УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ

Зоран М. Марјановић

ОДВРАЋАЊЕ КАО СТРАТЕШКИ КОНЦЕПТ У ПОСТХЛАДНОРАТОВСКОМ ПЕРИОДУ

докторска дисертација

Београд, 2023.

UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

Zoran M. Marjanović

DETERRENCE AS A STRATEGIC CONCEPT IN THE POST-COLD WAR PERIOD

Doctoral Dissertation

Belgrade, 2023

Подаци о ментору и члановима комисије

Ментор:
др Ненад Путник, редовни професор, Факултет безбедности, Универзитет у Београду

Чланови комисије:
др Зоран Драгишић, председник, редовни професор, Факултет безбедности, Универзитет у Београду

др Зоран Јефтић, члан, ванредни професор, Факултет безбедности, Универзитет у Београду

др Милан Миљковић, члан, доцент, Школа националне одбране „Војвода Радомир Путник”, Универзитет одбране у Београду

Датум одбране:_____

Изрази захвалности:

Спроведено истраживање изискивало је велики напор, уз редовне обавезе у породици и на радном месту, и резултат је моје вишедеценијске едукације и радног ангажовања. Извор снаге за завршетак докторских студија, у овом тешком времену, пронашао сам искључиво у својој породици, те им се овом приликом захваљујем на њиховим одрицањима током мог школовања.

Посебну заслугу у остварeним резултатима животним, па и овом, завређују моји родитељи, посебно мој отац, који ми је пружао подршку не само у лепим, већ и тешким тренуцима, давао савете и водио ме кроз живот усмеравајући ме. Нажалост, отац није дочекао завршетак мојих студија, што би га чинило веома сретним и поносним. Најбитнију тему, како постати човек, бити прво добар родитељ, частан, поштен и честити човек, стручан официр у свом послу, научио сам од њега, углавном само гледајући његове поступке и због тога му се захваљујем.

На крају, захваљујем се свом ментору на уложеном несебичном труду, без кога ово истраживање не би имало ваљан ток. Захвалност упућујем и професорима Факултета безбедности ангажованим на докторским студијама – једном изузетном, организационо и професионално састављеном колективу.

ОДВРАЋАЊЕ КАО СТРАТЕШКИ КОНЦЕПТ У ПОСТХЛАДНОРАТОВСКОМ ПЕРИОДУ

Сажетак

У спроведеном истраживању анализирани су технички термини у стратегијским документима великих сила – Сједињених Америчких Држава и Руске Федерације – који на раличите начине реферирају на термин *одвраћање* и експлицитно или посредно, настоје да га денотирају. Терминолошко одређење појма *одвраћање* (енг. *deterrence*) у англосаксонској литератури подразумева поступак обесхрабривања или обуздавања некога. Поступак се односи на сферу међународне политике и спољнополитичке циљеве, усмерене према националним државама, ради остваривања одређене присиле у циљу спречавања нежељених радњи или оружаног напада. Садржај овог појма укључује напор да се актер присили да поступа на одређени начин. Из угла Руске Федерације, стратешки циљеви одбрамбене политике треба да се реализују применом *стратешког одвраћања*. Два термина се у руском језику синонимно употребљавају за појам *одвраћање*: рус. *сдерживание* (обуздавање, одржавање, суздржавање) и рус. *устрашение* (застрашивање). Први термин обухвата све активности усмерене на превенцију рата, укључујући и оно што се у западном лексикону назива *задржавање*. Руско стратешко одвраћање је много шири појам од западног еквивалента (САД) и обухвата координисану активност војних и невојних мера (политичких, дипломатских, економских, научно – техничких, идеолошких и др.) ради остварења присиле у спречавању стратешке штете. То је концепт који обухвата оне активности које се на Западу називају доктрином *хибридног ратовања* Руске Федерације. Основна карактеристика одвраћања је да се користи како у доба мира, тако и у време рата, уз примену свих расположивих средстава. Други термин, *устрашение*, је уже повезан са нуклеарним способностима, тзв. нуклеарном присилом.

Истраживање је пратило историјску димензију развоја стратешко – доктринарног оквира Сједињених Америчких Држава и Руске Федерације. Фокус спроведеног истраживања био је на концептима одвраћања у постхладноратовском периоду, будући да су тада значајно мењани садржај и обим овог појма у стратегијским документима две велике силе, а самим тим и његово значење.

