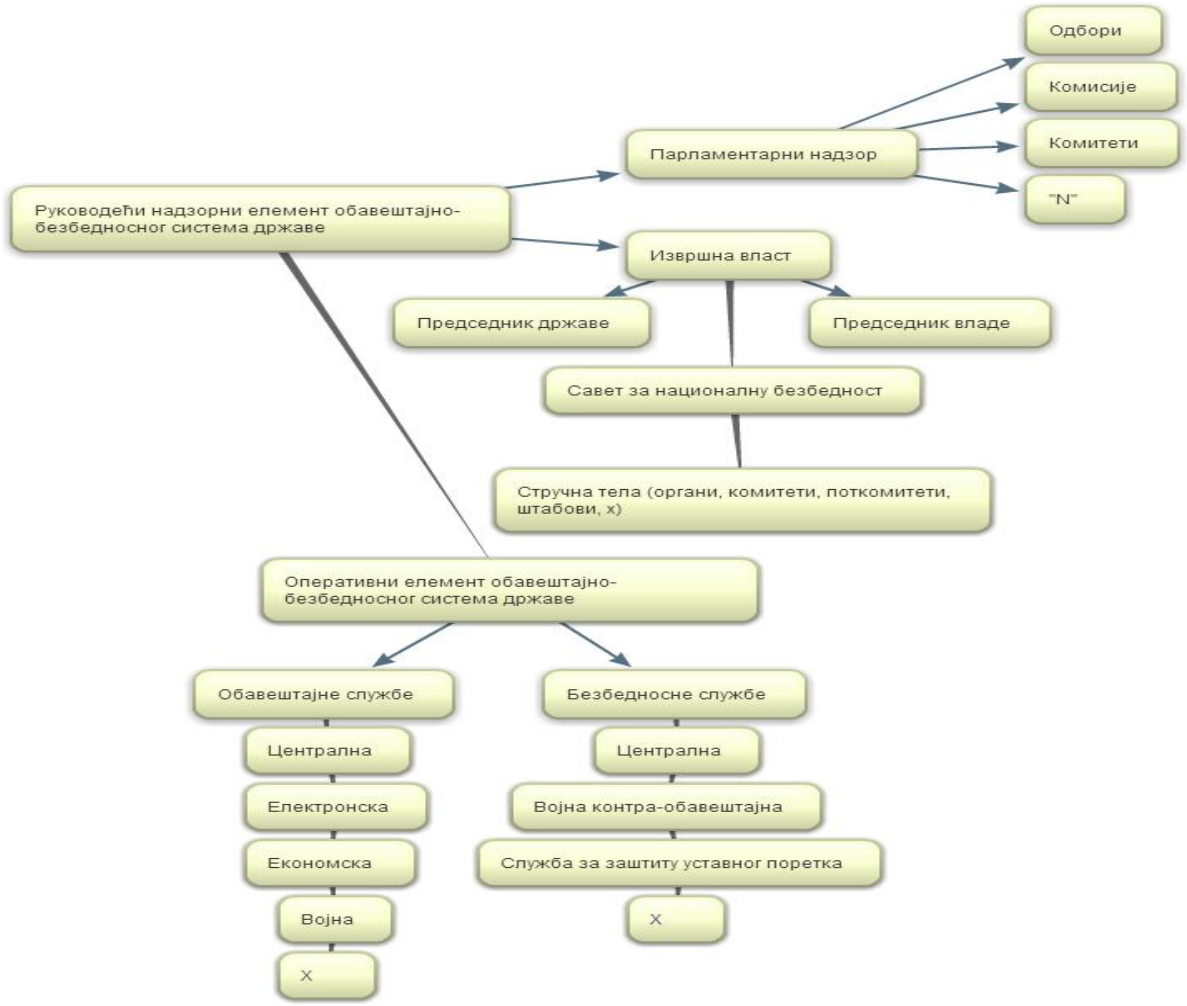
[28] Драгишић, З., *Систем националне безбедности: Покушај дефинисања појма*, Војно дело 3/2009, (162-176), стр. 164.
[29] Исто, стр. 162.
[30] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 39.
[31] Република Србија (2009), *Стратегија националне безбедности Републике Србије*, Београд, октобар, 2009, Службени Гласник, стр. 18.
[32] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 40, 41.

У ширем смислу, обавештајно-безбедносни систем сачињавају: [33]

1) контролне и усмеравајуће структуре и

2) оперативне структуре које, у складу са надлежностима и овлашћењима, настоје да допринесу заштити виталних државних вредности. У оперативне структуре спадају све обавештајне, безбедносне, безбедносно-обавештајне и полицијске службе (агенције, министарства). Обавештајно-безбедносни систем сачињавају обавештајне, контраобавештајне, безбедносне установе, и координациона, саветодавна и надзорна тела.

Основне компоненте обавештајно-безбедносног система државе приказане су на шеми 1.



Шема 1: *Основне компоненте обавештајно-безбедносног система државе*[34]

[33] Мијалковски, М., *Обавештајне и безбедносне службе*, Факултет безбедности, Службени гласник, Београд, 2009, стр. 35.

По својим организационим, кадровским, техничко-технолошким потенцијалима један од најбољих и најразвијенијих безбедносно-обавештајних система је обавештајно-безбедносни систем Јапана, као изузетно комплексан подсистем система националне безбедности. Чине га следеће установе, тела и агенције: [35]

1. Савет безбедности
2. Канцеларија за истраживање при Кабинету премијера (анализирају информације из иностранства)
3. Одбрамбена агенција
4. Војно-обавештајни биро
5. Војно-обавештајни штаб
6. Електронска војно-обавештајна служба
7. Обавештајни елементи видова оружаних снага:
    а) Обавештајни елементи копнених снага
    б) Обавештајна командна флота поморских снага
    в) Обавештајно одељење
8. Агенција националне полиције и биро за безбедност Националне Комисије државне безбедности
9. Биро за обавештајни рад и анализе Министарства спољних послова
10. Јавна агенција за безбедносне истраге Министарства правде
11. Спољно-трговинска организација Јапана при Министарству економије и друге установе.

Неке од значајнијих обавештајних и безбедносних агенција Јапана су:

Јавна агенција за безбедносне истраге Министарства правде је извршна обавештајно-безбедносна агенција основана 1952. године као агенција за истраге и контролисање унутрашње субверзије. Бави се питањем националне безбедности унутар и ван земље, а најчешће је ангажована на пословима контраобавештајне заштите. У циљу спровођења истраге потребне за контролу субверзивних организација, ова

[34] Мијалковски, М., *Обавештајне и безбедносне службе*, Факултет безбедности, Службени гласник, Београд, 2009, стр. 37.
[35] Japan intelligence and Security Agencies, доступно на: http://www.fas.org/irp/world/japan/, приступљено: 20. 11. 2014.

агенција има стациониране истражитеље јавне безбедности у целој земљи. Тренутно има око 1800 припадника, међутим планирано је смањење броја за 600 до 700.[36]

Биро за безбедност Националне Комисије државне безбедности формулише и врши надзор над спровођењем безбедносне политике у земљи. Биро је одговоран за прикупљање обавештајно-безбедносних података о странцима и радикалним политичким групама које могу да угрозе националну безбедност.[37]

Јапанска Централна обавештајна агенција је Наичо (Naicho). Има само око 80 запослених и сви раде при канцеларији премијера. Углавном се баве анализирањем страних обавештајних података. Прикупљање података и анализе се углавном односе на новинске чланке и званична документа из иностранства. Претпоставља се да делује као веза и координатор активности између обавештајних служби и владе.[38]

Одбрамбена обавештајна агенција обавља обавештајне и безбедносне операције унутар државе и на територији страних држава. Подељена је у две оперативне секције, прву и другу обавештајну дивизију. Прва спроводи обавештајне и безбедносне активности само унутар државе, са циљем да прикупи информације које се односе на угрожавање националне безбедности. У свом саставу има контраобавештајне и контратерористичке стручњаке. Друга је одговорна за спољне обавештајне информације.[39]

У 2013. години Јапан је усвојио посебан закон о тајности података, који је поставио јединствен систем поретка међу агенцијама и који прописује јасне и озбиљне последице за цурење информација. Раније су различите агенције на различите начине штитиле податке од виталног државног интереса, што је доводило до стварања неповерења међу њима, због могућности цурења информација. Овај закон је стандардизовао област чувања тајних података и уједно омогућио подстицање боље и ефикасније сарадње међу службама.[40] Јапански обавештајно-безбедносни систем има укупно око пет хиљада обавештајних официра, који раде на различитим задацима у иностранству, укључујући и контраобавештајне послове, што је по неким проценама

[36] Public Security Investigation Agency (Koancho), доступно на: http://fas.org/irp/world/japan/koancho.htm, приступљено: 20. 11. 2014.
[37] Security Bureau, доступно на: http://fas.org/irp/world/japan/sb.htm, приступљено: 20. 11. 2014.
[38] Cabinet Research Office, доступно на: http://fas.org/irp/world/japan/naicho.htm, приступљено: 20. 11. 2014.
[39] Japan, Intelligence and Security, доступно на: http://www.faqs.org/espionage/Int-Ke/Japan-Intelligence-and-Security.html, приступљено: 20. 11. 2014.
[40] Stratfor: Global Intelligence, *Japan's Intelligence Reform Inches Forward*, 2015, доступно на: https://www.stratfor.com/analysis/japans-intelligence-reform-inches-forward, приступљено: 25. 11. 2014.

веома мало. Требало би повећати и годишњи буџет обавештајно-безбедносног сектора који износи око 700 милиона фунти, што је око 2% укупног војног буџета Јапана.[41]

Поред одређених предности које сложени обавештајно-безбедносни апарат Јапана има, мора се истаћи и да због великог броја обавештајних и безбедносних служби често долази до преклапања дужности међу њима, иако је реформски процес одавно започет. Такође, у оквиру овог система не постоји институција која би објединила све службе, и која би осигурала ефикасну размену информацијама између различитих служби.

3. УГРОЖАВАЊЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

3.1. Појам угрожавања

Опасност се у свом основном облику испољава као угрожавање нечијег битисања, опстанка, слободе и развоја. Угрожавање може бити: 1. намерно-свесно, када се циљано или организовано користи сила за уништење, онемогућавање, принуду, присилу људи, група, организација итд. или када се жели постићи одређена промена насупрот њиховој вољи; 2. ненамерно-несвесно, када се без намере угрожава егзистенција појединца или групе људи. [42] Угрожавање безбедности је супротност-антипод безбедности и подразумева све појаве (природног, људског или техничко-технолошког порекла) и процесе који су деструктивни по референтне вредности и интересе. [43] Одговор друштва и државе као суверeног тела (на међународном нивоу) на појаве угрожавања безбедности је стварање и уређење динамичних система, који имају функцију заштите од различитих појава угрожавања. Потенцијал угрожавања, учесталост, обим негативних последица и степен угрожености од одређених појава могу утицати на доношење одлуке државе у правцу стратешког опредељења борбе против таквих негативних појава. Тај процес најчешће започиње усвајањем платформе, стратегије, доношењем закона, чиме се обично формира подсистем у оквиру система безбедности, чија је основна функција заштита виталних вредности државе и друштва

[41] Kotani, K., *Current Japanese Intelligence Reform*, n.d., доступно на: http://www.nuffield.ox.ac.uk/Research/OIG/Documents/kotani1.pdf, приступљено: 25. 11. 2014.
[42] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 49.
[43] Мијалковић, С., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009, стр. 109, 112.

од конретних појава угрожавања, као што је случај са тероризмом у САД-у. Према циклусу угрожавања, извори, облици и носиоци угрожавања чине три елемента угрожавања и изостанком једног од њих нема ни угрожавања. Извори представљају основ, базу неке будуће појаве, али они сами по себи нису угрожавање. Извор угрожавања може бити: супротност интереса (националних, политичких, верских и др.), неусклађеност циљева и средстава, екстремизам и др. Чињеница је да систем безбедности може деловати само на носиоце и облике, јер постојање извора не имплицира и постојање угрожавања.[44] У даљем тексту пажња ће бити усмерена на облике и носиоце угрожавања.

Носилац (реализатор) угрожавања безбедности својом радњом, или пропуштањем радње спроводи конретне облике угрожавања и може бити: појединац, група (криминална, терористичка група итд.), правно лице или организација, држава, међународна организација и међународна заједница.[45] Носиоци угрожавања могу бити нпр. терористичке организације или појединци (индивидуални тероризам), екстремне политичке групације, али и обавештајне службе страних држава, које организују и посредно или непосредно спроводе одређене активности на територији других држава, ради реализације државних и политичких циљева својих држава.

Према месту настанка, облици угрожавања деле се на: спољне и унутрашње. Спољни облици угрожавања безбедности могу се поделити на:[46]

а) *оружану агресију, оружану интервенцију и оружани притисак* (оружани облици) и

б) *специјални рат*- изазивањем унутрашњих немира, међународним тероризмом, субверзијама (неоружани облици). Унутрашњи облици угрожавања безбедности такође могу бити: [47]

- *оружани* (оружана побуна и тероризам масовнијих размера); и
- *неоружани* (обавештајно-извиђачка делатност, саботаже, диверзије, грађански нереди, деструктивна психолошко-пропагандна делатност, разне криминалне појаве, екстремизам и др.).

[44] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 52-54.
[45] Мијалковић, С., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009, стр. 115,116.
[46] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 72.
[47] Исто, стр. 73.

Необавештајне (субверзивне) делатности обавештајних и безбедносних служби представљају компоненту спољне политике државе, чија примена подразумева увек силу и насиље према држави, мети напада. Необавештајне делатности се често налазе у комбинацији са обавештајним уколико се ради о реализацији спољно-политичких планова, и реализују се само по захтеву државног руководства.[48] Са аспекта међународног права, државама је забрањено мешање у унутрашње ствари других држава, што је и регулисано великим бројем докумената усвојених у УН, међутим, необавештајна дејства обавештајних служби у пракси често нису уопште или нису ефикасно санкционисана, и због тога су ова дејства једно од најпоузданијих и најефикаснијих средстава за остваривање спољно политичких циљева и интереса.[49]

Необавештајне делатности обавештајних служби државе хегемона против друге државе могу се поделити на:[50]

- *непосредне* (носиоци: припадници обавештајне службе) и
- *посредне* (носиоци: агенти од утицаја).

Непосредне необавештајне делатности су: пропагандне, терористичке и диверзантске, а посредне: саботирање доношења одлука, опструисање донетих одлука, индоктринарне, психолошко-пропагандне, организовано-криминалне, терористичке, саботажне, побуњеничке, превратничке, изазивање и управљање кризама и др.[51] У даљем тексту ће бити издвојене и објашњене неке од необавештајних делатности обавештајних служби.

Субверзивна делатност. Према Љ. Стајићу: „Под субверзијом, у ширем смислу, подразумева се организована подривачка делатност из иностранства против политичког и друштвеног уређења неке државе или њених политичких, економских или правних установа.“[52] Крајњи циљ је промена носилаца власти или руководећих лица у држави, односно измена њеног уставног или друштвеног система. Учесници који спроводе разне облике планираних субверзивних активности су наменске снаге

[48] Мијалковски, М., Конатар, В., *Необавештајна роварења обавештајаца: у лавиринтима специјалних операција*, Прометеј, Нови Сад, 2010, стр. 93-95.
[49] Конатар, В., *(Не)Обавештајне операције као акти агресије*, Култура полиса, год. IX, 2012, бр. 17, 27-44, стр. 32.
[50] Мијалковски, М., Конатар, В., *Необавештајна роварења обавештајаца: у лавиринтима специјалних операција*, Прометеј, Нови Сад, 2010, стр. 96.
[51] Исто, стр. 96.
[52] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 74.

(стране обавештајне и војнообавештајне службе), снаге за специјална дејства и друге снаге (политичке партије, организације, терористичке групе и организације). Субверзија се испољава кроз доста различитих облика, од деструктивних психолошко-пропагандних до диверзантских, терористичих и побуњеничких активности.[53]

Саботажа. „Саботажа је тихо и прикривено деловање од стране појединаца или група у оквиру вршења радних и друштвено-политичких обавеза са циљем изазивања дезорганизације рада и наношења материјалне штете, како конкретном привредном субјекту, тако и ради подривања постојећег привредног и политичког поретка у целини.“[54] Саботажа се разликује од тероризма по томе што је саботер један од запослених, тј. ради у организацији у којој изводи саботажу и нипошто не показује да је причињена штета резултат намерне, свесне делатности. Циљ је стварање утиска да је штета настала као последица случајности, немара, јавашлука или лошег материјала. Највећу опасност по државу и њен систем безбедности представљају саботаже које се изводе на системима од националног значаја, нпр. на енергетским системима.[55] Нуклеарна постројења и војна индустрија су посебно рањива места, која морају бити под снажном заштитом обавештајних и безбедносних служби, укључујући и активну контраобавештајну заштиту.

Деструктивна психолошко-пропагандна делатност је континуирана и деструктивна активност, планирана са циљем дискредитације одређене земље (мете угрожавања) и избегавања изношења истине о стварним догађајима унутар земље. Она је често увод или почетак планираних субверзивних активности, које се надовезују или се упоредо са њом спроводе, тако да је један од њених циљева проналажење и подстицање снага које су спремне да се укључе у субверзивну делатност.[56] Субверзивну пропаганду спроводе цивилне и војне обавештајне службе, које уколико је потребно ангажују и додатне снаге за испуњавање осталих субверзивних активности. Веома је битно да контраобавештајна служба или контраобавештајни сектор у обавештајној служби правовремено и тачно процени намере страних обавештајних служби, како би се у што краћем року спровеле контра мере.

---

[53] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 74.
[54] Гаћиновић, Р., *Унутрашњи неоружани облици угрожавања капацитета безбедности државе*, Политичка ревија, 2012, (31), 229-251, стр. 233.
[55] Мијалковић, С., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009, стр. 258, 259.
[56] Гаћиновић, Р., *Унутрашњи неоружани облици угрожавања капацитета безбедности државе*, Политичка ревија, 2012, (31), 229-251, стр.234.

Обавештајна и извиђачка делатност је као планска и континуирана активност, која се спроводи с циљем прикупљања великог броја тачних података о стању економских, друштвено-политичких, војних, полицијских, културних и других односа, стању у војсци, њеној спремности и способности за одбрану земље. Врше је припадници страних обавештајних служби посредно и непосредно. Они могу бити уграђени у страна представништва (пре свега дипломатска) у земљи и иностранству, посредством којих формалним и неформалним путем долазе до података, који су у средишту интересовања. [57]

Изазивање и управљање кризама је веома сложена метода обавештајних служби која служби за планско стварање или искоришћавање постојеће кризне ситуације у другој земљи према којој се врши субверзија. Обично се искоришћавају постојећи друштвени проблеми и стварају се услови за њихову ескалацију, али могу се и вештачки изазвати политички, економски, међунационални, међуверски и други друштвени проблеми. Обавештајне службе продиру у велики број друштвених структура државе објекта напада, циљајући на средства јавног информисања (која су један од кључних фактора), синдикалне институције, омладинске и студентске организације које су врло погодне за индоктринацију и др. Након успешног изазивања кризе прелази се на друге методе субверзивног деловања, од саботаже и тероризма до насилних преврата.[58]

Тероризам. Обавештајне службе примењују тероризам као методу деловања онда када њени руководиоци процене да је у одређеном тренутку тај начин најпогоднији за постизање конкретних, планираних резултата.[59] Последице тероризма по државу и друштво су вишеструке и манифестују се кроз најмање три димензије: људску димензију (угрожавање живота људи, кршење људских права и др.); економску (негативни ефекти на економију, нарочито изражено код држава у транзицији); безбедносну димензију (све последице које се тичу угрожавања националне безбедности).[60]

---

[57] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 75.
[58] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 199, 200; Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 243.
[59] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 244.
[60] Милашиновић, Р., Мијалковић, С., *Тероризам као савремена безбедносна претња*, Министарство унутрашњих послова Републике Српске, Висока школа унутрашњих послова у сарадњи са Ханс Зајдел фондацијом, Супротстављање тероризму- међународни стандарди и правна регулатива, Козара, 29-30. март, Висока школа унутрашњих послова, Бања Лука, 2011, 1-16, стр. 8, 9.

Према Д. Симеуновићу: „Као вишедимензионални политички феномен савремени тероризам се може теоријски најопштије одредити као сложени облик организованог групног, и ређе индивидуалног или институционалног политичког насиља обележен застрашујућим брахијално-физичким и психолошким методама политичке борбе којима се обично у време политичких и економских криза, а ретко и у условима остварене економске и политичке стабилности једног друштва, систематски покушавају остварити „велики циљеви“ на начин непримерен датим условима.“ [61] Државни тероризам се као израз обично употребљава да би се осудом означили терористички акти које организује и спроводи нека држава односно њени органи.[62]

Међудржавни тероризам се везује за обавештајне службе, јер се оне јављају као организатори терористичког деловања са циљем угрожавања одређених субјеката на међународном плану, док су реализатори терористичке групе или организације из тих земаља, које од обавештајних служби добијају организациону, обавештајну, материјалну и другу помоћ.[63]

Терористичке организације нису војне организације, нити је тероризам војно деловање, већ је изразито политички феномен, који се налази у „сивој зони“ између политике и рата. [64] Коришћење само војне силе против тероризма није дало очекиване резултате, стога систематско супротстављање тероризму поред војног фактора подразумева и активно учешће полиције, обавештајних и безбедносних служби и коначно целокупног друштва, успостављањем посебних механизама борбе против тероризма и подизањем нивоа безбедносне културе становништва. Национални интереси савремених држава најчешће се дефинишу кроз призму актуелних безбедносних ризика и претњи по њихову безбедност, који су претежно невојне природе. Обавештајна делатност и тероризам представљају неке од најраспрострањенијих претњи по националну безбедност савремених држава.

3.2. Информациона револуција и претње у сајбер простору

Информациона технологија и умрежавање значајно утичу на сваки сегмент живота и рада човека, односно на све аспекте људског понашања. Сва технологија коју

[61] Симеуновић, Д., *Тероризам: Општи део*, Правни факултет, Београд, 2009, стр. 78.
[62] Исто, стр. 81.
[63] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 221.
[64] Bilandžić, M., *Terorizam i restrukturiranje društvene moći*, Polemos 16 (2013), 2: 31-49, str. 41.

су људи створили могла би се користити за добробит свих нас, али такође, она може бити злоупотребљена у сврху напада, односно уништења. Данас је она доступна свима, и чињеница је да је појединци или групе лако могу искористити да остваре своје циљеве, који су усмерени против интереса већине људи.[65] Зависност државних институција и великих корпорација од информационих система повећава њихову рањивост на различите нападе страних обавештајних служби, конкурентских корпорација, терориста, хакера, чији циљ може бити неовлашћено прикупљање података, поремећај рада или трајно уништење нападнутог система.

Због сложености сајбер простора, веома је тешко прецизно дефинисати претње које угрожавају информационе инфраструктуре. Њих карактерише динамичност, разноврсност, константно ширење на нове области паралелно са већом употребом рачунара и глобалних рачунарских мрежа, тешка сагледивост последица, отежано откривање и доказивање, специфичан профил починилаца итд.[66]

Потенцијални нападачи у сајбер простору могу бити:[67]

- појединци са криминалним намерама;
- криминалци (појединце, групе и организовани криминал);
- терористи и разне екстремистичке групе;
- државе (пријатељске и/или непријатељске), без обзира на њихов мотив (крађа, превара, шпијунажа, утицај или ратовање).

Нападачима, односно починиоцима кривичних дела с једне стране одговарају иновације и увођење нових оперативних система због периода адаптације, који је корисницима потребан да конфигуришу бољу и ефикаснију заштиту, а с друге стране када дође до стандардизације у овој области (нпр. Windows оперативни систем) онда такав систем постаје главна мета нападача.[68] Због тога неке обавештајне и безбедносне службе и поједине државне институције поседују специјално креиране програме или

[65] Janczewski, L., Colarik, A., *Cyber Warfare And Cyber Terrorism*, Information Science Reference, New York, 2008, стр. X.
[66] Цетинић, М., *Компјутерска кривична дела и њихови појавни облици*, Правни живот бр. 10, Удружење правника Србије, Београд, 1998, стр.263-267.
[67] Петровић, С., *Кибер простор- извориште нових претњи националној безбедности*, Међународни научно-стручни скуп: Информациона безбедност 2009, Београд, стр. 256.
[68] Shinder D., *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., Rockland (USA), 2002; цитирано према: Вулетић, Д., *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011, стр. 20.

оперативне системе који су прилагођени њиховим потребама коришћења, са високим степеном заштите.

Интернет и тероризам

Генерално гледано, злоупотреба интернета од стране терористе може бити тројака: као оружје, као начин комуникације међу активистима и као медиј преко кога се обраћају јавности и шаљу своје поруке. Терористичке групе данас користе интернет и доступне севисе на њему као средство комуникације између својих припадника, разменом енкриптованих порука; за организовање и мобилизацију људства; екстремистичке пропагандне активности; прикупљање новчаних средстава и оружја итд. [69] Велики број терористичких организација има сопствене интернет стране преко којих врше пропагандне активности, као нпр: Хамас, Либански Хезболах, ЕТА, ИРА, Тамилски тигрови, Радничка партија Курда, јапанска Црвена армија, исламски покрет Узбекистана, Оружане револуционарне снаге Колумбије, Врховна истина, покрет Кахане и др. Интернет стране ових и многих других оранизација обично делују ван државе против које спроводе своје активности. На неким интернет сајтовима је чак наглашено у називу сајта или на почетној страни да то није званични сајт терористичке организације.[70]

Сајбер тероризам. Тероризам је данас један од најраспрострањенијих облика насиља за изражавање незадовољства, који излази из свог традиционалног облика употребом компјутерске технологије и интернета за покретање напада. Сајбер тероризам подразумева „смишљене, политички мотивисане нападе субнационалних група, тајних агената или појединаца против информационих и рачунарских система, компјутерских програма и података који доводе до насиља.“ [71] „Да би се напади одредили као сајбер тероризам, требало би да резултирају насиљем против лица или имовине или бар да изазову довољно штете за генерисање страха“, који је само средство за постизање политичких циљева. [72] Америчка безбедносна служба (FBI) дефинише сајбер тероризам као планиране, политички мотивисане нападе на

[69] Зиројевић,Фатић, М., *Злоупотреба интернета у сврхе тероризма*, 2011, LXIII, (3), 417–448, стр. 418-421.
[70] Weimann, G., Tsfati, Y., Terror on the Internet, Studies in Conflict & Terrorism, 2002, 25:317–332, стр. 320, 321.
[71] Janczewski, L., Colarik, A., *Cyber Warfare And Cyber Terrorism*, Information Science Reference, New York, 2008, стр. XIII.
[72] Denning, D., *Cyber terrorism: Testimony before the Special Oversight Panel on Terrorism*, Committee on Armed Services U.S. House of Representatives, Georgetown University, May 2000, стр. 1.

рачунарске системе, рачунарске програме, информације и податке од стране суб-националних група или страних агената.[73]

Постоји и ***сајбер рат*** или информациони рат, који се дефинише као унапред „планирани напад од стране једног народа или агената на информације и рачунарске системе, компјутерске програме и податке који доводе до великих губитака.“[74]

Поред информационог рата и сајбер тероризма постоји и феномен ***сајбер криминала*** који „представља такав облик криминалног понашања, једног или више лица у сајбер простору, у којем се рачунарске мреже појављују као средство, циљ, доказ или окружење извршеног кривичног дела.“[75]

Постоје различити облици сајбер криминала:[76]

– *Сајбер шпијунажа* (прикупљање обавештајних података употребом информационо-комуникационе технологије, нпр. систем за надзор комуникација ‘’Eshelon’’ који контролишу пет држава енглеског говорног подручја – САД, Велика Британија, Аустралија, Канада и Нови Зеланд);

– *‘’Хакинг’’* (неовлашћен приступ рачунарским ресурсима, нпр. неовлашћен упад у рачунски систем владиних организација ради остварења одређених политичких циљева);

– *Сајбер саботажа* (оштећење, уништење и на друге начине чињење неупотребљивим података, програма, рачунара или рачунарских мрежа);

– *Сајбер преваре* (подразумева прикривање и лажно приказивање података с циљем се себи или другоме прибави противправна имовинска корист и тиме другом лицу нанесе штета, нпр. наруџба неког производа путем Интернета давајући при томе личне податке друге особе);

---

[73] Elmusharaf, M., *Cyber Terrorism: The new kind of Terrorism*, Computer Crime Research Center, 2004, доступно на: http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism, приступљено: 15. 4. 2015.
[74] Janczewski, L., Colarik, A., *Cyber Warfare And Cyber Terrorism*, Information Science Reference, New York, 2008, стр. XIV.
[75] Вулетић, Д., *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011, стр. 23.
[76] Исто, стр. 24.

– *Криминал везан за садржаје* подразумева производњу и дистрибуцију недозвољених и штетних садржаја на Интернету, нпр. ширење дечијег порнографског материјала, расистичких, нацистичких и сличних идеја и ставова.

– *Криминал везан за производе и супстанце* (рачунарска мрежа се користи за манипулацију забрањеним производима, супстанцама и робама, нпр. трговина дрогом, људским органима или оружјем помоћу Интернета).

– *Повреде приватности* (подразумева долазак до података о личности нпр. коришћењем одређених алата на мреже врши се надгледање електронске поште илиприслушкивање).

Информационе инфраструктуре које су посебно осетљиве и од великог значаја за националну безбедност треба посебно заштити. Ту спадају: енергетски систем, водовод, финансијски сектор, систем безбедности и др. велики државни системи. Вероватноћа напада у великој мери зависи од степена дигитализације организација и друштва, као и од величине и развијености организације.[77]

Најбитнији задаци у заштити критичне националне инфраструктуре су:[78]

- превенција и рано упозорење;
- откривање;
- реакција;
- управљање кризама.

Европска унија је предузела одређене кораке у правцу заштите критичних информационих структура усвајањем стратегије за сајбер сигурност (2013), конвенције о сајбер криминалу, доношењем програма за заштиту критичних инфраструктура, усвајањем акционог плана, као и организовањем бројних конференција земаља чланица, на којима су се износила различита искуства и планирале будуће акивности на плану заштите критичне инфраструктуре.[79] Чињеница да државе односно владе

[77] Вулетић, Д., *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011, стр. 20.
[78] Suter, M., *A Generic National Framework for Critical Information Infrastructure Protection,* Center for Security Studies, Zurich, 2007, стр. 1.
[79] Cybersecurity, доступно на: https://ec.europa.eu/digital-agenda/en/cybersecurity, приступљено: 19. 4. 2015; Вулетић, Д., *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011, стр. 58, 59; Dogrul, M., Aslan, A., Celik, E., *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*, 3rd International Conference on Cyber Conflict, Estonia, 2011, pp. 29-43, str. 38.

немају монопол у области информационих технологија значи да оне не могу да контролишу темпо технолошких достигнућа у комерцијалном сектору. Последица тога је да софистицирану информациону технологију може користити било ко (терористичке и криминалне групе, појединци-хакери, обавештајне службе и др.).[80]

Одбрана од сајбер напада је дуготрајан и сложен процес и подразумева знатне финансијске и људске ресурсе, зато је едукација професионалаца за сајбер безбедност и имплементација нових решења у области заштите информационих система изузетно важна. Сајбер напади су непредвидиви и брзи, и изискују адекватан одговор од стране стручњака за сајбер безбедност, па је зато пожељно формирати тим за одговор на инцидент који ће чинити група експерата за информациону безбедност.[81] Без обзира да ли постоји национални тим за одговор на инцидент, контраобавештајна служба мора имати сектор који ће бити задужен за област информационе безбедности.

Контраобавештајна делатност данас подразумева и заштиту у сајбер простору и њене функције су остале исте: детекција, идентификација, процена, неутрализија или искоришћавање. Посебна пажња треба бити посвећена дефинисању и заштити критичне инфраструктуре која може садржати научне, технолошке, војне податке, државне тајне и др. Заштита критичне инфраструктуре је дефинисана као стратегија, политика, и спремност да се одврати, спречи, а када је то потребно, одговори у случају напада на критичне инфраструктуре.[82] Са друге стране, терористи све чешће користе сајбер простор за комуникацију, па су обавештајне и контраобавештајне службе често онемогућене да врше надзор над комуникацијама због тога што расположивом технологијом могу надзирати само промет између појединих тачно одређених електронских адреса, тј. само пошту која кружи мрежом.[83] Међународна сарадња, размена података и искустава експерата, неопходне су за развој бољих система заштите и превенције таквих напада.

Технологија је одувек имала утицаја на обавештајни и контраобавештајни рад, али никада није променила њихову суштину. Она данас представља моћно средство откривања тајни и крађе тајних података, а такође утиче и на компликације у

[80] Liaropoulos, A., *A (R)evolution in Intelligence Affairs? In Search of a New Paradigm*, Research paper No. 100, Research Institute for European and American Studies, 2006, str. 10.
[81] Вулетић, Д., *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011, стр. 52, 53.
[82] Lewis, G., *Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation*, John Wiley & Sons Inc. Hoboken, New Jersey (USA), 2006, стр. 4.
[83] Зиројевић, Фатић, М., *Злоупотреба интернета у сврхе тероризма*, 2011, LXIII, (3), 417–448, стр. 420.

обавештајној и контраобавештајној пракси повећањем обима доступних информација.[84] Повећан обим доступних информација отежава њихову проверу што доводи до успоравања процеса рада контраобавештајних служби. Са друге стране, капацитети складиштења су драстично повећани, а и знатно је лакше класификовање и претраживање података у сопственој бази употребом савремених програма. Допринос успостављању чвршће сарадње и размени података са другим службама једна је од предности убрзаног развоја информационо-комуникационих технологија, међутим увек треба постојати опрезност приликом дељења таквих података, како не би дошло до изненадних негативних последица по националну безбедност.

Приватни сектор је у многим аспектима напреднији од државног у области информационих технологија, зато је успостављање њихове сарадње од великог значаја за унапређење контраобавештајне заштите критичне инфраструктуре значајне за националну безбедност. Поред овога, успешност контраобавештајне заштите зависи и од спремности на организационе и кадровске промене условљене убрзаним развојем информационих технологија, које производе нове софистициране претње са великим потенцијалом угрожавања националне безбедности.

4. ОПШТИ ПРЕГЛЕД ТЕРОРИСТИЧКИХ НАПАДА У СВЕТУ У 2008. ГОДИНИ

Имајући у виду чињеницу да је тероризам данас једна од највећих безбедносних претњи многим државама, и један од најопаснијих видова политичког насиља, у даљем тексту ће бити укратко приказани подаци о терористичким нападима, жртвама по категоријама и броју повређених и погинулих у свету у 2008. години. Иако крајњи циљ терориста нису људске жртве већ изазивање страха и изнуђивање одређених политичких уступака (стварање политичких и социјалних промена), реализација терористичког акта за последицу може имати велики број повређених и погинулих људи.

[84] Wesley, W., Introduction: „Learning to Live With Intelligence“, Intelligence and National Security, 2003, 18 (4), 1-14, стр. 3,4.

Објекти напада терористa су државни, верски, национални и политички симболи, укључујући ту и обично становништво.[85] „Жртве тероризма су разноврсне, од оних које су уплетене у политичко-идеолошки проблем (циљане- селективне жртве), до оних које с тим немају никакве везе (недужни грађани као деперсонализација државе).“[86]

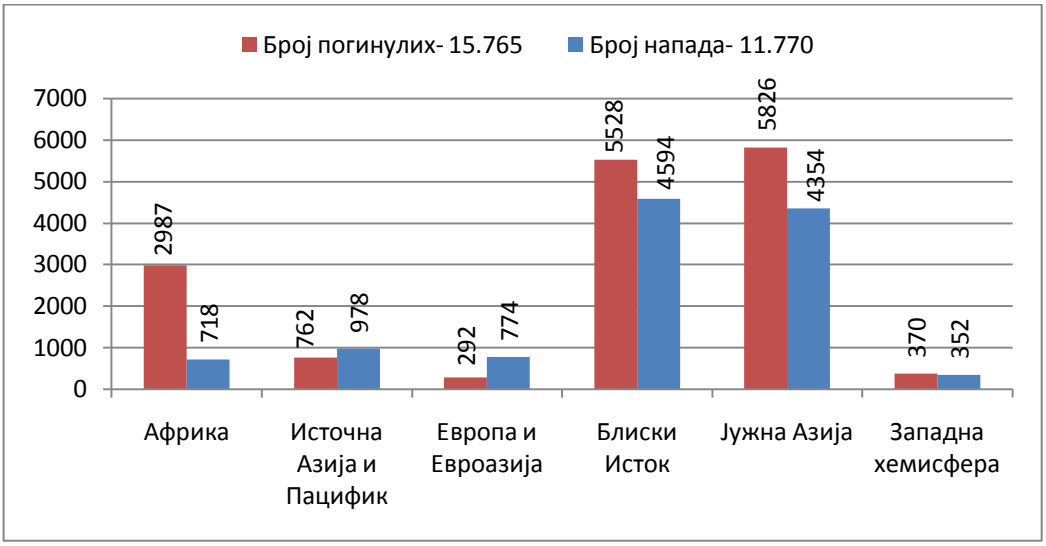


График 1- Поређење броја напада и погинулих у свету у 2008. години[87]

У графицима 1, 2 и 3 представљен је извештај Националног антитерористичког центра (NCTC) о терористичким нападима у свету у 2008. години (број напада и жртава, нападнути објекти по категоријама, број погинулих по категоријама), који је примарна организације у влади САД за интегрисање и анализу свих обавештајних података који се односе на тероризам.

График 1 приказује да је на тлу Европе и Евроазије у 2008. години најмањи проценат погинулих по једном нападу и он износи 0.38 или другачије речено, на сто терористичких напада просечно страда 38 људи. Са друге стране најлошији однос напада и људских жртава је на тлу Африке и он износи 4.16, где на сто напада има 416 људских жртава, при том не треба занемарити чињеницу да је број повређених некада и вишеструко већи од броја погинулих. Поред овога, примећује се драстична разлика у

[85] Симеуновић, Д., *Тероризам: Општи део*, Правни факултет, Београд, 2009, стр. 33.
[86] Милашиновић, Р., Мијалковић, С., *Тероризам као савремена безбедносна претња*, Министарство унутрашњих послова Републике Српске, Висока школа унутрашњих послова у сарадњи са Ханс Зајдел фондацијом, Супротстављање тероризму- међународни стандарди и правна регулатива, Козара, 29-30. март, Висока школа унутрашњих послова, Бања Лука, 2011, 1-16, стр. 4.
[87] National Counterterrorism Center, 30 April 2009, 2008 Report on Terrorism, Office of the Director of National Intelligence National Counterterrorism Center, Washington, стр. 19.

броју напада у регионима Блиског Истока и Јужне Азије. Збирно гледано на просторима ових региона догодило се 76% укупних терористичких напада и 72% укупних жртава у свету у 2008. години. Државе у којима има највише погинулих у оваквим нападима су: Ирак, Пакистан, Авганистан, Индија и др.