У истраживању је, осим тога, описана и објашњена улога служби безбедности (тајних служби обавештајног и контраобавештајног карактера) у реализацији активности одвраћања, дефинисаних у стратегијским и доктринарним документима двеју великих сила. У том смислу, анализиране су обавештајне, контраобавештајне и *необавештајне активности* (енг. *covert action* /*тајне акције*/, рус. *активные мероприятия* /*активне мере*/ или *мероприятия содействия* /*мере подршке*) њихових служби безбедности. Ове активности су се прилагођавале актуелним концептима одвраћања и углавном су подразумевале политичке, пропагандне, економске и паравојне активности, а почетком XXI века попримиле су форму и назив *информационих операција* и *сајбер одвраћања*.

Активности служби безбедности у реализацији стратегијских циљева одвраћања реализују се посредством најмодерније технике, а посебно информационо – комуникационих технологија. Различити концепти одвраћања и улога служби безбедности у њима су, у овом истраживању, елаборирани кроз конкретне студије случајева Естоније, Крима и Украјине. Наведене студије приказују начин на који су необавештајне активности спроведене у пракси, посебно апострофирајући улогу информационо – комуникационих технологија у конкретним операцијама.

У посебном одељку истраживања дата је предикција будућих активности одвраћања великих сила. У даљој прошлости ове активности биле су углавном везане за развој нуклеарног наоружања, док у новије време све већи утицај на одвраћање има развој или

поседовање нових хиперсоничних ракета и других напредних система за спровођење присиле над другима. Поседовање савремених техничко – технолошких средстава као што су беспилотне летелице, и развој нових и унапређење постојећих информационо – комуникационих технологија, детерминисаће стратешку предност над противником и у будућности дефинисати стратегијска и доктринарна документа технолошки напредних држава, а тиме и садржај и обим термина *одвраћање*.

Кључне речи: стратегија, доктрина, одвраћање, служба безбедности, обавештајна активност, контраобавештајна активност, необавештајна активност, дипломатија, сајбер одвраћање.

Научна област: науке безбедности.

Ужа научна област: студије безбедности.

DETERRENCE AS A STRATEGIC CONCEPT IN THE POST – COLD WAR PERIOD

Abstract

The conducted research analyzed the technical terms in the strategic documents of the great powers – the United States of America and the Russian Federation – which in different ways refer to the term deterrence and explicitly or indirectly try to denote it. The terminological definition of deterrence in Anglo – Saxon literature implies the process of discouraging or restraining someone. The procedure refers to the sphere of international politics and foreign policy goals, aimed at national states, in order to achieve certain coercion in order to prevent unwanted actions or an armed attack. This term inherently includes an effort to force an actor to act in a certain way. From the point of view of the Russian Federation, the strategic goals of the defense policy should be realized through the application of strategic deterrence. Two terms are used synonymously in the Russian language for deterrence: *сдерживание* (restraint, maintenance, restraint) and *устрашение* (intimidation). The first term includes all activities aimed at preventing war, including what is called containment in the Western lexicon. Russian strategic deterrence is a much broader concept than the Western equivalent (USA) and includes the coordinated activity of military and non – military measures (political, diplomatic, economic, scientific – technical, ideological, etc.) in order to achieve coercion in preventing strategic damage. It is a concept that includes those activities which in the West are called the doctrine of hybrid warfare of the Russian Federation. The main feature of deterrence is that it is used both in times of peace and in times of war, with the application of all available means. The second term, intimidation, is more closely related to nuclear capabilities, the so – called nuclear coercion.

The research followed the historical dimension of the development of the strategic – doctrinal framework of the United States of America and the Russian Federation. The focus of the conducted research was on the concepts of deterrence in the post – Cold War period, since the content and scope of this concept in the strategic documents of the two great powers, and therefore its meaning, were then significantly changed.

In addition, the research described and explained the role of the *security services* (secret services of an intelligence and counterintelligence character) in the implementation of deterrence activities, defined in the strategic and doctrinal documents of the two great powers. In this sense, the intelligence, counterintelligence and *non – intelligence activities* (English: *covert action*, Russian: *активные мероприятия* /active measures/ or *мероприятия содействия* /support measures) of their security services were analyzed. These activities were adapted to the current concepts of deterrence and mainly included political, propaganda, economic and paramilitary activities, and at the beginning of the 21st century they took the form and name of information operations and cyber deterrence.