График 2- Број терористичких напада у свету према категорији нападнутих објеката у 2008. години[88]

Са графика се може уочити да су саобраћајна средства, заједнице, резиденције и јавна места доминантни објекти терористичких напада у свету, а занимљив податак је да су влада, полиција и војска биле мете у 10% напада.

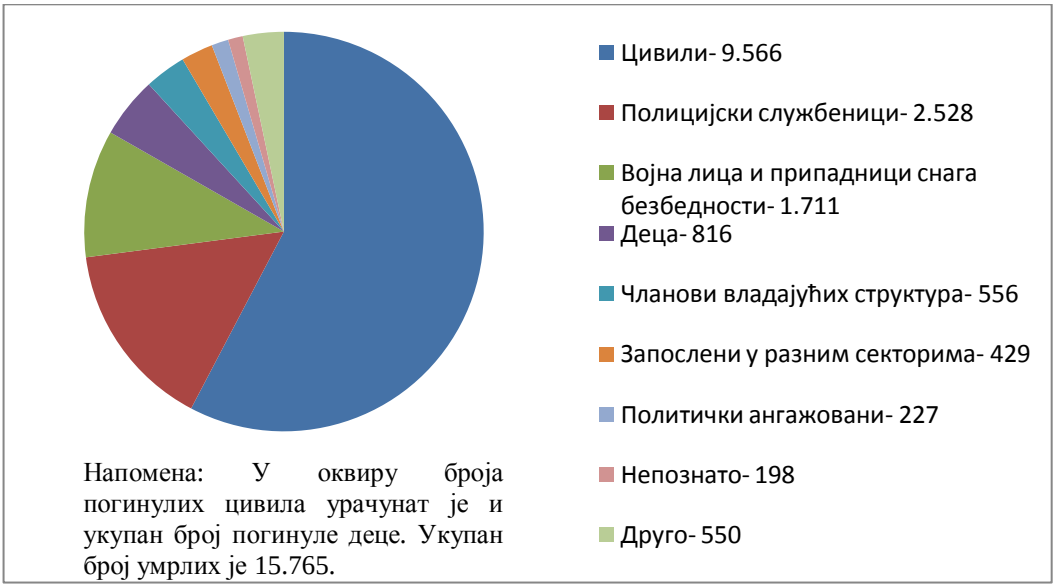


График 3- Број погинулих цивила и службених лица у 2008. години[89]

[88] National Counterterrorism Center, 30 April 2009, 2008 Report on Terrorism, Office of the Director of National Intelligence National Counterterrorism Center, Washington, стр. 30.

Од укупног броја погинулих (15.765), било је чак 61% цивила, 27% полицијских и војних лица, а посебно забрињавајући податак је да је од укупног броја погинулих 5.17% деце.

Велики број жртава, нарочито цивила, показује њихову тежњу ка спектакуларности као суштинском елементу функционисања тероризма. Због своје малобројности желе сваким нападом да оставе што јачи утисак и пошаљу снажну поруку јавности о својим циљевима, ради се заправо о класичној компензацији снаге.[90] Уопштено, њихов циљ је да акцијама насиља према недужнима скрену пажњу домаће и светске јавности на себе, односно да је застраше или придобију за остварење својих циљева и интереса, како би та иста јавност извршила притисак на државу да удовољи захтевима терориста.[91] Терористи своје нападе и убиства невиних људи (цивила-небораца) правдају на разне начине, па и тиме да грађани које они нападају нису невини зато што пружају подршку режимима који угрожавају интересе терориста. Ово објашњење није исправно макар из разлога политичке плуралности западних и других држава, а убијање не малог броја недужне деце у најмању руку показује да је њихово осећање за правду потпуно померено.[92] Међутим, убијање великог броја недужних грађана указује на њихову слабост да се обрачунају са онима којима шаљу поруке, носиоцима државне власти.

4.1. Улога обавештајне и контраобавештајне делатности у превентивном антитерористичком деловању

Борба против терористичких активности страних обавештајних служби незамислива је без обавештајне и контраобавештајне компоненте. Обавештајне и безбедносне агенције су једине надлежне и овлашћене да употребом тајних метода и средстава откривају носиоце тајних припрема и делатности који представљају опасност

---

[89] National Counterterrorism Center, 30 April 2009, 2008 Report on Terrorism, Office of the Director of National Intelligence National Counterterrorism Center, Washington, стр. 23.
[90] Симеуновић, Д., *Тероризам: Општи део*, Правни факултет, Београд, 2009, стр. 40.
[91] Милашиновић, Р., Мијалковић, С., *Тероризам као савремена безбедносна претња*, Министарство унутрашњих послова Републике Српске, Висока школа унутрашњих послова у сарадњи са Ханс Зајдел фондацијом, Супротстављање тероризму- међународни стандарди и правна регулатива, Козара, 29-30. март, Висока школа унутрашњих послова, Бања Лука, 2011, 1-16, стр. 1.
[92] Симеуновић, Д., *Тероризам: Општи део*, Правни факултет, Београд, 2009, стр. 29.

по систем националне безбедности.[93] Контраобавештајна делатност поред онемогућавања спровођења активности шпијунаже, рушења и саботаже, подразумева и спречавање терористичких активности против државе од стране различитих терористичких организација или иностраних обавештајних служби, које посредно или непосредно учествују у оваквим активностима, или других група контролисаних из иностранства. Ове делатности укључују одбрамбене мере као што су истраге, инспекције и праћење, али и офанзивне контраобавештајне мере које подразумевају операције продирања, обмањивања, ометања и вршења других утицаја на ове организације.[94] Оно што је сигурно је да не постоје лака решења и једноставне процедуре за успешно супротстављање овим активностима, већ је за то неопходан читав низ поступака и радњи, који поред обавештајне и контраобавештајне компоненте подразумевају и укључивање великог броја државних органа и институција, које појединачним или здруженим ресурсима и међусобном сарадњом учествују у супротстављању.

5. ОБАВЕШТАЈНЕ И КОНТРАОБАВЕШТАЈНЕ СЛУЖБЕ

5.1. Појам обавештајне службе (дефинисање појма)

Иако је у прошлости имала веома значајну улогу у унутрашњој и у спољној политици држава, а посебно у ратним околностима, обавештајна служба није добила одговарајући третман у званичној историографији. Ниподаштавање њене улоге (резултата рада) и укупног значаја довели су до стварања феномена потпуне мистификације, често и преувеличавања њене улоге, а ту се нажалост губи контакт са науком. Одувек је била повезана са политиком, па и не чуди то што „обавештајна служба увек стоји у функцији политичке власти, којој је подређена и чијим интересима служи.“[95] Све значајније политичке одлуке (посебно ако је реч о спољној политици) доносе се уз претходну проверу обавештајних информација, до којих се долази

[93] Гаћиновић, Р., *Тероризам*, Београд, 200, стр. 329., преузето из: Ђорђевић З., Шаљић Е., *Улога обавештајних служби у борби против тероризма*, Међународна и национална сарадња и координација у супротстављању криминалитету, 2010, 3/1, 500-514., стр. 505.
[94] Ђорђевић, З., Шаљић Е., *Улога обавештајних служби у борби против тероризма*, Међународна и национална сарадња и координација у супротстављању криминалитету, 2010, 3/1, 500-514., стр. 508.
[95] Милашиновић, Р., Милашиновић С., *Основи теорије конфликата*, Факултет безбедности, Београд, 2007, стр. 466.

систематизованим радом. „Свака савремена држава настоји да прикрије властите, а сазна туђе (пријатељске и непријатељске) тајне намере. У том смислу, испреплетеност и различитост интереса у међународним односима, а посебно тајновитост стратегије њиховог остваривања у свакој држави, условљава обавештајну и контраобавештајну делатност. У том процесу обавештајне службе имају посебан значај.“[96] Константна опасност од тероризма, развој наоружања за масовно уништење, велики број конфликата, сложеност и разноврсност савремених претњи, сложеност односа у међународној заједници, и многи други фактори, потврдили су оправданост и неопходност постојања снажних савремених обавештајних служби.

Обавештајна служба је, историјски гледано, прошла кроз више фаза развоја, имајући сталну тенденцију прерастања од неорганизоване ка организованој категорији. Иако су и раније постојале организације које су се бавиле обавештајним радом, она је све до XIX века у највећем броју земаља представљала активност без званичне форме и организације. [97] Неретко се дешава да се обавештајна служба изједначава са шпијунажом, што је апсолутно погрешно, јер шпијунажа представља само један део укупне обавештајне делатности и подразумева „агентурно долажење до тајних података“.[98]

Данас је готово незамислив опстанак државе без обавештајног апарата. Улога обавештајне службе је од непроцењивог значаја, како на спољном, тако и на унутрашњем плану. Према Љ. Стајићу: „Обавештајна служба се данас дефинише као специјализована, релативно самостална институција државног апарата, овлашћена да легалним, али и тајним средствима и методама, прикупља значајне обавештајне податке и информације о другим државама или њеним институцијама и могућим унутрашњим противницима сопствене државе, потребне за вођење политике земље и предузимање других поступака у миру и у рату и да сопственом активношћу, самостално или у сарадњи са другим државним органима, спроводи део државних и политичких циљева земље.“ [99]

Улога обавештајне службе је интегративна у погледу сакупљања, обраде, процене и достављања података. Она често има саветодавну улогу, али без могућности

[96] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 223.
[97] Милашиновић, Р., Милашиновић, С., *Основи теорије конфликата*, Факултет безбедности, Београд, 2007, стр. 470. и 471.
[98] Исто, стр. 475.
[99] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 223.

одлучивања, односно доношења политичких одлука. Контрола над службом се успоставља на више начина, и углавном зависи од политичког система. У парламентарном систему, председник владе је лице које има највећу моћ контроле преко различитих контролних и надзорних тела; у председничком систему контролу спроводи председник државе.

Анализом постојећих дефиниција стиче се утисак да мали број дефиниција обавештајне службе садржи и њене субверзивне активности. Интересантно тумачење обавештајних служби дао је Милошевић М. који поред спровођења обавештајних и безбедносних активности, уводи сегмент субверзивних активности, карактеристичних за савремене обавештајне службе.[100]

Између обавештајних служби и носиоца политичке власти мора постојати складан однос, простије речено, обе стране морају поштовати обавезе преузете у процесу одлучивања. Врхови обавештајних служби не смеју бити отуђени и превише самостални, они морају да ускладе обавештајна истраживања захтевима политичких креатора, координирају израду обавештајних докумената и изврше њихову интерпретацију. [101] Њихова самосталност се односи на оперативни рад (утврђен статутом), који мора бити у складу са законима матичне државе и са међународно-правним прописима.

5.2. Међународна обавештајна сарадња

Сарадња се може одредити као процес споразумевања којим се на равноправној основи врши усклађивање интереса страна које учествују у том процесу ради извршења заједничког задатка. [102] Успостављање и реализација процеса размене обавештајних података има дугу историју и једноставнија је од обавештајне сарадње, која је тек у XX веку постала пракса у обавештајном раду.[103]

[100] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 23.
[101] Бајагић, М., *Шпијунажа у 21. веку- Савремени обавештајно-безбедносни системи*, Београд, 2010, стр. 6.
[102] Група аутора, *Руковођење и командовање*, ЦВШ ВЈ, Војна академија ВЈ, Београд, 1997, стр. 101., преузето из: Лазовић, Р., *Међународна обавештајна сарадња*, Војно дело, 2013, 33-56, стр. 38.
[103] Herman, M., *Intelligence Power in Peace and War*, The Royal Institute of International Affairs, Cambridge University Press, 2003, стр. 200.

Обавештајна сарадња је процес усклађивања обавештајних интереса ради постизања планираних циљева два или више учесника у сарадњи, и укључује активну размену обавештајних података, и широк спектар других активности, нпр. приступ технологији, обука кадра, дељење искустава и знања, заједничке операције и др. Примарни субјекти такве сарадње су националне обавештајне службе, а као секундарни јављају се различите врсте недржавних субјеката, попут обавештајних удружења, обавештајних органа у међународним организацијама, али и приватни обавештајно-безбедносни сектор.[104]

Последњих петнаестак година борба против тероризма упућује на повећање билатералне и мултилатералне обавештајне сарадње, а успоставља се и боља сарадња у националним системима безбедности између обавештајних и безбедносних агенција. Размена података је једна од најизраженијих манифестација обавештајне сарадње након 11. септембра.[105]

Размена обавештајних података, као кључни чинилац обавештајне сарадње, подразумева: [106]

а) дељење специчних, актуелних и понекад веома осетљивих информација у реалном времену;

б) много генералних процена ситуације, трендова и могућности на основу широког спектра тајних и јавних извора.

Неки аутори сматрају да се поверење у обавештајној заједници често изједначава са спремношћу да се преузме ризик понашања других учесника и да оно никада није безусловно. Треба имати у виду да је поверење неопходан, али не и довољан и једини услов за успостављање и одржавање пријатељских међуагенцијских односа у међународној заједници.[107] Тај однос поверења треба стално доказивати, доградивати, нарочито ако се ради о неједнаком односу обавештајних капацитета.

[104] Лазовић, Р., *Међународна обавештајна сарадња*, Војно дело, 2013, 33-56, стр. 39, 41.
[105] Born, H., Leigh, I., Wills, A., *International Intelligence Cooperation and Accountability*, Routledge, 2011, str. 4, 12.
[106] Dorn, N., *European Strategic Intelligence: How far integration?*, Erasmus Law Review, Vol. 5, No. 1, 2008, 163-180, стр. 166.
[107] Hoffman, A., *A Conceptualisation of Trust in International Relations*, European Journal of International Relations, SAGE Publications and ECPR, Volume 8, 2002, стр. 375-401, 376, 377.

Међународна обавештајна сарадња има много облика, од институционалне *ad hoc* размене информација до међудржавних размена обавештајних података. Сарадња се може остварити на билатералном нивоу (најчешћи облик сарадње), мултилатералном нивоу у оквиру удружења и група држава (The Club of Bern, UKUSA Agreement); и обавештајна сарадња у оквиру међународних организација као што су EU и NATO.[108]

Парламентарни и други механизми надзора рада обавештајних служби развијени су у време када је међународна размена обавештајних информација између обавештајних и безбедносних служби била врло ограничена, сходно томе, та тела нису направљена да преиспитују међународну обавештајну сарадњу. Тако у неким државама парламентарни надзорни органи немају мандат да испитују међународну обавештајну сарадњу, а и тамо где поседују мандат често су овлашћења врло ограничена. Не само да не постоји надзор над међународном обавештајном сарадњом, већ ни утврђени стандарди за регулисање обавештајне сарадње, као нпр.: постојање општих стандарда за улазак у споразум (уговор) са другим земљама; постојање посебних стандарда за слање и примање информација и др. [109] Међутим, помаци у билатералним и мултилатералним облицима постоје када је конкретно у питању борба против тероризма и пролиферација оружја за масовно уништење у оквиру УН, ЕУ и НАТО. Приметна је тенденција унапређења обавештајне сарадње, што се види из акционих и извештајних докумената органа ЕУ, пре свега у области борбе против тероризма.

Циљеви обавештајне сарадње се на нивоу општости могу поделити на: [110]

- стратешке циљеве (одређује их политички врх државе);
- оперативне циљеве (одређује их руководство службе);
- тактичке циљеве (одређују се на ниову органа који практично реализују обавештајну сарадњу за сваку појединачну активност).

Највиши ниво обавештајне сарадње је оперативна сарадња, која указује на висок ниво поверења између страна, а остварује се у фазама прикупљања и обраде података. Други специфичан вид обавештајне сарадње је обука и размена кадра, који подразумева трансфер знања, размену научених лекција и јачање професионалних

[108] Born, H., *International Intelligence Cooperation: The Need for Networking accountability*, NATO Parliamentary Assembly Session at Reykjavik, 6 October 2007, str. 2,3.
[109] Исто, str. 4.
[110] Лазовић, Р., *Међународна обавештајна сарадња*, Војно дело, 2013, 33-56, стр. 44.

стандарда, а представља и моћно средство за изградњу међусобног поверења припадника различитих служби. Као трећи специфичан вид обавештајне сарадње јавља се формирање заједничких база података о објектима заједничког интересовања.[111]

Многе савремене безбедносне претње имају транснационалну димензију, а ефикасна одбрана није могућа без сарадње са другим државама, јер капацитети тих претњи превазилазе могућности појединачних држава. У будућности се може очекивати шири обим размене података и обавештајне сарадње, како на међународном тако и на билатералном нивоу, међутим на нивоу међународне заједнице морају постојати чрсти механизми и заједничке структуре сарадње, успостављање аутоматских система за обраду и размену података и др. Генерално гледано, основне предности обавештајне сарадње су: смањење опаративних трошкова (уштеде у буџету који је ограничен), повећање националних обавештајних капацитета и могућност провере доступних података.

5.3. Контраобавештајна служба

Успон обавештајног рада током историје, је слободно се може рећи, мање-више константан, а последње две или три деценије представљају период достизања врхунца обавештајног потенцијала спољних обавештајних служби. Завршетак Хладног рата и након тога настанак новог светског поретка умногоме је утицао на редефинисање националних обавештајно-безбедносних система. Данашње државе су константно оптерећене питањем безбедности у смислу активности које угрожавају њихово државно и друштвено уређење, како од стране унутрашњих политичких противника, који врше различите облике политичког насиља (*основни облици*: политичко убиство, атентат, диверзија итд., *сложени облици*: побуне нереди, немири, тероризам, терор, устанак, рат и др.)[112] у супротности са уставом, тако и од стране страних офанзивних обавештајних служби које врше различите субверзивне и обавештајне активности. Што се тиче сложених облика, често је потребна спољна подршка, што свакако отвара и питање умешаности страних обавештајних служби посредством разних друштвених канала (НВО, дипломатска представништва, појединци у оквиру разних мисија ОЕБС-

[111] Лазовић, Р., *Међународна обавештајна сарадња*, Војно дело, 2013, 33-56 стр. 50, 51.
[112] Симеуновић, Д., *Теорија политике: Ридер I део*, Наука и друштво, Београд, 2002, стр. 155.

а, УН-а и других организација). Да би се одбранила од спољних претњи, (страних обавештајних служби) ове и сличне природе, држава оснива специјализоване установе и организације (контраобавештајна служба, посебно служба за контрашпијунажу) у оквиру свог апарата ради вршења заштитне функције. Потребно је истаћи да се све до половине XX века сматрало да су безбедносни послови били саставни део контраобавештајних активности, и у складу са тим су све специјализоване организације за ове послове носиле назив „контраобавештајна служба“. Заштита сопствене државе била је окренута супротстављању различитим угрожавајућим делатностима страних држава, односно њихових служби, полазило се од тога да је главни непријатељ „нека друга држава“. Из тог разлога се израз контраобавештајна служба користио да означи службу безбедности у целини, што свакако данас није прихватљиво.[113]

„Контраобавештајна делатност је тек од краја XVIII века добила посебне организационе облике. Њу су, током развоја државе, обављали цивилни и војни органи у оквиру својих редовних задатака.“[114] Обавештајне службе су у ранијем периоду, правац свог деловања углавном усмеравале на прикупљање обавештајних података војне природе, самим тим контраобавештајне службе су у почетку биле формиране у оквиру војних структура држава.[115] Тако је, рецимо, у Краљевини СХС постојала војна обавештајна и контраобавештајна служба при Министрарству војске и морнарице.

Претње од стране страних обавештајних служби, које нису своје активности усмеравале искључиво ка војном сектору, већ су постепено проширивале своје активности на разне друге области, утицале су на формирање цивилних контраобавештајних служби, претежно при Министарству унутрашњих послова. Развој офанзивних обавештајних служби условио је развој контраобавештајних служби, како у смислу прогреса у погледу обуке кадрова, специфичних метода и средстава, тако и у смислу проширења делокруга њиховог рада. Узимајући то у обзир, може се рећи да контраобавештајна служба еволуира у службу безбедности, јер не користи превасходно само обавештајне методе у супротстављању другим службама, већ примењује и читав низ контраобавештајних и безбедносних мера којима онемогућава њихов рад.

---

[113] Милошевић, М., *Одбрана од тероризма*, Свет књиге, Београд, 2005, год., стр. 92, 93. преузето из Лукић, Д., *Савремена шпијунажа*, Привредна штампа, Београд, 1982., стр. 121.; Савић, А., и др, *Основи државне безбедности*, ОИЦ, Београд, 1988, стр. 44.

[114] Развој контраобавештајне делатности, доступно на: http://www.vba.mod.gov.rs/I_faza.html#.VI9CQ8kl9fw, приступљено 20. 11. 2014.

[115] Милошевић, М., *Одбрана од тероризма*, Свет књиге, Београд, 2005, стр. 94.

Неке од безбедносних мера које примењују контраобавештајне службе јесу: контрола границе, поморских и ваздушних пристаништа, општа контрола странаца, контрола избеглица, ограничење кретања и саобраћаја, физичко обезбеђење објеката, ограничења у јавном објављивању одређених информација и слично.[116]

„Оперативни елемент обавештајно-безбедносног система државе сачињавају обавештајне и безбедносне службе. С обзиром на то да највећи број држава у савременом свету има више обавештајних и безбедносних служби, те да је једна од њих централна (главна) а друге ресорне, овај елемент се разликује од државе до државе и подложан је честим променама (реформама) у смислу промене назива одређених служби, формирања нових, укидања неких дотадашњих и слично.“[117] Промене назива, укидање и формирање нових служби, условно јесу честе појаве, и неретко се дешава да оне буду пратилац глобалних безбедносних дешавања и промена, као и промена у самом друштвеном уређењу једне земље. Њихова основна улога и задаци се врло ретко потпуно мењају, евентуално долази до одређеног степена прилагођавања постојећим безбедносним потребама.

Данас је готово немогуће замислити одрживост обавештајно-безбедносног система без постојања контраобавештајних служби или контраобавештајне делатности у оквиру постојећих безбедносних институција. Свака развијенија држава тежи јачању и унапређењу безбедносног сектора, па самим тим и унапређењу контраобавештајних активности, јер да би опстала, (сачувала своје структуре и становништво), и даље напредовала, прво се мора заштити како од унутрашњих, тако и од спољних непријатеља који организују и спроводе обавештајне и субверзивне активности. У том смислу, контраобавештајна служба представља „специјализовану организацију државног апарата која специфичним методима и средствима спроводи контраобавештајне и антисубверзивне активности против противничких обавештајних служби, с циљем откривања, спречавања и сузбијања њиховог деловања, заштите унутрашње и спољне безбедности државе, односно другог одговарајућег ентитета, као и заштите сопствених интереса и дезинформисања актуелног и потенцијалног непријатеља.“[118]

[116] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд 2001, стр. 167, 168.
[117] Мијалковски, М., *Обавештајне и безбедносне службе*, Факултет безбедности, Службени гласник, Београд, 2009, стр. 41,42.
[118] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр.167.

Овој дефиницији би можда требало додати да се коришћење специфичних метода и средстава одвија у тајности и да је рад припадника контраобавештајне службе ограничен постојећим законом о њеном раду, у коме су најчешће њихова овлашћења прецизно дефинисана. Офанзивна и одбрамбена улога служе да онемогуће и неутралишу непријатељске намере непријатеља (њихових служби) или да искористе самог непријатеља за сопствену корист.

Према документима ЦИА-е, са којих је скинута ознака тајности, контраобавештајна организација подразумева кадрове, који својим радом производе контраобавештајно знање, укључујући ту вештине које поседују и методе рада, као и постојање организованих досијеа података. У пракси, на терену појединачни кадрови су најчешће експерти за једну или неколико неопходних области, на пример за везу. Контраобавештајна организација подразумева постојаност и континуитет рада на досијеима, као и сталну надограгрању искуства оперативног и штабног особља. Контраобавештајне организације се морају одликовати непристрасношћу, јасноћом и професионализмом из кога произилази знање неопходно за заштиту и очување војске, економске и продуктивно снаге САД. Изградња и одржавање високог квалитета рада контраобавештајних служби може позитивно деловати на грађане у смислу лојалности и сарадње, али и јавног признања квалитетног рада, може подстицати законодавство, и бити осног судског деловања, и бити водич извршној власти у успостављању безбедносних мера.[119]

Задаци контраобавештајне службе могу се свести на спречавање односно онемогућавање обавештајних и субверзивних делатности стварног или потенцијалног непријатеља. С обзиром на чињеницу да је базична делатност контраобавештајних служби била и остала обавештајна делатност, подразумевајући под тим прикупљање, обраду и достављање података, може се констатовати да она представља вид обавештајне делатности. Поред ове делатности, савремена контраобавештајна служба предузима и извршне радње, цивилне и војне мере у домену шпијунаже, диверзије, саботаже и других видова субверзивне делатности.[120]

Субверзивна делатност као неоружани облик угрожавања представља подривачку делатност из иностранства против друштвеног и политичког уређења или

[119] Counterintelligence for National Security, доступно на: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a10p_0001.htm приступљено: 25.11.2014.
[120] Милошевић, М., *Одбрана од тероризма*, Свет књиге, Београд, 2005, стр. 94, 95.

њених виталних институција. Да би обавештајне службе страних држава успешно спровеле различите облике субверзивне делатности, морају пре свега добро познавати претходно и тренутно стање у земљи, али и добро предвидети правце развоја даљих догађаја. Са друге стране, радећи на откривању страних агената (укључујући њихов начин рада, методе и средства), контраобавештајне службе истовремено прикупљају доказе о њиховом штетном раду и те податке предају другим службама безбедности или полицији, који у складу са овлашћењима онемогућавају њихов даљи рад, у случају да се ради о неоперативној служби.[121] Неоперативна служба се разликује од оперативне по томе што у својој надлежности нема извршна овлашћења, те послове уместо њих раде други органи. Са друге стране, оперативне службе предузимају репресивне мере и истражне радње уколико за тим има потребе. У случају да се ради о агенту у оквиру редовне или специјалне дипломатске мисије, та особа се проглашава за непожељну личност-*persona non grata*. Међутим, оперативне службе једино што могу урадити у случају откривања активности дипломате, против поретка земље у којој је акредитован је да обавесте доносиоце политичких одлука, или да у сарадњи са њима предузму одређене мере безбедности, а све у складу са законом.

„Дипломатски представници уживају кривично-правни и грађанско-правни имунитет, они могу бити изведени пред суд само од стране њихове сопствене земље.“[122] Са друге стране „за кривично дело може да одговара и страни правни субјект под условом да се по праву Републике Србије сматра правним лицем.“[123] Пример је регистрована страна организација која у оквиру својих редовних активности обавља и послове који имају везе са обавештајним и субверивним радом.

Није свака контраобавештајна служба оперативна, то пре свега зависи од обавештајно-безбедносног система државе, његове сложености, структуре, потреба и др. Рад сваке службе је ограничен законом, који прописује овлашћења и ограничења њеног рада, односно рада професионалних припадника службе, у коме се између осталог и наводи да ли је служба оперативна или неоперативна.

Вербовање непријатељских агената јесте једна од могућности коју контраобавештајне службе користе како би обавиле одређене задатке и

[121] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 168.
[122] Аврамов, С., Крећа, М., *Међународно јавно право*, Београд, Савремена администрација, 2003, стр. 154.
[123] Илић, Г., *Маргиналије уз закон о одговорности правних лица за кривична дела*, CRIMEN (I) 2/2010, 246–256, стр. 248.

дезинформисале службу за коју агент ради.[124] Много је таквих случајева, а неки од најпознатијих се везују за период Хладног рата и двоструких агената на релацији Велика Британија-СССР или САД-СССР.

Контраобавештајна служба се бави и откривањем и идентификацијом обавештајаца противничких служби; прати њихов рад и процењује способности; ради на утврђивању слабих тачака и мана; разоткрива локације обавештајних центара; прати њихове контакте са другим лицима и организацијама; открива и прати друге видове делатности; предузима одговарајуће мере којима им онемогућава рад и извештава носиоце политичке власти и друге субјекте система безбедности у циљу ангажовања на сузбијању активности противника.

Поред овога, ради на идентификацији структура, објеката и других безбедносно интересантних циљева, који могу бити предмет истраживања страних служби, самим тим открива намере и њихове методе рада што јој користи за креирање ефикаснијег система заштите тих структура.[125] Контраобавештајна служба се бави и планирањем, организовањем и реализацијом послова којима штити своје интересе и тајне, као и одређених политичких структура, спроводи унутрашњу контролу својих припадника, а бави се и заштитом одређених безбедносно осетљивих радних места у структури државе, на којима постоји могућност злоупотребе тајних података због честог додира запослених са таквом врстом података. [126] Контраобавештајна служба се бави и контраобавештајном заштитом великих и важних индустријских комплекса у својој земљи, као што је област војне индустрије (коју обично штити војна контраобавештајна служба). Заштита одређених личности подразумева контраобавештајну и општебезбедносну функцију, и у складу са тим контраобавештајна служба обавља контрадиверзионе и противприслушне прегледе просторија у којима одседа личност коју штите. Сталну заштиту углавном имају водећи носиоци политичке власти државе, као што су председник државе или председник Владе.

[124] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр.168.
[125] Исто, стр. 168.
[126] Исто, стр. 168, 169.

5.3.1. Организација и класификација контраобавештајних служби

Контраобавештајна служба, у зависности од државног и друштвеног уређења, унутрашње организације, степена централизације контраобавештајне активности, може бити различито организована у различитим обавештајно-безбедносним системима. Према М. Милошевићу, управљање контраобавештајним радом може бити:[127]

- *централизовано* (једна установа управља и цивилном и војном контраобавештајном активношћу)
- *делимично подељено* (подела контраобавештајне службе на војну и цивилну, али свака засебно има обједињену управу)
- *потпуно подељено* (одвојено постојање ресорних цивилних и видовских војних контраобавештајних служби).

У складу са тим, а узимајући у обзир и правце активности као и потребе обавештајно-безбедносног система државе, контраобавештајне службе се могу поделити на: офанзивне и дефанзивне, односно ресорне и територијалне. Дефанзивне се могу поделити на оперативне и неоперативне,[128] о чему је већ било речи у поглављу под бројем 5.3.

Најчешћи офанзивни принципи контраобавештајне службе су принцип обмане и принцип неутрализације. Принцип *обмане*, подразумева стварање заблуде код непријатеља при доношењу одлука о неким аспектима деловања агенције, или о њеним способностима и намерама. Послови обмане могу бити усмерени на стварање конфузије, одлажући могућност непријатељске службе да ефикасно реагује, или на пројектовање погрешног/лажног разумевања, који је упућује на трошење времена и ресурса. Применом принципа *неутрализације* може се блокирати прикупљање података од стране страних, противничких обавештајних служби. Он је заснован на концепту пораза, неуспеха или пропасти и подразумева уништење и блокаду непријатељских планираних акција.[129]

[127] Милошевић М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 171.
[128] Исто, 171.
[129] Prunckun, H., *Extending the theoretical structure of intelligence to counterintelligence*, Salus Journal, 2014, Issue 2, Number 2, 31-49, стр. 43, 44.

Када је реч о дефанзивним принципима, треба издвојити принцип одвраћања и принцип откривања или детекције. Принцип *одвраћања* се односи на способност спречавања непријатеља да приступи важним информацијама. Контраобавештајна (безбедносна) служба мора бити способна да причини велику штету противнику, док непријатељске службе морају бити свесне опасности којој се излажу приликом прикупљања одређених података. Принцип *откривања или детекције* подразумева уочавање извршене радње, која је повезана са преступом или потенцијалним злоупотребом поверљивих информација. Постоји пет претпоставки које се односе на остваривање принципа детекције и то су: [130]

1. Идентификација догађаја од великог интереса/значаја

2. Идентификација лица, учесника догађаја

3. Идентификација организација за које су одређена лица заинтересована

4. Утврђивање тренутне локације ангажоване особе/а

5. Прикупљање чињеница које потврђују да је лице починило одређено дело.

Узимајући у обзир правце активности и организацију контраобавештајног рада, контраобавештајне службе се могу поделити на офанзивне и дефанзивне, односно на ресорне и територијалне.

5.3.1.1. Офанзивна контраобавештајна служба

Основни задатак офанзивне контраобавештајне службе је организација и реализација контраобавештајних активности на откривању деловања противничких обавештајних служби на његовој територији. [131] Офанзивна контраобавештајна служба врши класичну шпијунажу према противничким обавештајним службама и то продором у оне структуре из којих се организује и управља обавештајним активностима,[132] као што су: централа (у оквиру централе: јединица за оперативне

[130] Prunckun, H., *Extending the theoretical structure of intelligence to counterintelligence*, Salus Journal, 2014, 2, (2), 31-49, стр. 40, 41.
[131] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 171.
[132] Исто, стр. 172.

послове, јединица за аналитичке послове, јединица за послове везе, за документацију итд.); центри (одсеци), подцентри, и други организациони нивои.

Циљеви овакве офанзивне контраобавештајне делатности према противничким службама јесу првенствено откривање начина рада, метода као и средстава које користе и њихових података.[133] За разлику од дефанзивне контраобавештајне службе, која је организована тако да ради на спречавању противничких служби на сопственој територији, офанзивна својим ангажманом (активностима) на теритоји противничке државе угрожава њен суверенитет. Угрожавање државног суверенитета овим начином, без обзира на степен угрожавања, наводи на закључак да данас не постоји држава која је апсолутно суверена.

Офанзивним продором у структуре противника, она се ангажује на прикупљању сазнања и података о сопственим изворима до којих је дошла непријатељска служба, а који се у њима налазе. Тиме се постиже правовремено откривање битних сазнања противника, како би извори у његовим структурама били заштићени од деконспирације, или како би спречили противничку обавештајну службу да их врбује и тако створи двојне комбинације. По правилу офанзивна контраобавештајна служба нема свој организациони облик, већ послове из њеног делокруга рада обавља офанзивна обавештајна служба или служба безбедности.[134]

5.3.1.2. Дефанзивна контраобавештајна служба

Дефанзивна контраобавештајна служба се ангажује на заштити тајних података, одбрани значајних државних институција и државних органа на сопственој територији од противничких офанзивних обавештајних служби. Назив дефанзивна или одбрамбена се односи на ограниченост деловања у оквирима сопствене државе, а не на њену концептуалну оријентацију, јер је она свакако офанзивна у својим активностима. Дефанзивне контраобавештајне службе постоје као посебне организације али и као сектори рада служби безбедности, а неке од најпознатијих таквих служби јесу: FBI

[133] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 172.
[134] Исто, стр. 172.

(САД), Дирекција за надзор територије-DST (Француска) и Уред за заштиту устава-BfV (Немачка). [135]

5.3.1.3. Ресорна и територијална контраобавештајна служба

Ресорна контраобавештајна служба се ангажује на заштити одређеног ресора или његових делова, који су у безбедносном смислу најрањивији, па се њен задатак своди на онемогућавање продора страних агентурних мреже у те структуре и узимање тајних података. Територијална, користећи своје методе, средства, радње и мере, ради на заштити целе државне територије или једног њеног дела. Оне се често јављају као сектор рада служби безбедности у административно-територијалним јединицама, или ужим друштвено-политичким јединицама. [136]

[135] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 173.
[136] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 173, 174.; Милошевић, М., *Одбрана од тероризма*, Свет књиге, Београд, 2005, стр. 99.

6. КОНТРАОБАВЕШТАЈНА ДЕЛАТНОСТ

6.1. Основна схватања и карактеристике контраобавештајне делатности

Од окончања Другог светског рата обавештајна компонента прераста у један од три основна инструмента у стратегијама националне безбедности, поред дипломатије и војне силе. Већина безбедносних служби у развијеним државама су бирократизоване у тој мери да су постале инертне институције које су превише споре и троме у суочавању са новим изазовима. Међутим, треба напоменути и да је дошло до повећања субверзивних капацитета обавештајних служби, тако да свака држава настоји да унепреди контраобавештајну делатност, како би на прави начин одговорила на нове изазове у погледу националне безбедности.

Све савремене државе чешће се суочавају са мирнодопским, односно невојним претњама, него са ратовима, који се релативно ретко догађају у односу на организовани криминал, тероризам, корупцију, политичку и социјалну нестабилност који су стално присутни у свакој држави.[137] У савременим условима међународних односа, контраобавештајна активност је један од примарних елемената националне снаге сваке државе. Приметно је прилагођавање контраобавештајног рада глобализацијским трендовима, који са собом носе и многе штетне последице по националну безбедност. Развој офанзивног деловања обавештајних служби, ширење транснационалног тероризма (како групног тако и индивидуалног тероризма), пролиферација оружја за масовно уништење, пораст организованог криминала, само су неке од претњи које својим потенцијалом деструкције посредно утичу и на реорганизацију и јачање контраобавештајних капацитета држава.

Данас су обавештајне претње по националну безбедност сваке државе много агресивније, дифузније, технолошки софистицираније и успешније у односу на ранији период. Да би се правовремено и ефикасно заштитиле, државе морају ускладити своју законодавну политику новим изазовима, ризицима и претњама по националну

[137] Драгишић, З., *Систем националне безбедности: Покушај дефинисања појма*, Војно дело 3/2009, стр. 172.

безбедност.[138] Оне усвајају нове стратегије националне безбедности, стратегије контраобавештајног рада, као широке платформе на основу којих усвајају конкретне законе из ових области. Да у области контраобавештајног деловања има динамике и промена у погледу доношења нових стратегија и закона, показује и пример САД-а, које су у периоду од 2005. до 2010. године четири пута усвајале односно модификовале националну стратегију контраобавештајне делатности. Генерално, сваки систем националне безбедности своју динамичност и прилагодљивост изражава кроз способност прилагођавања новим безбедносним изазовима, ризицима и претњама.[139]

Поред усвајања стратегије, која је од великог значаја, често се намеће потреба брже интеграције националних контраобавештајних капацитета, која се може постићи иновирањем контраобавештајне мисије и циљева, побољшањем кадровских, техничких и других контраобавештајних потенцијала, уз већу безбедносну сарадњу са партнерским односно пријатељским државама.[140] Успешност контраобавештајне делатности зависи од много фактора, а неки од њих могу бити и законске препреке или надлежности за одређене послове, који могу представљати неопходан корак у реализацији контраобавештајног рада. Узимајући у обзир и чињеницу да су обавештајне претње доста разнолике и софистициране, јасно је да контраобавештајна активност мора редефинисати своју улогу, и ширити обим свог деловања у складу са тренутним или будућим безбедносним стањем у непосредном окружењу, и у међународној заједници.

Борба против продора страних обавештајних служби није једина претња по националну безбедност. Постоји широк круг претњи које контраобавештајне службе морају изнова идентификовати и предузимати превентивне и системске активности ради њиховог неутралисања. Политички одлучиоци су ти који одређују безбедносне приоритете у датом тренутку, али и стварају законски оквир, који пружа одговарајуће могућности, али и ограничава контраобавештајну делатност. Наравно, не треба стварати средину у којој се одобрава прекорачење овлашћења, или службама омогућава много више слободе у раду него што је то потребно у извршавању њихове делатности, али свакако треба направити праву равнотежу деловања у складу са

[138] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 46, 47.
[139] Драгишић, З., *Систем националне безбедности- покушај дефинисања појма*, Војно дело 3/2009, стр. 169.
[140] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 47.