The activities of the security services in the realization of the strategic goals of deterrence are realized through the most modern techniques, especially information and communication technologies. Different concepts of deterrence and the role of security services in them are elaborated in this research through concrete case studies of Estonia, Crimea and Ukraine. The mentioned studies show the way in which non – intelligence activities were carried out in practice, especially apostrophizing the role of information and communication technologies in concrete operations.

In a separate section of the research, a prediction of the future deterrence activities of the great powers is given. In the distant past, these activities were mainly related to the development of nuclear weapons, while more recently, the development or possession of new hypersonic missiles and other advanced systems for enforcing coercion on others has a growing influence on deterrence. The possession of modern technical and technological means such as unmanned aerial vehicles, and the development of new and improvement of existing information and communication technologies, will determine the strategic advantage over the opponent and in the future define the strategic and doctrinal documents of technologically advanced states, and thus the content and scope of the term deterrence.

Key words: strategy, doctrine, deterrence, security service, intelligence, counterintelligence, non – intelligence, diplomacy, cyber deterrence.

Scientific field: Security Sciences.

Specialized Scientific Field: Security Studies.

САДРЖАЈ

1. УВОД

Историјски посматрано, у тренуцима кад је долазило до преломних тренутака испољавања међународног утицаја држава, односно до испољавања моћи (политичке, економске, војне и др.) на другу или друге државе како би се остварили национални интереси, кључне улоге у државним стратегијама одвраћања имале су службе безбедности кроз примену обавештајних, контраобавештајних и необавештајних активности. Ово је примењивано онда кад дипломатија није имала могућност да доврши циљеве постављене од стране доносилаца политичких одлука дате државе. Раније су те методе држане у строгој тајности, па се мало тога или готово ништа није могло спознати кроз научна сазнања, односно научно истраживати. Међутим, неколико деценија уназад је спроведен велики број научних истраживања у Сједињеним Америчким Државама (у даљем тексту: САД) и другим државама о *тајној акцији* (термин који се користи у литератури САД) и *активним мерама* (термин који се користи у литератури Руске Федерације, у даљем тексту: РФ) служби безбедности. Када говоримо о тајним акцијама и активним мерама у Републици Србији, употребљавамо појам *необавештајне активности* (термин који користе Милошевић, 2005; Мијалковски и Конатар, 2010; Мијалковић 2011; Бајагић, 2010; 2013; 2015а; Конатар, 2015; Трбојевић, 2017; Лабовић и Марјановић, 2021; Марјановић, 2022; и др.; за потребе овог истраживања, уместо појмова тајна акција и активне мере биће коришћен општији појам – необавештајне активности), док је данас готово немогуће говорити о овим активностима служби безбедности, а да то не буде с посебним освртом на информационе операције (Миљковић, 2016). У питању су активности одвраћања у којима учествују или их спроводе службе безбедности, а где је веома тешко установити идентитет лица која их спроводе; сами извршиоци су физички удаљени од ефеката оваквих операција (напада), и интензивно се користе као замена за савремени агентурни рад.

Ради одвраћања других држава, необавештајне активности су подразумевале деловања служби безбедности у политичким, економским, пропагандним, као и у паравојним активностима. Сједињене Америчке Државе су биле у великој мери изненађене кад су њихове службе безбедности открили да је РФ покренула неколико необавештајних активности почев од сајбер напада у Естонији 2007. године, затим у руско – грузијском оружаном сукобу 2008. године и приликом анексије Крима 2014. године, све до широко распрострањене операције утицаја усредсређене на америчке председничке изборе 2016. године, сајбер напада у Украјини 2017. године, сајбер напада у Пољској 2021. године усмерених на политичаре, и других сличних активности. Овакве операције присутне су скоро свакодневно широм планете, али поменуте операције су најбитније и највеће акције овог типа. Савез Совјетских Социјалистичких Република је развијао и примењивао утицајне операције, тада називане *активним мерама* против САД и њихових савезника. Током последње деценије хладног рата, САД су се активно бориле против ове претње што је с распадом Савеза Совјетских Социјалистичких Република 1991. године „одвело" необавештајне активности „на одмор", али САД су наставиле са применом необавештајних активности и у овом периоду. Кроз ово истраживање се тврди да је трансформацијама стратегија одвраћања РФ „прекинула одмор" активним мерама и почела да их користи широм света ради остварења стратешких националних интереса одвраћања које код РФ

предвиђају не само мере одвраћања дефанзивног већ и офанзивног карактера, мере које се предузимају са циљем одвраћања друге државе од нежељених утицаја.