актуелним претњама и легалним могућностима супротстављања. Данас се контраобавештајна активност све више креће у правцу офанзивности, у настојању да открије обавештајне и субверзивне планове, потенцијале и акције страних сила пре њиховог изазивања негативних последица, притом неретко долази до преплитања офанзивних контраобавештајних потенцијала са обавештајном активношћу, све у циљу очувања и унапређења националне безбедности.[141]

Контраобавештајна делатност продукује сазнања која не употребљава само контраобавештајна организација већ и тужилаштво, законодавац, команданти и руководиоци који утврђују безбедносне мере. Пошто постоји тенденција да се контраобавештајна делатност и безбедносне мере третирају као синоними, треба напоменути да када се говори о безбедносним мерама претежно се мисли на одбрамбене техничке уређаје и процедуре који се примењују од стране извршне власти ради заштите.[142] Процедуре се успостављају на основу искустава обавештајних и контраобавештајних служби. Контраобавештајна активност обухвата прикупљање информација и спровођење активности на заштити од шпијунаже, других обавештајних активности, међународних терористичких активности, атентата од стране или у корист страних влада, или њихових елемената, страних организација или страних лица.[143]

Контраобавештајна делатност подразумева активности посредством којих се идентификују и ублажавају претње по националну безбедност, које изазивају непријатељске обавештајне службе, организације или појединци који се баве шпијунажом, саботажом, субверзијом или тероризмом.[144] Контраобавештајна делатност пружа информације које руководиоци цивилних и војних агенција искоришћавају у процесу доношења одлука, при успостављању безбедносних мера.

Контраобавештајна истрага се спроводи онда када постоје индиције да неко у име стране владе, организације, терористичке групе или неког другог субјекта организује или спроводи шпијунажу или необавештајне активности (као што су: саботажа, побуњеничка, терористичка и превратничка делатност, изазивање и управљање кризама и др.). Резултати контраобавештајних истрага могу пружити

[141] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 47, 48.
[142] CIA, *Counterintelligence for National Security*, Center for the Study of Intelligence, 2(4), 1993.
[143] *The Definition of Counterintelligence*, National Security Act of 1947, Congressional declaration of purpose-50 U.S.C.401. , January 3, 2012, United States Code
[144] Cooper, B., *CFIS: A Foreign Intelligence Service for Canada*, Canadian Defence & Foreign Affairs Institute, 2007, стр. iv

доказне елементе за кривично гоњење одређених лица, такође, оне могу бити и основа за спровођење контраобавештајних операција, а на основу њих се може потврдити и подобност особља за приступ поверљивим подацима.

Контраобавештајне истраге су веома важан сегмент контраобавештајног рада и због чињенице да пружају информације које ако се на прави начин искористе доприносе не само отклањању активних претњи, већ и смањењу рањивости система и побољшању целокупног безбедносног амбијента.

Појмови контраобавештајна делатност и контрашпијунажа имају сличности, али је потребно указати на њихове разлике, како не би долазило до њиховог изједначавања, односно појмовног преклапања. У наредном делу текста ће бити дефинисана контрашпијунажа.

У најужем смислу, шпијунажа би се могла свести на агентурну активност усмерену на прибављање тајних података. Укључујући кривично-правни аспект, шпијунажа представља онај део обавештајне делатности, који се по међународном праву или унутрашњим законским прописима држава може квалификовати као кривично дело шпијунаже. Скоро све државе света инкриминишу шпијунажу у својим кривичним законицима, разлози за то леже у простој чињеници да је усмерена на задовољење интереса „друге стране“ а поред тога садржи елементе издајничког, неморалног, односно непријатељског понашања.[145]

Контрашпијунажа се може представити као део контраобавештајне делатности која подразумева онемогућавање и супротстављање деловању непријатељских служби, употребом конспиративних метода.[146]

Контраобавештајна делатност подразумева активности на заштити тајни и блокирању покушаја обавештајних служби других држава да те тајне и добију преко својих шпијуна, који стоје иза тих покушаја. [147] Потпуније дефинисање би поред прикупљања информација и блокирања планова страних обавештајних служби обухватало и спровођење офанзивних (као подједнако битних) активности и противсубверзивних активности.

[145] Милашиновић, Р., Милашиновић, С., *Основи теорије конфликата*, Факултет безбедности, Београд, 2007, стр. 475-476.
[146] Милошевић, М., *Одбрана од тероризма*, Свет књиге, Београд, 2005, стр. 96.
[147] Wettering, F.,.: *„Counterintelligence: The broken triad“*, International Journal ofIntelligence and CounterIntelligence, 2000, 13:3, 265-300, стр. 265.

„Дефанзивна улога обухвата откривање и пресецање обавештајних продора страних обавештајних служби, израду поверљивих извештаја о страним обавештајним операцијама, безбедносну селекцију кадрова у институцијама власти, планирање и успешно извођење различитих и сложених безбедносних операција, а офанзивна улога подразумева продоре у структуре непријатеља, хватање страних шпијуна и двоструких агената, пласирање дезинформација, коначно и уништење непријатељских обавештајних установа.“[148]

Важно је истаћи да поред великог броја дефиниција контраобавештајне делатности, постоје и различита тумачења у оквиру различитих земаља, чији се приступи овој области разликују.

6.2. Дефинисање контраобавештајне делатности

Постоји много дефиниција контраобавештајне делатности али се ни једна не сматра универзалном. У наредном тексту биће представљене још неке од дефиниција контраобавештајне делатности.

Према Кембрицовом (Cambridge) електронском речнику, контраобавештајна делатност је тајна активност коју једна земља спроводи са циљем спречавања друге земље да открије њене војне, индустријске или политичке тајне.[149] Контраобавештајну делатност чине активности и методе које земља користи да заустави непријатељске земље у откривању њених тајни.[150]

Према Роју Годсону (Roy Godson) главни задатак контраобавештајне делатности је да идентификује, неутралише претње и искористи обавештајне податке које поседује о непријатељском обавештајном раду, користећи своја одбрамбена и нападачка средства. [151]

[148] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 48.
[149] Counterintelligence, Cambridge dictionary, доступно на: http://dictionary.cambridge.org/dictionary/british/counterintelligence, приступљено: 5. 1. 2015.
[150] Counterintelligence, MACCMILLAN Dictionary, доступно на: http://www.macmillandictionary.com/dictionary/british/counterintelligence, приступљено: 5. 1. 2015.
[151] Godson, R., *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence*, Transaction Publishers, New Brunswick, New Jersey, Third printing 2004, str. xxviii.

Према Башкатову и сарадницима, контраобавештајна делатност је традиционално важан елемент очувања безбедности појединаца, друштва и државе. Истовремено, њена затворена природа не дозвољава јавности увид у њену делатност и разумевање друштвеног значаја.[152]

Према Милану Милошевићу, „под контраобавештајном активношћу најчешће се подразумева посебан вид обавештајне делатности који има за циљ заштиту тајних података сопствене државе, одбрану виталних државних органа и институција и спречавање деловања противничких обавештајних служби на територији своје земље.“[153]

Према Националном контраобавештајном и безбедносном центру САД-а контраобавештајна делатност подразумева послове идентификовања и суочавања са страним обавештајним претњама по безбедност САД. Главни актери против којих су усмерене активности су: обавештајне службе страних држава, и сличне организације недржавног типа(недржавни субјекти), као што су транснационалне терористичке групе. Контраобавештајна делатност има *дефанзивни задатак* -штити тајне и имовину нације од страних обавештајних продора и *офанзивни* -сазнаје планове страних обавештајних организација продором у њихове структуре.[154]

Према извршној наредби председника Регана (12333) „Контраобавештајна делатност подразумева прикупљене информације и активности усмерене на заштиту од шпијунаже, других обавештајних активности, саботаже или атентата, спроведених за или у име страних сила, организација или појединаца, или међународних терористичких активности, али не укључујући програме заштите персонала, објеката, докумената и комуникација.“[155]

Обавештајни комитет Сједињених држава (United States Senate Select Committee on Intelligence- SSCI) је у свом извештају дефинисао контраобавештајну делатност као посебан облик обавештајне активности, чија је сврха откривање страних обавештајних

[152] Башкатов, Л. Н., Изоитко, С. И., Козилов, Е. Н., Устинков, А. В., *Контрразведывательная и оперативно-розыскная деятельность органов федеральной службы безопасности* (соотношение и правовое регулирование), Журнал: Право и безопасность, 2010, 1 (34), , 9-18, стр. 9.
[153] Милошевић, М., *Одбрана од тероризма*, Свет књиге, Београд, 2005, стр. 93.
[154] Office of the Director of National Intelligence, National Counterintelligence and Security Center, н.д., доступно на: http://ncix.gov/about/index.php (приступљено 9.1.2015.).
[155] Definitions: Counterintelligence, The provisions of Executive Order 12333, Dec. 4, 1981, United States intelligence activities; Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 48.

операција и њихово уништавање. Формално посматрано, она је обавештајна активност посвећена подривању планова непријатељских обавештајних служби, ради заштите нације.[156]

„Закон о Федералној служби безбедности Руске федерације дефинише контраобавештајну активност као делатност којом се откривају, одвраћају и пресецају обавештајна и друга опасна деловања страних обавештајних служби, организација, појединаца, усмерених на угрожавање безбедности Руске федерације.“[157]

Контраобавештајна делатност је веома сложен појам, који се не може свести искључиво на послове откривања и хватања шпијуна, већ се односи на целовито и темељно разумевање и неутрализацију свих аспеката обавештајне активности као претње по националну безбедност.[158] Појам *counterintelligence* треба схватити као активност, знање и организацију, односно прикупљачка активност, специфично обавештајно сазнање (од великог значаја у политичком одлучивању) и организација која реализује контраобавештајне активности.[159]

6.3. Примарне функције контраобавештајне делатности

Основне функције контраобавештајне делатности (представљене кроз поделу), на које се надовезују и друге функције су:[160]

1. заштита сопствених тајни и прикупљање информација о страним обавештајним службама и њиховим активностима и намерама;

2. откривање активности страних обавештајних служби и њихових позиција у сопственим структурама;

---

[156] Select Committee to Study Governmental Operations with Respect to Intelligence Activities (April 26, 1976), Foreign and Military Intelligence, Book I –Final Report, Washington, U.S. Government Printing Office.

[157] Федеральный закон Об органах Федеральной службы безопасности в Российской Федерации, 03.04.95, Но. 40-ФЗ (СЗ Но. 15-95 г. ст. 1296), Принят Государственной Думой 22 февраля 1995 г., С изменениями и дополнениями 30.12.99.. цитирано према: Бајагић М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 49.

[158] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 48. стр.

[159] CIA, *Counterintelligence for National Security*, Center for the Study of Intelligence, 1993, 2 (4), 87-92, str. 87-91.

[160] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 52, 53.

3. истраживање и анализа структуре, кадрова и операција страних служби;

4. операције уништавања и неутралисања потенцијала страних обавештајних и безбедносних служби које предузимају субверзивне и друге активности против националних интереса и националне безбедности.

Заштита сопствених тајни као прва функција контраобавештајног рада подразумева успостављање заштитних система на радним местима, која су у безбедносном смислу „рањива“ и од посебног националног интереса. Она се могу штитити: физички, техничким средствима, заштитним режимом и персонално. Физичка и техничка заштита се остварују онемогућавањем приступа у просторије непозваним лицима, односно контрадиверзионим средствима, инсталирањем видео надзора и уграђивањем алармних уређаја. Заштитни режим радних места подразумева нормативно уређење поступања са тајним документима (одређивање степена тајности, начина на који се документа преносе између одређених органа, лица која могу бити упозната са садржином одређених докумената и др.). Персонална заштита се постиже испуњавањем прописаних безбедносних квалитета од стране запослених лица.[161]

Откривање страних обавештајних активности обухвата идентификацију разноврсних појавних облика присуства обавештајних активности страних служби, применом проактивних безбедносних мера и динамичким прикупљањем (контра)обавештајних сазнања о страним обавештајним продорима.[162]

Анализом обавештајне активности противника или савезника, конкурената или партнера, отвара се могућност откривања њихових интересовања, сврхе и планова, али и могућност припреме одбране или противнапада. [163] Потребно је омогућити анализирање узрока претходних догађаја како би се идентификовали ризици и места рањивости.[164]

Уништавање и нутралисање потенцијала страних обавештајних служби „подразумева примену најофанзивнијих мера, радњи и поступака, којима се правовремено и ефикасно може спречити штетно дејство страних непријатељских

[161] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 169.
[162] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 53.
[163] Michelle, K., Van C., *Intelligencer: Journal of U.S. Intelligence Studies*, 2013, Volume 20 • Number 2, 57-65, стр. 61.
[164] Counterintelligence, Department of the Navy-Headquarters United States Marine Corps, Washington, D.C. MCWP 2-14, 5 September 2000.

ентитета.“ Неутралисање страних обавештајне претњи је суштински део процеса заштите тајни.[165]

Основне функције контраобавештајног сектора у САД-у су: [166]

1. Идентификација

2. Процена

3. Неутралисање

4. Експлоатација страних обавештајних активности усмерених против САД-а

6.4. Основни принципи контраобавештајног рада

Постоје принципи који се могу сматрати универзалним и којих се генерално придржавају све обавештајне и контраобавештајне службе, као што су тајност рада, објективност, тимски рад и други, а има и оних који су специфични за конкретну контраобавештајну службу. Принципи као начела по којима се поступа, када се успоставе и прихвате морају се поштовати. Принципи контраобавештајног рада представљају основу на којој се успостављају и обликују модели функционисања припадника контраобавештајних служби, и они не морају обавезно бити утврђени службеним правилима.

Генерално, принципи рада контраобавештајне службе проистичу из опште политичке концепције државе, конкретних безбедносних циљева одређене државе, улоге контраобавештајне службе у њиховој реализацији и сл.[167] Без обзира на тип активности или оперативне околности, обављање контраобавештајних послова праћено је поштовањем основних принципа рада: [168]

- усклађеност са мисијом,
- тајност рада (избегавање публицитета),

[165] Michelle, K., Van C., *Intelligencer: Journal of U.S. Intelligence Studies*, 2013, Volume 20 • Number 2, 57-65, стр. 58, 59.
[166] Michelle, K., Van C., *Intelligencer: Journal of U.S. Intelligence Studies*, 2013, Volume 20 • Number 2, 57-65, стр. 58.
[167] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008., стр. 234.
[168] *Counterintelligence Operations*, Headquarters Department of the Army US, Washington DC, No. 30-17, 24 January 1972.

- објективност,
- потврђивање поузданости прикупљених података,
- офанзивност,
- флексибилност (прилагодљивост),
- непрекидност,
- континуитет.

Усклађеност рада (усаглашеност) са мисијом. Контраобавештајни задаци морају бити у складу са начелним опредељењем и функцијама службе, потребно је поштовати законска овлашћења и придржавати се упутстава надређених у обављању задатака.

Тајност рада. Неизоставни елемент рада обавештајних и контраобавештајних служби је тајност. Обавештајне и контраобавештајне службе условно излазе из домена тајновитости онда када се износе резултати одређене истраге, или када противничка страна дође до сазнања о прикупљеним обавештајним подацима о њима, или сазнањем о плановима, активностима, локацијама деловања и др. Поред редовних мера безбедности, често се обманом и дезинформацијама супротне стране покушава допринети већем степену тајности свог рада.[169]

Објективност и потврда поузданости података (провера). Прикупљени подаци о деловању противника морају бити проверени, односно потврђени из више извора како би били веродостојни, јер на основу њих служба доставља извештаје политичким структурама. Обавештења која добијају носиоци политичке моћи одређују правац и начин супротстављања деструктивном деловању, те стога не смеју бити пристрасна и једнострана, јер грешке начињене у овој фази могу имати огромне последице по националну безбедност, зато се од обавештајних и контраобавештајних служби захтева потпуна објективност у раду. Поштовање принципа објективности се подразумева у контраобавештајном раду, тако да је независна потврда поузданости података веома битна у контраобавештајним истрагама. Потврда се може спровести на више начина, од испитивања поузданости извора који се користе током дужег времена, затим употребом додатних истражних техника, укључивањем додатних извора информација, интерном контраобавештајном провером свог персоналан у случају да постоје сумње у постојање дуплих агената и др.

[169] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 236.

Офанзивност. „Независно од тога што је контраобавештајна делатност и основи дефанзивна- одбрамбена, органи који се њоме баве најчешће се постављају веома офанзивно.“[170] Продором у противничке обавештајне службе откривају се методи и средства противничких служби, откривају се њени извори података, али и подаци о сопственим изворима. Поред продора у непријатељске службе, офанзивност се огледа и у хватању страних агената, дезинформисању противника, упадима у информационе системе противника (енг. hacking- неовлашћен упад у туђ информациони систем да би се украле информације или урадиле неке друге нелегалне ствари[171]). и др. Свака па и дефанзивна контраобавештајна служба има елементе офанзивности у свом раду.

Флексибилност. Сви контраобавештајни елементи, почев од појединаца до највећих оперативних јединица, морају бити спремни и у стању да правовремено и адекватно одговоре на безбедносне и обавештајне догађаје и промене, на пример: брза промена од мирнодопског у непријатељско окружење.[172] Обзиром на динамичност ове области, контраобавештајни рад подразумева висок степен прилагодљивости, било да се ради о политичко-безбедносним или оперативно-тактичким променама или проблемима.

Непрекидност. Контраобавештајна делатност је континуирано ангажовање (активност) на откривању и спречавању рада страних обавештајних служби и других организација, које организују и спроводе подривачке активности, и подразумева стални ангажман претежно на сопственој територији.

Координација. Посматрано из угла фунционалности, координација је веома битна за ефикасно функционисање организационе целине, каква је контраобавештајна служба, и њених појединачних делова. У вођењу контраобавештајних истраживања, координација са другим службама, са којима се размењују подаци, је веома битна. Обично је уређена законом или је уређује неко државно тело (у Републици Србији је то Савет за националну безбедност као консултативно тело, односно Биро за координацију рада служби безбедности као оперативни орган Савета[173]).

---

[170] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 230.
[171] Hacking, Britannica, доступно на: http://www.britannica.com/search?query=hacking, (приступљено: 10.1.2015.).
[172] *Counterintelligence Operations*, Headquarters Department of the Army US, Washington DC, January 1972, No. 30-17, 24, стр.1-3.
[173] Одлука о Савету за националну безбедност Републике Србије, „Службени гласник РС“ бр. 50/07, 31.05. 2007.

Треба нагласити да поред наведених принципа рада постоје и други, који нису од примарног значаја за контраобавештајну делатност, те о њима неће бити речи у даљем тексту.

6.5. Методе рада

Метод води порекло од грчке речи methodos што значи пут, тражење или начин. Начин односно метод се најшире може одредити као „*укупност радњи и средстава којим се стиче истинито сазнање*“.[174] Да би се правилно одредиле и обухватиле методе које се користе приликом обављања контраобавештајне функције мора се знати шта она представља и који су њени циљеви. Будући да је контраобавештајна делатност детаљније обрађена у претходном делу рада, овде ће бити представљена једноставнија дефиниција из Закона о Федералној служби безбедности Руске Федерације, која може дати одговоре на постављена питања.

Према поменутом закону, контраобавештајна активност је „делатност која је усмерена на откривање, одвраћање и пресецање обавештајних и других специјалних активности страних обавештајних служби, организација и појединаца, које су организоване у циљу наношења штете безбедности“ државе.[175] Треба напоменути да ће се контраобавештајна делатност односно примењене методе искључиво посматрати кроз призму контраобавештајне и обавештајне службе, као посебних организација које су организоване ради заштите сопствених структура, државне територије, и других значајних државних вредности које су потенцијално угрожене/безбедносно рањивих нападима страних обавештајних служби, институција, организација и појединаца.

Ангажовање на откривању и пресецању обавештајних и других активности је ранијих година искључиво било повезано и у складу са дефанзивном улогом контраобавештајне делатности, са друге стране, да би се правовремено открили

[174] Миљевић, И. М., *Скрипта из Методологије научног рада*, Филозофски факултет, Источно Сарајево-Пале, 2007, стр. 68.
[175] Федеральный закон "О федеральной службе безопасности" (с изменениями и дополнениями) Глава II. *Основные направления деятельности органов Федеральной службы безопасности*, 3 апреля 1995 г. N 40-ФЗ, (15-95), доступно на: http://base.garant.ru/10104197/, приступљено 25.1.2015.

субверзивни планови и намере пре него што дође до негативних последица, поред стандардних, потребно је користити офанзивне и агресивне методе.

Активности непријатељских обавештајних служби, институција, организација и појединаца условљавају постојање перманентне потребе прикупљања обавештајних информација о њима, њиховим плановима, намерама, потенцијалима итд.

Методе које се користе у функцији реализације обавештајне активности могу се поделити на:[176]

- методе прикупљања почетних обавештајних сазнања, које се даље могу поделити на обавештајне методе у ужем смислу и коришћење легалних могућности за обавештајни рад;
- научне методе и поступке који се примењују у вишим фазама обавештајног циклуса у функцији обраде, анализе, класификовања и обједињавања обавештајних података, као и израде завршних обавештајних докумената.

У методе прикупљања сирових обавештајних информација спадају:[177]

а) агентурни метод;

б) технички метод (у ширем и ужем смислу);

в) иследни метод;

г) метод сарадње, и

д) поједини научни методи и методски поступци.

Једна од основних функција контраобавештајне делатности односни се на прикупљање информација о страним обавештајним службама и њиховим активностима и намерама, из чега се могу одредити основне конспиративне методе прикупљања података. Према мишљењу Милана Милошевића ту спадају:

- агентурни (класични) метод;
- метод инфилтрације у структуре противника;
- метод тајног коришћења техничких средстава и

[176] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 94.
[177] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 112.

– метод прикривеног прикупљања података.[178]

а) *Агентурни метод* је основни метод за прикупљање сазнања о тајнама противника, и почива на тајно успостављеном (непрофесионалном) односу између појединца и обавештајне/контраобавештајне службе иницијатора таквог односа. Елемент непрофесионалности прави разлику између обавештајца, коме је то стално занимање и агента као лица које формално није члан одређене службе, тј. није професионални припадник.

Лица (агенти) која непосредно реализују агентурни метод морају бити посебно припремљена и обучена за спровођење специфичних, сложених, ризичних и разноврсних задатака, а контролу односно стални надзор над њима врши служба којој помажу, тј. њени професионални припадници.[179] Према Р. Ронину агентурни рад се одвија кроз неколико етапа: [180]

- проналажење кандидата;
- обрада кандидата;
- формирање досијеа;
- оцена кандидата;
- вербовање; и
- опхођење са вербованим (усмеравање његове делатности, провера, одржавање везе и прекид сарадње).

б) *Метод инфилтрације* је карактеристичан и за (офанзивну) контраобавештајну и за обавештајну службу. Једноставно речено, потребно је да се професионални припадник обавештајне/контраобавештајне службе или неко друго лице, тајно, на одговарајући начин угради у виталне структуре противника, укључујући и сам врх државне и политичке власти, излажући се великом, релном ризику откривања, како би открио виталне тајне противника. Да би се смањила могућност откривања и избегле негативне последице, потребно је поред детаљно испланираног процеса инфилтрације и добро управљати ризицима. „Управљање ризицима може се дефинисати као процес у којем организације или појединци методички сагледавају и процењују ризике

[178] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 96.
[179] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 114.
[180] Ронин, Р., *Обавештајни рад: Практични приручник*, Службени гласник, Факултет безбедности, Београд, 2009, стр. 61-91.

предузетих активности ради постизања одрживих, односно планираних вредности у оквиру сваке активности коју организација спроводи.“[181]

Прикупљена сазнања се искоришћавају за спровођење виталних државних интереса, а посебан циљ који се поставља је спречавање изненађења, чији ефекти могу имати негативне последице по државу. Да би се спречила могућност стратегијских изненађења потребно је правовремено открити највиталније тајне противника. Процес инфилтрације је сложен и може веома дуго трајати (од пар месеци до неколико година), а састављен је од бројних добро испланираних предрадњи и поступака. [182] Овим методом се веома често постижу одлични резултати уколико је претходно цео процес инфилтрације плански добро припремљен, а продором у обавештајно-безбедносни систем могу се открити припремљени планови, тајна ангажованост, предмет и методе рада, а све у циљу предупређења планираних напада на државу, односно могућих изненађења.

Британска контраобавештајна и безбедносна служба MI5 је методом инфилтрације у највише кругове IRA-е (Ирска републиканска армија) спречавала многе трагедије у Енглеској (пр. минирање аутопута, хиподрома и др.). [183]

Кључни фактори успешне реализације контраобавештајне делатности у овом случају јесу правовремено сазнање и брзина одговора (адекватног начина реализације плана осујећења такве делатности).

в) *метод тајног коришћења техничких средстава.* Иако се данас све више користе легални извори за прикупљање важних информација, не треба потценити важност тајних метода, а посебно тајног коришћења техничких средстава. [184] Технолошки прогрес остварује јак утицај на могућности примене различитих техничких средстава у контраобавештајне сврхе. Технички метод може се схватити у ужем и у ширем смислу. У ужем смислу, овај метод се своди на тајно

[181] Ђорђевић, М., Кековић, З., *Управљање ризицима у тајним акцијама*, Војно дело, 2008, 1, 103-123, стр. 104.
[182] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд 2001, стр. 123, 124.
[183] Лопушина, М., *Тајне службе света*, Књига-комерц, Београд, 2005, стр. 336.
[184] Милашиновић, Р., Милашиновић, С., *Основи теорије конфликата*, Факултет безбедности, Београд, 2007, стр. 492, 494.

уграђивање техничког средства ради прикупљања одређених података о противнику, а техничка средства која се том приликом користе могу се класификовати на: [185]

- електронска средства;
- фото, тв и видео техничка средства;
- хемијска средства.

У ширем смислу, могуће је извршити поделу на следеће дисциплине: [186]

- SIGINT (Signals Intelligence- електронске обавештајне активности)
- IMINT (Imagery Intelligence- обавештајно снимање)
- MASINT (Measurement and Signature Intelligence- мерне и потписне обавештајне активности)
- ITINT (Information Technology Intelligence- информационе обавештајне активности).

г) *Метод прикривеног прикупљања података* реализује се кроз: 1) прикривено опсервирање; 2) прикривено анкетирање; и 3) прикривено научно истраживање. Овакав начин прикупљања података је економичнији од коришћења других конспиративних извора, јер је бржи, једноставнији и јефтинији, тако се нпр. употребом ове методе штеде тајни извори у иностранству и избегава опасност од компромитовања државе у међународној заједници. Прикупљање података могу обављати и стручњаци из одређених области, које су у том тренутку у фокусу интересовања, али је претходно неопходно спровести њихову безбедносну проверу, како би се избегао сталан процес преиспитивања поузданости извора при оцењивању прикупљених података.[187]

Од осталих прикупљачких метода треба навести :

- *метода испитивања ратних шпијуна*, од којих се могу добити важна сазнања о снази противника, распореду јединица, наоружању, опреми, а нарочито важно је прикупити сазнања о борбеним намерама и плановима, краткорочним и дугорочним циљевима и сл. Поред обављања информативног разговора, често се изучавају и

[185] Савић, А., *Обавештајне службе и национална безбедност*, Правни факултет, Крагујевац, 2006, стр. 104-108.
[186] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 137.
[187] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 129.

заплењена непријатељска документа, која могу бити од велике користи, зато им се приступа на најозбиљнији могући начин. О заплењеним документима сачињава се посебан извештај у коме се наводи ко је, када и како, односно под којим условима дошао до њих.[188] Састављање извештаја је важно и због могућности потурања лажних докумената у циљу дезинформисања противника и навођења на погрешне закључке, који могу произвести негативне (понекад и фаталне) последице.

- *метода испитивања политичких емиграната-избеглица.* Стране обавештајне службе често злоупотребљавају избеглиштво за убацивање агентуре и инфилтрирање обавештајаца у структуре противника, зато је битно обавити испитивање емиграната, посебно политичких, како би се избегли такви покушаји. Испитивање које обавља контраобавештајна служба обавља се систематски и темељно. Процес саслушавања воде иследници, специјализовани за одређену државу (познају језик, културу, обичаје, политичку ситуацију у тој земљи и др.). Најчешће се састоји из две фазе: I фаза- тзв. општи тест (велики број детаљних питања), II фаза- обављају је специјалисти за поједине области. [189]
- *метода праћења рада чланова дипломатске мисије.* Примењује се онда када постоји основана сумња да је дипломата прекорачио овлашћења у погледу спровођења илегалне обавештајне делатности или учествовања у организовању субверзивне делатности. [190]
- *метода пласирања лажних обавештења посредством медија* у циљу дезинформисања страних служби (нпр. о војсци, њеном наоружању, стању борбене готовости, развоју одређеног наоружања), како би пореметила, успорила или пресекла њихове планове.
- *прикупљање података методом сарадње* и друге методе.

6.6. Контраобавештајне мере

Веома важан елемент заштите безбедности државе, односно њених виталних вредности, представља супротстављање делатностима обавештајних служби, које захтева предузимање специфичних мера и активности. Приликом планирања

[188] Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001, стр. 137.
[189] Исто, стр. 139, 140.
[190] Исто, стр. 152.

контретних мера и активности посебну пажњу треба посветити спречавању или умањивању штетних ефеката на оним пољима која највише угрожавају државу. [191] Контраобавештајне мере могу се условно поделити на активне и пасивне. Пасивним мерама тежи се прикривању информација до којих противник може доћи, односно отежавању начина долажења до тајних података, а активне су оне мере којима се стално блокирају покушаји долажења до тајних података, и којима се спречавају покушаји реализације планова саботажа или диверзија. Под пасивним мерама се подразумева: поступање у тајности; заштиту класификованих докумената и материјала; заштита комуникационих уређаја од прислушкивања; забрана или контрола кретања; примена цензуре; поступке прикривања; и др. У активне мере се убрајају: противизвиђачка дејства, противсаботажна, противсубверзивна дејства и контрашпијунажа.[192]

У јавном извештају о раду Министарства одбране Литваније наводи се да активне контраобавештајне мере подразумевају: контраобавештајне истраге, анализе, и активности неопходне за утврђивање, процењивање, елиминисање или ублажавање фактора ризика и претњи по националну одбрамбену моћ. Пасивне мере су унапред припремљене радње са циљем организовања и спровођења мониторинга и заштите виталних података (државна или службена тајна). Ту спадају: превентивне радње којима се омогућава успешно спровођење физичке заштите тајних података и заштита кадрова националног система одбране, испитивање поузданости сопствених кадрова, омогућавање безбедне размене тајних података у оквиру система одбране.[193]

Неке од мера које се примењују у државним институцијама и у државним компанијама, које се контраобавештајно штите, а односе се на мрежну сигурност и компјутерску заштиту јесу: [194]

- спровођење мониторинга (у реалном времену) и вођење евиденције ко и када приступа серверима, модификује, коппира, брише или преузима податке,
- проналажење адекватних софтверских решења за чување података,

[191] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 245.
[192] Anon, Military Intelligence, s.n., s.l., n.d., доступно на: http://www.dlsu.edu.ph/offices/osa/rotc/pdf/ms1/military-intelligence.pdf, приступљено: 11.02.2015.
[193] Second Investigation Department under the Ministry of National Defence, *Public Report on Activities 2013*, Vilnius, 2014, стр. 6.
[194] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace:Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, October 2011, стр. 24,25.

- криптовање података на серверима и заштита информација компаније лозинком,
- креирање и имплементација стратегије смањења губљења података путем друштвених мрежа и др.

Када је реч о сајбер претњама као све већим ризиком по безбедност, потребно је донети мере које се генерално односе на: усавршавање IT (Information technology) стручњака, осавремењивање заштитних софтвера, институционалну сарадњу и дељење информација са органима других држава приликом истраживања сајбер инцидената.

Неке од превентивних мера (заштите тајних података и заштите од шпијунаже, врбовања и сл.) које контраобавештајна (безбедносна) служба спроводе су: едукација и саветовање високих званичника система одбране, носилаца власти; обављање безбедносних састанака са лицима која се враћају са привремених иностраних регуларних или специјалних мисија (амбасадори, конзули и други државни званичници који су имали мандат у некој међународној организацији) и др.

Овде ће бити представљени неки од значајнијих индикатора шпијунаже:[195]

- сваки покушај проширења приступа тајним подацима изван граница надлежности одређених лица, или покушаји добијања информација од стране неовлашћених лица;
- неовлашћено уклоњање тајног материјала из радног простора;
- обимна употреба копирања поверљивих материјала;
- продужење радног времена или накнаднадно обављање посла ван уобичајеног радног времена;
- неовлашћен унос компјутера, уређаја за снимање и пренос података у подручја у којима се чувају тајни подаци;
- отварање неколико банковних рачуна који садрже значајне суме новца а да не постоји логични извор прихода;
- изненадна отплата великих финансијских дугова, кредита;
- непријављен контакт са званичницима земаља од посебног интереса;
- честа или необјашњива краткотрајна путовања у стране земље;
- поновно учешће у кршењу безбедности;

[195] Wood, S., Kent, C., Eric, L., *Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers*, Defense Personnel Security Research Center, Monterey, 2005, стр. 4, 5.

– посета страних амбасада, конзулата или трговинских представништава, итд.

Мере које предузимају контраобавештајни органи у оквиру редовних делатности могу се поделити на две компоненте: активну и пасивну. Иако нису ограничене на одређен број делатности, требало би издвојити неке од најчешћих и најзначајнијих активних контраобавештајних мера, усмерених најчешће на неутралисање претњи од стране страних обавештајних служби. То су пре свега: мере против саботаже, шпијунаже, субверзије, тероризма, извиђања, прикривања, обмане. Пасивним мерама треба прикрити податке од непријатеља, заштити особље од субверзивних и терористичких активности, као и инфраструктуру и материјал од саботаже. Оне се једноставно стандардизују у сталне оперативне процедуре. Ове мере укључују, али такође нису ограничене само на: заштиту класификованих материјала, заштиту персонала, средстава комуницирања, тајних података, укључујући и цензуру.[196]

Контраобавештајне мере могу се поделити на три опште мере[197]: одбијање, детекцију и обману.

1. *Мере одбијања* се примењују за спречавање приступања тајним и осетљивим информацијама, подривање особља, и физичког продора безбедносних препрека успостављених на командним местима објеката. Једна од мера одбијања које се често примењују је противизвиђање.

2. *Мере детекције* имају важну улогу у процесу разоткривања и неутрализације планова непријатеља усмерених на прикупљање обавештајних података, саботажу, субверзију и тероризам. Неке од ових мера подразумевају: разне типове испитивања, превод и анализу докумената, праћење рада и прослеђивање могућих непријатељских агената вишим нивоима ради саслушања, офанзивне и дефанзивне контраобавештајне активности и др.

3. *Мере обмане* се користе за збуњивање непријатеља или стварање заблуде у вези са постојећим капацитетима, способностима, плановима и намерама, тачкама рањивости, и оне могу укључивати: лажне нападе, трикове, пласирање лажних информација итд. Процес реализације мера обмане је веома сложен, зато се посебна пажња посвећује

[196] *Counterintelligence*, Department of the Navy-Headquarters United States Marine Corps, Washington, D.C., MCWP 2-14, 7 Oct 1998., 1-6,7.
[197] Исто, стр. 7.

креирању плана и спровођењу предрадњи, које ће осигурати да ни у једној фази процеса не дође до цурења информација и пропадања плана.

Контраобавештајне службе обично штите наменску индустрију у својим земљама, и претежно покривају шпијунажу у области војне индустрије, која је стратешки важна за сваку државу.

Федерални истражни биро (енг. Federal Bureau of Investigation- FBI) пружа америчким компанијама заштиту од шпијунаже и осигурава конкурентске позиције, а уколико компанија посумња да има шпијуна у својим редовима, може добити директну подршку у виду истраге, односно идентификовања, ублажавања и елиминисања тих претњи. Опште мере и активности које FBI препоручује компанијама како би се заштитиле од крађе тајних података су: организовање редовних едукација и тренинга запослених из области безбедности; коришћење одговарајућих процеса селекције при избору нових радника; обезбеђење погодних начина за пријаву сумњивих активности; осигурање безбедности рачунара (инсталирање заштитних програма); подизање свести запослених о значају пријављивања безбедносних проблема. FBI пружа директну помоћ компанијама и у смислу организовања безбедносних и контраобавештајних обука и семинара у циљу подизања свести запослених о овим проблемима.[198]

Неке од мера које предлаже Љ. Стајић: [199]

- изучити и пратити методологију рада страних обавештајних служби;
- спречавати обавештајне делатности дипломатско-конзуларних представништава, војно-дипломатских представништава и страних међународних организација;
- вршити продоре у стране обавештајне службе;
- обавити контраобавештајну заштиту објеката од посебног значаја за земљу;
- заштити тајност докумената, објеката и слично;
- енергично пресећи све обавештајне делатности страних обавештајних служби у нашој земљи;

[198] FBI, Counterintelligence, *The Insider Threat: An introduction to detecting and deterring an insider spy*, доступно на: http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat, приступљено: 14.02.2015.
[199] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, Београд, 2008, стр. 246.

- посебно уредити и контролисати рејоне и објекте који су од значаја за безбедност;
- пратити, открити и спречавати делатности „ослонаца“ страних обавештајних служби у земљи;
- стално пратити и изучавати стране државе и њихове обавештајне службе;
- организовати стручну помоћ осталим структурама друштва на супротстављању делатности страних обавештајних служби и др.

Безбедносне и контраобавештајне службе примењују велики број мера којима се супротстављају страним обавештајним активностима. Овде су наведене само неке од најбитнијих, а које ће мере бити примењене у сваком појединачном случају зависи од многих ситуационих фактора.[200]

6.7. Реализација контраобавештајне делатности

Активности које спроводе стране обавештајне службе, друге институције, органи и организације који се баве обавештајним и субверзивним активностима могу угрозити институције једне државе, виталне државне органе, технолошки развој, тајне податке, и друштво у целини. Носиоци угрожавања (субјекти који предузимају „радњу извршења“ тј. спроводе облике угрожавања)[201] неретко у сарадњи са опозиционим снагама државе учествују у организовању политичког насиља и нелегалних начина освајања власти. „Најчешћи начини илегалног освајања власти су преврати у форми политичког удара, државног удара и пуча, затим превратустанком и револуција, а свима њима увек претходе политичке завере.“[202] Да би заштита државе од таквих активности била ефикасна, законском регулативом треба уредити област безбедности, а посебно област контраобавештајне заштите државе.

По правилу, контраобавештајне послове реализују посебне организације, чија је основна активност базирана на заштити сопствених структура, државне територије и

[200] Стајић, Љ., *Основи система безбедности*, Факултет безбедности, 2008, Београд, стр. 247.
[201] Исто, стр. 53.
[202] Симеуновић, Д., *Увод у политичку теорију*, Институт за политичке студије, Београд, 2009, стр. 108.

других виталних вредности од страних обавештајних служби и других организација и институција које организују и спроводе обавештајне и субверзивне активности.[203]

„Процес реализације контраобавештајних активности у циљу откривања страних обавештајних операција подразумева и текући (current) и упозоравајући (warning) контраобававештајни рад, као одговор на непредвидиво и изненадно штетно деловање офанзивних и умрежених страних обавештајних продора и других савремених претњи безбедности.“[204]

У стратегијском смислу, реализација контраобавештајних активности обухвата следеће фазе:[205]

1. развој контраобавештајних потенцијала;

2. руковођење контраобавештајним надзором;

3. развој контраобавештајних планова;

4. руковођење контраобавештајним операцијама

5. помоћ у имплементацији контраобавештајних мера.

Реализација контраобавештајне делатности је састављена из неколико фаза које су међусобно повезане и успешне само у одређеној (заједничкој) корелацији, и чине целину познату као контраобавештајни циклус. За разлику од обавештајног циклуса код кога почетно место најчешће заузима прикупљање података, чијом се даљом обрадом добијају обавештајне информације, код контраобавештајног циклуса полази се од дефинисања планова и мера и заштите сопствених потенцијала од различитих претњи безбедности, а у следећој или некој од следећих фаза долази до спровођења обавештајног истраживања. Може се рећи да контраобавештајни циклус у себи садржи обавештајни циклус као свој саставни део.

Неке од карактеристика обавештајног и контраобавештајног циклуса јесу систематичност, плански рад, аналитичност, цикличност, законитост, непрекидност у

[203] Милошевић, М., *Одбрана од тероризма*, Свет књиге, Београд, 2005, стр. 93.
[204] Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 55.
[205] Counterintelligence, US Marine Corps, MCWP 2-14, 5 September 2000; цититано према: Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 55.

раду, тимски рад и др.[206] Без обзира на број фаза, да би се остварио контраобавештајни циклус, битно је реализовати последњу фазу, односно заокружити процес.

На основу многобројних и различитих практичних искустава о начину, односно процесу реализације контраобавештајних активности, у основне фазе контраобавештајног циклуса могу се сврстати:[207]

а) дефинисање планова и мера и заштита сопствених потенцијала и безбедносних интереса (definition/protection);

б) реализација истраживања у циљу откривања и процене природе претњи (competitors/identify and evaluate);

в) уочавање и разумевање претњи и процена рањивости (vulnerabilities/evaluate and identify);

г) дефинисање и реализација акција на плану одвраћања претњи (dissuasion/define actions);

д) анализа реализованих акција из угла процене коришћених људских и технолошких потенцијала (analysis/people and technology) и

ђ) дефинисање будућих (контра)обавештајних потреба и планова (intelligence decisions).

7. УЛОГА КОНТРАОБАВЕШТАЈНЕ ДЕЛАТНОСТИ У СПРЕЧАВАЊУ УГРОЖАВАЊА НАЦИОНАЛНЕ БЕЗБЕДНОСТИ

Једна од најзначајнијих улога контраобавештајне делатности односи се на заштиту националне безбедности од страних обавештајних операција и шпијунаже. Контраобавештајна делатност заједно са обавештајном делатношћу даје подршку националној политици, пружајући информације које носиоцима политичке власти могу

[206] Саздовска, М., *Обавештајни циклус*, НБП, XII, (1), 131 – 147, 2006, стр. 144.
[207] Taborda and Ferreira, 2002, p. 185; цитирано према: Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010, стр. 55.

бити од значаја при доношењу спољно-политичких одлука. [208] Офанзивним контраобавештајним радом могу се спречити субверзивни планови страних обавештајних служби, терористичких или других организација, али и пружити подршка спољној политици земље омогућавањем увида у извештаје о планираним активностима страних обавештајних служби.

Заштита војне индустрије је од великог значаја за систем одбране и националну безбедност сваке државе. Она је стална мета страних обавештајних служби, чији је циљ прикупљање што већег броја информација о стању индустријског комплекса, броју произведеног оружја, врстама оружја, новом наоружању и иновацијама, будућим плановима и другим подацима. Успостављање јаке контраобавештајне заштите сектора војне индустрије значајно је, како у погледу спречавања индустријске шпијунаже, тако и у погледу ремећења евентуалних припрема за оружани напад употребом метода обмане, дезинформисања и сл. Контраобавештајну заштиту министарства одбране и војске обављају војне контраобавештајне службе, које штите лица, тајне податке, снаге, објекте, активности, информационо-комуникационе системе и др. у складу са својим овлашћењима. Када се открије страни агент једна од опција је покушај превербовања, уколико се процени да је организација за коју ради важна за добијање података, или опасна по безбедност државе.

Контраобавештајна делатност пружа подршку и правосудним органима уступањем података о незаконитим активностима лица или група које делују противзаконито или противуставно. Носиоци контраобавештајне делатности могу нпр. у откривању и документовању кривичних дела прикупљати и обрађивати личне податке, вршити полиграфско тестирање, предузимати мере надзора, снимања разговора и друге мере у складу са својим овлашћењима. Подаци добијени контраобавештајним радом могу бити прослеђени некој другој служби у земљи или иностранству. Контраобавештајна делатност продукује знања, која могу бити од користи законодавној власти у фази доношења нових, или модификовања постојећих закона у овој области, или усвајања стратегијских докумената за развој контраобавештајног рада и стратешког супротстављања одређеним појавама попут међународног тероризма.

[208] Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, The Commission's report, 1996, p. 21.

Иако није област која излази у први план када се говори о одбрани земље, она је стално присутна и активна у одбрани националне безбедности сваке државе, која има успостављен обавештајно-безбедносни апарат. Ради се о делатности која се одвија у строгој тајности, у складу са својим специфичностима.

Контраобавештајна делатност на директан начин доприноси јачању националне безбедности представљајући истовремено „штит“ и „мач“. У складу са својом дефанзивном улогом, она симболично представља штит који одбија покушај продора страних обавештајних служби у виталне државне структуре, а са друге стране мач, јер уништава стране обавештајне способности спровођењем офанзивних контраобавештајних операција.[209]

Заштита система националне безбедности не може се ефикасно бранити само на сопственој територији и конвенционалним средствима, јер су данас доминантне невојне претње попут тероризма, организованог криминала, обавештајно-субверзивних активности и др. Због тога офанзивна контраобавештајна делатност подразумева спровођење добро испланираних активности на територији непријатељских држава са урачунатим ризиком од откривања. Она на тај начин представља (поред спољних обавештајних активности) прву линију одбране од ризика и претњи против националне безбедности државе.

Када је реч о тероризму, тајни информатори или агенти су вероватно најефикаснији инструмент у борби против терористичких група, пружајући детаље о организацији, профилу вође, структури, начину финансирања, повезаности са обавештајним службама, плановима и операцијама. Продор у терористичку групу извршава се запошљавањем, уценом или корумпирањем њених припадника.[210] Најразвијеније контраобавештајне службе су врло успешне у спровођењу оваквих активности.

Контраобавештајна делатност омогућава заштиту осетљивих информација националне безбедности и спречава губитак критичних технолошких, индустријских и комерцијалних информација. Квалитетан и континуалан контраобавештајни рад пружа

[209] Van Cleave, M., *Counterintelligence and National Strategy*, School for National Security Executive Education, National Defense University Press, Washington, D.C., 2007, стр. 3.
[210] Mazumdar, K., *Intelligence and Counterintelligence: First Line of Defence*, Research Institute for European and American Studies, 2012, доступно на: http://rieas.gr/research-areas/2014-07-30-08-58-27/transatlantic-studies/1719-intelligence-and-counterintelligence-first-line-of-defence, приступљено: 14. 4. 2015.

свеобухватан безбедносни програм и сталну евалуацију намера и циљева страних обавештајних служби.[211] Контраобавештајна делатност је основа контрареактивног деловања и не сме бити пасивна компонента националне безбедности, односно имати улогу пасивне одбране.

8. КРАЋИ ПРИКАЗ АМЕРИЧКЕ FBI СЛУЖБЕ ДАНАС

Заштита националне безбедности од шпијунаже, тероризма и сличних претњи у САД-у поверена је агенцији са извршним законским овлашћењима при вршењу безбедносне и контраобавештајне функције, Федералном истражном бироу (FBI).[212] Према новој организационој шеми из 2014. године у оквиру ФБИ централе делује седам уреда за: јавне послове, конгресне послове, опште савете, једнакост запошљавања, професионалну одговорност, помоћ омбдусмана, интегритет и усаглашеност и шест оперативних управа: [213]

- управа за обавештајни рад;
- управа за националну безбедност;
- управа за криминал, сајбер, и услуге;
- управа за науку и технологију;
- управа за информационе технологије; и
- управа за људске ресурсе.

У управи за националну безбедност делују: дивизија за контратероризам, дивизија за контраобавештајни рад, и директорат за оружје за масовно уништење. [214] У децембру 2001. године централа службе се реорганизује и добија контратерористичку дивизију која обједињује све неопходне елементе борбе против тероризма и планира, усмерава активности у том правцу.[215] Федерални истражни биро има веома широк

[211] Counterintelligence, CIA- Annual Reports 1999, доступно на: https://www.cia.gov/library/reports/archived-reports-1/ann_rpt_1999/dci_annual_report_99_16.html, приступљено: 23. 2. 2015.
[212] Kalkavage, M., *Counterintelligence in the Kingdom and the States: A Historical Comparison of the FBI and MI5*, Master's Thesis, Boston University, Boston, 2014.
[213] Organizational Chart, Преузето са: http://www.fbi.gov/contact-us/fbi-headquarters/org_chart, приступљено: 24. 02. 2015.
[214] Исто
[215] U.S. Department of Justice, Federal Bureau of Investigation, April 14, 2004, Report to the National Commission on Terrorist Attacks upon the United States: *The FBI's Counterterrorism Program: Since September 2001*, Office of Public Affairs, Washington., стр. 20.

делокруг рада, а за примарну делатност има све оно што је везано за откривање присуства и намера страног обавештајног фактора. У складу са својим овлашћењима и функцијом коју обавља, служба је врло блиско повезана са носиоцима политичке власти у чему кључну улогу има директор, који има велика овлашћења али и дужности.[216]

„Под надзором генералног јавног тужиоца и сходно прописима које овај тужилац донесе, директор Федералног истражног бироа дужан је да“:[217]

- открива и спречава шпијунажу, саботажу, субверзију и друге незаконите активности од стране или за рачун страних сила;
- на захтев старешина Обавештајне заједнице које одреди председник, спроводи у Сједињеним Државама и на њеним територијама законите активности, укључујући електронску контролу, које дозволи председник и специјално одобри генерални јавни тужилац;
- прикупља обавештајне податке о страним земљама применом законитих средстава у Сједињеним Државама и на њиховим територијама када то захтевају старешине Обавештајне заједнице које одреди председник;
- доставља своје обавештајне и контраобавештајне информације о страним земљама одговарајућим федералним агенцијама, федералним локалним органима и службама, као и владама са којима је успостављена сарадња;
- врши или уговара истраживања, развојне програме и набавку техничких система и средстава неопходних за извршење горе наведених функција.

У случају корпорацијске контраобавештајне заштите, FBI је дефинисао контраобавештајну делатност као проактивну категорију којом се тежи утврдити да ли иностранa конкуренција или агенти неке стране владе злоупотребљавају особље компаније, или на неки други начин долазе до важних информација или тенхнологија.[218]

[216] Милашиновић, Р., ЦИА: *Моћ и политика*, Југоштампа, Београд, 1979, стр. 84.
[217] Милашиновић, Р., Милашиновић С., *Основи теорије конфликата*, Факултет безбедности, Београд, 2007, стр. 521.
[218] FBI, (09.18.2009 version), *Counterintelligence Vulnerability Assessment for Corporate America*, s.n.

Од напада Ал Каиде у септембру 2001. године, FBI је суштински променио начин супротстављања тероризму, који је више базиран на обавештајној и контраобавештајној компоненти, него на традиционалном спровођењу закона.[219]

Драстично повећање издвајања новца из буџета за потребе националне безбедности реализује се након терористичког напада на Сједињене Државе 11.09.2001. и усвајања контраобавештајног програма. Године 2001. укупан буџет FBI-а био је 3.81 милијарди долара, од чега је 32% издвајано за програме заштите националне безбедности, у којима приоритетна места заузимају борба против тероризма и контраобавештајна делатност. За 2004. годину планирана издвајања за потребе националне безбедности расту са 32 на 40%, а за 2005. годину планирано је повећање до 44% укупног буџета. Број ангажованих људи у борби против тероризма и у контраобавештајним мисијама, порастао је за чак 80% у периоду од 2001-2005. године. Од 29. фебруара 2004. године, ФБИ има нешто преко 28.000 запослених, од којих је око 12.000 специјалних агената.[220] Буџет за 2012. годину је био 8.12 милијарди долара.[221]

После 11. септембра FBI пролази кроз реформски процес свих области рада, придодаје нове функције, проширује капацитете и врши редефинисање и преобликовање својих планова и програма и усваја 10 приоритетних активности. Неке од њих су:[222]

- заштита САД-а од терористичког напада;
- заштита од страних обавештајних операција и шпијунаже;
- заштита од сајбер напада и високо технолошких кривичних дела;
- заштита људских права од транснационалних/националних криминалних организација;
- технолошка надоградња за успешно обављање мисије FBI

[219] Theoharis, A., *Chasing Spies: How the FBI Failed in Counterintelligence But Promoted the Politics of McCarthyism in the Cold War Years,* FBI- Center for the Study of Intelligence, 2002, 47 (3), стр. 1, доступно на: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article07.html, приступљено: 6. 5. 2015.
[220] U.S. Department of Justice, Federal Bureau of Investigation, April 14, 2004, Report to the National Commission on Terrorist Attacks upon the United States: *The FBI's Counterterrorism Program: Since September 2001*, Office of Public Affairs, Washington.
[221] U.S. Department of Justice, Federal Bureau of Investigation, n.d., Today's FBI: Facts & Figures 2013-2014, Office of Public Affairs, Washington.
[222] U.S. Department of Justice, Federal Bureau of Investigation, April 14, 2004, Report to the National Commission on Terrorist Attacks upon the United States: The FBI's Counterterrorism Program: Since September 2001, Office of Public Affairs, Washington.

Један од циљева након терористичког напада био је организационо усмеравање ка превенцији и проактивном деловању уместо устаљеног реактивног спровођења закона. Убрзо након 11. септембра усвојен је и Патриотски акт (октобар 2001.) којим ФБИ проширује своја истражна и контраобавештајна овлашћења у оквиру борбе против тероризма.

FBI има канцеларије у 78 кључних градова широм света, преко којих обезбеђује покривеност за више од 200 земаља, територија и острва.[223]

Делокруг рада Федералног истражног бироа је нормативно одређен Законом о FBI (31.7.1979. год.) и извршним наредбама председника 12036 и 12333 обухвата три групе послова: контраобавештајни рад, делатност политичке полиције и послове кривичне полиције.[224] Сазнања за контраобавештајно ангажовање добија из сопствених извора, од других обавештајних служби, и приликом размена информација са страним обавештајним службама и службама безбедности. Активности које обављају ради испуњења тог циља су: надзор над лицима осумњиченим за шпијунажу у корист страних обавештајних служби; праћење активности страних дипломатских мисија и квазидипломатских представништава.[225]

FBI, у складу са својим циљевима борбе против шпијунаже, саботаже, тероризма и осталих безбедносних претњи, спроводи безбедносну процедуру за сва лица која раде у владиним установама и министарствима, и кандидате за ступање у радни однос у њима.[226]

Између 11. септембра 2001. и 19. фебруара 2004. године само дивизија безбедности (контратероризам и контраобавештајни рад) примила је и углавном успешно обрадила велики број захтева који ће бити представљени у табели испод.

[223] U.S. Department of Justice, Federal Bureau of Investigation, n.d., FBI Information Sharing & Safeguarding Report 2012, Office of Public Affairs, Washington.
[224] Бајагић, М., *Шпијунажа у 21. веку- Савремени обавештајно-безбедносни системи*, Београд, 2010, стр. 99.
[225] Tyrus, G. F., *The intelligence Community: History, Organization, and Issues*, New York:R.R. Browker Company, 1977, p. 384-387., према: Бајагић, М., *Шпијунажа у 21. веку- Савремени обавештајно-безбедносни системи*, Београд, 2010, стр. 100.
[226] Милашиновић, Р., *ЦИА: Моћ и политика*, Југоштампа, Београд, 1979., стр. 85.

Управљање извршним поступцима	Број случајева	Предмети који се односе на терористичке инциденте	Број случајева
Примљени безбедносни захтеви	2.707	Захтеви са највишим степеном тајности	1.589
Успешно обрађени	2.351	Успешно обрађени	1.414
Прекинути или административно затворени	87	Прекинути или административно затворени	0
Отворени предмети (на чекању)	87	Отворени предмети (на чекању)	175

Табела 1 –Број процесуираних случајева FBI-а од 11. септембра 2001. године до 19. фебруара 2004. године.[227]

Још осамдесетих година дведесетог века, FBI се мање-више континуирано сусретао са терористичким активностима до данас, међутим треба истаћи да их ипак није било много на тлу Сједињених држава. Према статистици коју води FBI од 1980-2005. год., укупан број терористичких напада је 318, а највеће губитке је изазвао напад на Светски трговински центар 11. септембра 2001. године, са 2.997 погинулих и 12.017 повређених људи и огромном материјалном штетом.[228] MI5 је у односу на FBI имала нешто лакшу трансформацију и стратешки прелаз у еру борбе против тероризма, као једне од највећих савремених и актуелних безбедносних претњи, пре свега због дугогодишњег успеха у супротстављању тероризму и великог искуства у контраобавештајној делатности.

[227] U.S. Department of Justice, Federal Bureau of Investigation, April 14, 2004, Report to the National Commission on Terrorist Attacks upon the United States: *The FBI's Counterterrorism Program: Since September 2001,* Office of Public Affairs, Washington, стр. 42.
[228] U.S. Department of Justice, Federal Bureau of Investigation, n.d., Report, *Terrorism 2002-2005*, s.n., s.l., str. 15, 31.

ЗАКЉУЧАК

Свака држава успостављањем и развојем система безбедности тежи да њиме обезбеди своју целовитост и заштити своје виталне вредности. Стање и квалитет система националне безбедности зависи од много различитих елемената, а један од најважнијих је свакако контраобавештајни, којим руководе безбедносне односно контраобавештајне службе.

Контраобавештајна делатност доприноси стабилности националне безбедности пружајући заштиту од продора страних обавештајних организација у државне органе и институције, али и представљајући добро офанзивно средство којим се пресецају и уништавају обавештајно-субверзивни планови непријатеља. Она се временом мењала, односно прилагођавала новим изазовима, ризицима и претњама, а промене су биле одговор на опасности са којима се суочавао систем националне безбедности. Стиче се утисак да су промене (законске, организационе, оперативно-тактичке) у прошлости више биле реактивне, односно изнуђене негативним обавештајним, субверзивним и другим факторима него резултат превентивног, а још мање проактивног деловања. Проактивни приступ изискује и већа новчана улагања, што би државама у транзицији, у којој се налази и Србија, представљало финансијски проблем.

Систем националне безбедности не може се штитити само на сопственој територији и конвенционалним средствима, јер су данас доминантне невојне претње попут тероризма, организованог криминала, обавештајно-субверзивних активности, против којих успешност супротстављања често зависи од способности врбовања чланова или продора у њихове структуре из којих се врши планирање таквих активности. Самим тим, она је поред спољних обавештајних активности прва линија одбране државе од ризика и претњи националној безбедности.

Негативне последице јачања обавештајних капацитета држава и широка употреба обавештајних и субверзивних активности, довеле су до тога да је контраобавештајна делатност држава које трпе овакве последице постала офанзивнија у настојању да предупреди остваривање обавештајних и субверзивних планова. Офанзивност претежно подразумева хватање шпијуна и дуплих агената, као и продоре у структуре непријатељских служби, ради откривања метода и средстава рада, њихових

планова и др. Технолошка модернизација и нове претње попут тероризма утицале су на реорганизацију контраобавештајног рада. Долази до усвајања нових метода и средстава рада, појачане размене информација између агенција, и стратешког планирања развоја контраобавештајне делатности. Данас се много више инсистира на међуагенцијској сарадњи и размени информација него у ранијем периоду (пример сарадње FBI-а и CIA-е након 11. септембра 2001. године).

Контраобавештајни делатност данас укључује и заштиту у сајбер простору, на местима која су безбедносно осетљива и која се ослањају на информационе системе. Функције контраобавештајне делатности у сајбер простору су непромењене и своде се на детекцију, идентификацију, процену, неутрализацију или искоришћавање. Важно је дефинисати критичну инфраструктуру коју треба заштити од сајбер напада, то су углавном велики и значајни индустријски комплекси, системи који садрже научне, технолошке, војне и друге податке. Терористи често преко сајбер простора врше комуникацију у циљу извршења својих активности, тако да је контрола и праћење сумњивих комуникација у том простору један од важних фактора за пресецање терористичких напада. Међународна сарадња, размена података и искустава експерата, али и сарадња приватног и државног сектора у области информационих технологија неопходне су за развој бољих система заштите и превенције таквих напада.

Једна од могућих препрека контраобавештајној делатности је непрепознавање значаја системског развоја ове области (непостојање адекватних законских решења, стратегија развоја и др.), недовољан степен овлашћења и надлежности за обављање контраобавештајних послова или насупрот овоме, преширока овлашћења, која неретко доводе до кршења људских и грађанских права, зарад остваривања интереса националне или јавне безбедности. Зато је веома је важно и постојање снажног демократског надзора над применом посебних овлашћења.

Успостављањем чвршће сарадње безбедносних агенција са националним корпорацијама и државним органима (чија радна места захтевају ову врсту заштите) повећала би се ефикасност контраобавештајне заштите. Под тим се подразумева држање едукативних семинара, обука (тренинга), појединачних безбедносних састанака итд. а све у циљу подизања нивоа безбедносне културе и превентивног деловања.

У многим државама контраобавештајну делатност обавља неколико служби, цивилних или војних, којима је то примарна или секундарна делатност. У тим околностима може долазити до неспоразума у вези са расподелом послова и надлежности, али и проблема у вези са давањем предности одређеној агенцији над приоритетним областима и пословима заштите. Једно од могућих решења је формирање националне контраобавештајне службе (уколико не постоји) која би имала првенство над свим контраобавештајним активностима и која би у функционалном и организационом смислу објединила све службе задужене за обављање ових послова и била нека врста оперативно координационог тела. На тај начин би специјализована служба вршила расподелу послова, растерећивала друге службе преузимајући велики број најзахтевнијијих задатака, али и одговорност за евентуални неуспех. Омогућила би се бржа размена информција између агенција, успоставила боља сарадња и координација, као и спровођење заједничких активности са јасном поделом послова и одговорности. Она би морала имати на располагању јединствену базу података о свим контраобавештајним случајевима.

Држава односно њени органи остварују посредну корист од контраобавештајне делатности у спољно-политичким односима, имајући увид у извештаје, који садрже планове и намере непријатељских држава, које организују и управљају обавештајним и субверзивним операцијама.

Значај контраобавештајне делатности је и у томе што сазнања која она производи не користе само службе безбедности, већ и тужилаштво и законодавна власт. Носиоци контраобавештајног рада пружају директну подршку правосудним органима уступањем података о незаконитим активностима лица или група које делују противзаконито или противуставно. Сазнања и искуства у тој области могу бити од користи и законодавној власти у фази доношења нових односно редефинисања постојећих закона, или усвајања стратегијских докумената за развој контраобавештајног рада и стратешког супротстављања одређеним појавама попут међународног тероризма.

Агенције као што су FBI и MI5 представљају добар пример реорганизације контраобавештајне делатности и њено прилагођавање новом безбедносном контексту од завршетка Хладног рата до данашњих дана. Препознавање значаја развоја контраобавештајне делатности и њено стратешко планирање представљају темељ

успешне контраобавештајне заштите и чувања националне безбедности. Улагање у развој контраобавештајног система може се схватити и као рад на превенцији, јер ће многе противнике одвратити од њихових планова и намера уколико су свесни његове снаге.

ЛИТЕРАТУРА:

1. Аврамов, С., Крећа, М., *Међународно јавно право*, Савремена администрација, Београд, 2003.
2. Anon, *Military Intelligence*, s.n., s.l., n.d., доступно на: http://www.dlsu.edu.ph/offices/osa/rotc/pdf/ms1/military-intelligence.pdf, приступљено: 11. 02. 2015.
3. Бајагић, М., *Шпијунажа у 21. веку- Савремени обавештајно-безбедносни системи*, МАРСО, Београд, 2010.
4. Бајагић, М., *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд, 2010.
5. Башкатов, Н., *и др., Контрразведывательная и оперативно-розыскная деятельность органов федеральной службы безопасности (соотношение и правовое регулирование)*, Журнал: Право и безопасность, 1 (34), 9-18, 2010.
6. Bilandžić, M., *Terorizam i restrukturiranje društvene moći*, Polemos, 16, (2), 31-49, 2013.
7. Born, H., Leigh, I., Wills, A., *International Intelligence Cooperation and Accountability*, Routledge, 2011.
8. Van Cleave, M., *Intelligencer*, Journal of U.S. Intelligence Studies, 20 (2), 57-65, 2013.
9. Van Cleave, M., *Counterintelligence and National Strategy*, School for National Security Executive Education, National Defense University Press, Washington, D.C., 2007.
10. Weimann, G., Tsfati, Y., *Terror on the Internet*, Studies in Conflict & Terrorism, 2002, 25:317–332.
11. Вејновић, Д., Обреновић, П., *Дефендолошки изазови у међународним односима са погледом на Босну и Херцеговину*, Европски дефендологија центар за научна, политичка, економска, социјална, безбједносна, социолошка и криминолошка истраживања, Бања Лука, 2012.
12. Wesley, W., *Introduction: „Learning to Live With Intelligence“*, Intelligence and National Security, 18 (4), 1-14, 2003.

13. Wettering, F., *"Counterintelligence: The broken triad"*, International Journal of Intelligence and CounterIntelligence, 13, (3), 265-300, 2000.
14. Војнобезбедносна агенција, *Развој контраобавештајне делатности*, доступно на: http://www.vba.mod.gov.rs/I_faza.html#.VI9CQ8kl9fw, приступљено: 20. 11. 2014.
15. Wood, S., Kent, C., Eric, L., *Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers*, Defense Personnel Security Research Center, Monterey, 2005.
16. Вулетић, Д., *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011.
17. Гаћиновић, Р., *Унутрашњи неоружани облици угрожавања капацитета безбедности државе*, Политичка ревија, 1, (31), 229-251, 2012.
18. Godson, R., *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence*, (Third printing), Transaction Publishers, New Brunswick, New Jersey, 2004.
19. Denning, D., *Cyber terrorism: Testimony before the Special Oversight Panel on Terrorism*, Committee on Armed Services U.S. House of Representatives, Georgetown University, May 2000.
20. Definitions: *Counterintelligence*, The provisions of Executive Order 12333, United States intelligence activities, 1981.
21. Димитријевић, В., *Појам безбедности у међународним односима*, Савез удружења правника Југославије, Београд, 7-38, 1973.
22. Dictionary of U.S Military Terms of Joint Usage, Military Regulations. U.S. Army Regulation, pp. 310-25, 1983. доступно на: http://www.fas.org/irp/doddir/army/ar310-25.pdf, приступљено: 10. 12. 2014.
23. Dogrul, M., Aslan, A., Celik, E., *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*, 3rd International Conference on Cyber Conflict, Estonia, 2011, pp. 29-43.
24. Dorn, N., *European Strategic Intelligence: How far integration?*, Erasmus Law Review, 5, (1), 2008.
25. Драгишић, З., *Систем националне безбедности: Покушај дефинисања појма*, Војно дело, 3, 162-176, 2009.

26. Ђорђевић, З., Шаљић Е., *Улога обавештајних служби у борби против тероризма*, Међународна и национална сарадња и координација у супротстављању криминалитету, 3/1, 500-514, 2010.
27. Ђорђевић, М., Кековић, З., *Управљање ризицима у тајним акцијама*, Војно дело, 1, 103-123, 2008.
28. Elmusharaf, M., *Cyber Terrorism: The new kind of Terrorism*, Computer Crime Research Center, 2004, доступно на: http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism, приступљено: 15. 4. 2015.
29. Зиројевић, Фатић, М., *Злоупотреба интернета у сврхе тероризма*, Институт за међународну политику и привреду, LXIII, (3), 417–448, 2011.
30. Ивановић, А., *Теорије безбедности*, Универзитетска мисао, 11/2012, 55-82, 2012.
31. Iglesias, M., Ministrio de Defensa, 2011, *The Evolution of the concept of Security*, Instituto Español de Estudios Estratégicos.
32. Илић, Г., *Маргиналије уз закон о одговорности правних лица за кривична дела*, CRIMEN (I), 2 , 246–256, 2010.
33. Илић, П., *О дефинисању и дефиницијама националне безбедности*, Војно дело, 123-138, 2012.
34. Janczewski, L., Colarik, A., Cyber Warfare And Cyber Terrorism, Information Science Reference, New York, 2008.
35. Japan, Intelligence and Security, доступно на: http://www.faqs.org/espionage/Int-Ke/Japan-Intelligence-and-Security.html, приступљено: 20. 11. 2014.
36. Japan intelligence and Security Agencies, доступно на: http://www.fas.org/irp/world/japan/, приступљено: 20. 11. 2014.
37. Kalkavage, M., *Counterintelligence in the Kingdom and the States: A Historical Comparison of the FBI and MI5*, Master's Thesis, Boston University, Boston, 2014.
38. Кековић, З., *Системи безбедности*, Факултет безбедности, Београд, 2009.
39. Конатар, В., *(Не)Обавештајне операције као акти агресије*, Култура полиса, год. IX, бр. 17, 27-44, 2012.
40. Kotani, K., Current Japanese Intelligence Reform, n.d., доступно на: http://www.nuffield.ox.ac.uk/Research/OIG/Documents/kotani1.pdf, приступљено: 25. 11. 2014.

41. Крштенић, А., Матијашевић, М., *Проблеми обавештајних служби у процесу прилагођавања савременим изазовима, ризицима и претњама*, Војно дело, 105-125, 2014.
42. Лазовић, Р., *Међународна обавештајна сарадња*, Војно дело, 33-56, 2013.
43. Lewis, G., *Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation*, John Wiley & Sons Inc. Hoboken, New Jersey (USA), 2006.
44. Liaropoulos, A., *A (R)evolution in Intelligence Affairs? In Search of a New Paradigm*, Research paper No. 100, Research Institute for European and American Studies, 2006.
45. Лопушина, М., *Тајне службе света*, Књига-комерц, Београд, 2005.
46. Mazumdar, K., *Intelligence and Counterintelligence: First Line of Defence*, Research Institute for European and American Studies, 2012, доступно на: http://rieas.gr/research-areas/2014-07-30-08-58-27/transatlantic-studies/1719-intelligence-and-counterintelligence-first-line-of-defence, приступљено: 14. 4. 2015.
47. Мијалковић, С., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2009.
48. Мијалковски, М., Конатар, В., *Необавештајна роварења обавештајаца: у лавиринтима специјалних операција*, Прометеј, Нови Сад, 2010.
49. Мијалковски, М., *Обавештајне и безбедносне службе*, Факултет безбедности, Службени гласник, Београд, 2009.
50. Милашиновић, Р., Мијалковић, С., *Тероризам као савремена безбедносна претња*, Министарство унутрашњих послова Републике Српске, Висока школа унутрашњих послова у сарадњи са Ханс Зајдел фондацијом, Супротстављање тероризму- међународни стандарди и правна регулатива, Козара, 29-30. март, Висока школа унутрашњих послова, Бања Лука, 1-16, 2011.
51. Милашиновић, Р., Милашиновић, С., *Основи теорије конфликата*, Факултет безбедности, Београд, 2007.
52. Милашиновић, Р., *ЦИА: Моћ и политика*, Југоштампа, Београд, 1979.
53. Милошевић, М., *Систем државне безбедности*, Полицијска академија, Београд, 2001.
54. Милошевић, М., *Одбрана од тероризма*, Свет књиге, Београд, 2005.
55. Миљевић, М., *Скрипта из Методологије научног рада*, Филозофски факултет, Источно Сарајево-Пале, 2007.

56. National Counterterrorism Center, *2008 Report on Terrorism*, Office of the Director of National Intelligence National Counterterrorism Center, Washington, 2009.
57. Одлука о Савету за националну безбедност Републике Србије, „*Службени гласник РС*“ бр. 50/07, 31.05. 2007.
58. Organizational Chart-FBI, доступно на: http://www.fbi.gov/contact-us/fbi-headquarters/org_chart , приступљено: 24.02. 2015.
59. Office of the Director of National Intelligence, *National Counterintelligence and Security Center*, н.д., доступно на: http://ncix.gov/about/index.php, приступљено: 9.1.2015.
60. Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011.
61. Петровић, С., *Кибер простор- изворište нових претњи националној безбедности*, Међународни научно-стручни скуп: Информациона безбедност 2009, Београд.
62. Prunckun, H., *Extending the theoretical structure of intelligence to counterintelligence*, Salus Journal, 2, (2), 31-49, 2014.
63. Public Security Investigation Agency (Koancho), доступно на: http://fas.org/irp/world/japan/koancho.htm, приступљено: 20. 11. 2014.
64. Ронин, Р., *Обавештајни рад: Практични приручник*, Службени гласник, Факултет безбедности, Београд, 2009.
65. Савић, А., *Обавештајне службе и национална безбедност*, Правни факултет, Крагујевац, 2006.
66. Саздовска, М., *Обавештајни циклус*, НБП, XII, (1), 131 – 147, 2006.
67. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Foreign and Military Intelligence*, Book I –Final Report, Washington, U.S. Government Printing Office, April 26, 1976.
68. Second Investigation Department under the Ministry of National Defence, *Public Report on Activities 2013*, Vilnius, 2014.
69. Security Bureau, доступно на: http://fas.org/irp/world/japan/sb.htm, приступљено: 20. 11. 2014.
70. Симеуновић, Д., *Тероризам: Општи део*, Правни факултет, Београд, 2009.
71. Симеуновић, Д., *Увод у политичку теорију*, Институт за политичке студије, Београд, 2009.

72. Симеуновић, Д., *Теорија политике: Ридер I део*, Наука и друштво, Београд, 2002.
73. Стајић, Љ., *Основи система безбедности*, Факултет безбедности, 2008.
74. Станић, М., *Дефинисање садржаја појма безбедности*, Војно дело, 93-113, 2014.
75. Stratfor: Global Intelligence, *Japan's Intelligence Reform Inches Forward*, 2015, доступно на: https://www.stratfor.com/analysis/japans-intelligence-reform-inches-forward, приступљено: 25. 11. 2014.
76. Стратегија националне безбедности Републике Србије, Београд, април 2009, 4100309.042.doc/2.
77. The Definition of Counterintelligence, *National Security Act of 1947*, Congressional declaration of purpose- 50 U.S.C.401., January 3, 2012, United States Code, доступно на: http://www.gpo.gov/fdsys/granule/USCODE-2011-title50/USCODE-2011-title50-chap15-sec401, приступљено: 5. 2. 2015.
78. Theoharis, A., *Chasing Spies: How the FBI Failed in Counterintelligence But Promoted the Politics of McCarthyism in the Cold War Years*, FBI- Center for the Study of Intelligence, 2002, 47 (3), стр. 1, доступно на: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article07.html, приступљено: 6. 5. 2015.
79. U.S. Department of Justice, Federal Bureau of Investigation, Report to the National Commission on Terrorist Attacks upon the United States: *The FBI's Counterterrorism Program: Since September 2001*, Office of Public Affairs, Washington, April 14, 2004.
80. U.S. Department of Justice, Federal Bureau of Investigation, *Today's FBI: Facts & Figures 2013-2014*, Office of Public Affairs, Washington, n.d.
81. U.S. Department of Justice, Federal Bureau of Investigation, *FBI Information Sharing & Safeguarding Report 2012*, Office of Public Affairs, Washington, n.d.
82. U.S. Department of Justice, Federal Bureau of Investigation, Report, Terrorism 2002-2005, s.n., s.l., n.d.
83. FBI, *Counterintelligence Vulnerability Assessment for Corporate America*, s.n., 09. 18. 2009.
84. FBI Counterintelligence, *The Insider Threat: An introduction to detecting and deterring an insider spy*, доступно на: http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat , приступљено: 14.02.2015.

85. Федеральный закон о федеральной службе безопасности (с изменениями и дополнениями) Глава II, Основные направления деятельности органов Федеральной службы безопасности, 3 апреля 1995 г. N 40-ФЗ, (15-95), доступно на: http://base.garant.ru/10104197/, приступљено: 25.1.2015.
86. Hacking, Britannica, доступно на: http://www.britannica.com/search?query=hacking, приступљено: 10.1.2015.
87. Herman, M., *Intelligence Power in Peace and War*, The Royal Institute of International Affairs, Cambridge University Press, 2003.
88. Cabinet Research Office, доступно на: http://fas.org/irp/world/japan/naicho.htm, приступљено: 20. 11. 2014.
89. Цетинић, М., *Компјутерска кривична дела и њихови појавни облици*, Правни живот бр. 10, Удружење правника Србије, Београд, 1998.
90. CIA, *Counterintelligence for National Security*, Center for the Study of Intelligence, 2(4), 1993. доступно на: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a10p_0001.htm#5-security-measures-measures, приступљено: 10. 1. 2015.
91. Cooper, B., *CFIS: A Foreign Intelligence Service for Canada*, Canadian Defence & Foreign Affairs Institute, 2007.
92. Counterintelligence, Department of the Navy-Headquarters United States Marine Corps, Washington, D.C., MCWP 2-14, 5 September 2000.
93. Counterintelligence, Department of the Navy-Headquarters United States Marine Corps, Washington, D.C., MCWP 2-14, 7 Oct 1998.
94. Counterintelligence, MACCMILLAN Dictionary, доступно на: http://www.macmillandictionary.com/dictionary/british/counterintelligence, приступљено: 5.1.2015.
95. Counterintelligence, Cambridge dictionary, доступно на: http://dictionary.cambridge.org/dictionary/british/counterintelligence, приступљено: 5. 1. 2015.
96. Counterintelligence, CIA- Annual Reports 1999, доступно на: https://www.cia.gov/library/reports/archived-reports-1/ann_rpt_1999/dci_annual_report_99_16.html, приступљено: 23. 2. 2015.
97. Counterintelligence for National Security, доступно на: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a10p_0001.htm, приступљено: 25.11.2014.

98. Cybersecurity, Digital Agenda for Europe, доступно на: https://ec.europa.eu/digital-agenda/en/cybersecurity, приступљено: 19. 4. 2015.