У овом смислу, у истраживању ће се испитивати трансформација стратегија одвраћања, као и инструмената за спровођење одвраћања кроз необавештајне активности, али и потреба за сузбијањем различитих облика злонамерног утицаја и обмана непријатеља (непријатељске информационе операције које представљају важан узрок пропуста у раду служби безбедности). Ово истраживање треба да утврди колику моћ имају службе безбедности приликом реализације необавештајних активности, као и до којих све негативних последица може да дође због грешака у реализацији ових активности. Истраживање би се бавило и позитивним последицама, кроз сагледавања поступака у примени ових мера ради заштите државе. Традиционални, тј. класични (дуги) и скупи оружани сукоби се начелно и у пракси избегавају (код држава које немају економско – енергетску независност), док је трка у наоружању променила своју природу, како транзицијом у сајбер простор, тако и кроз надмудривања кроз различите врсте необавештајних активности. Такође, оно што је карактеристично за нове околности је изналажење нових решења у развоју наоружања, ратне технике, летелица и других војних и невојних средстава и опреме, који ће утицати на промену комплетних стратегија одвраћања, али и доктрина употребе јединица или уопште употребљивости неких борбених система. Најбољи примери за то су развој хиперсоничних ракета које нису доступне другима, развој беспилотних летелица – дронова, развој информационих и телекомуникационих технологија које су недоступне другима и слично.

2. ТЕОРИЈСКО МЕТОДОЛОШКИ ОКВИР ИСТРАЖИВАЊА

2.1. ПРЕДМЕТ И ЦИЉЕВИ ИСТРАЖИВАЊА

2.1.1. Предмет истраживања

У докторској дисертацији је истраживана генеза концепта одвраћања и трансформација стратегија одвраћања великих сила после Хладног рата до данас, као и начини спровођења ових стратегија. У том смислу, биће сагледана улога служби безбедности и њихових активности (првенствено необавештајних) у физичком и сајбер простору, с циљем одвраћања противника у извршавању спољнополитичких циљева државе.

Реч је о активностима одвраћања које спроводе савремене службе безбедности (или други државни органи) ради „јачег утицаја" на друге државе, владаре, институције, корпорације, фирме, појединце и друге актере, с тим да наведена активност није у обавези да буде усмерена искључиво према непријатељу, већ може бити примењена и ради помоћи савезнику. Активности су се мењале са променом технологија, наоружања, оружја и оруђа, нуклеарног наоружања, а посебно с појавом интернета који је омогућио концепт сајбер одвраћања.

Изучавањем литературе могу се констатовати одређене промене у стратегијама одвраћања како у САД тако и у РФ, а посебно у примени необавештајних активности служби безбедности. До промена доводи првенствено развој технологија и прилагођавање стратегија одвраћања држава новонасталим променама. Рад служби безбедности услед напретка

савремених информационо – телекомуникационих технологија, такође је претрпео промене као и други органи укључени у необавештајне активности, а поготово у сфери одвраћања.

Како бисмо утврдили садржај и обим предмета истраживања неопходно је извести његово теоријско одређење које се састоји из одређења појмова који се користе у овом истраживању као и прегледа постојећих сазнања.

Постављени предмет истраживања је сложен и недовољно истражен. *Операционализација предмета истраживања* је реализована кроз пет поглавља.

Прво поглавље је посвећено концепту одвраћања великих сила у периоду након Хладног рата. У овом делу рада су обухваћене две велике силе, САД и РФ. Концепт одвраћања у САД је сагледан кроз анализу стратегијско – доктринарних докумената (председничких доктрина, војних доктрина) који регулишу ову област и истраживања о стратегијама одвраћања. Стратешко одвраћање у РФ и концепти одвраћања после Хладног рата кроз анализу Стратегије националне безбедности и Војне доктрине приказали су специфичности које носи концепт одвраћања у РФ. У овом поглављу су сагледана и размимоилажења западних и источних теоретичара о одвраћању у САД и РФ.

Друго поглавље се бави основним појмовним одређењима служби безбедности, као и активностима којима се баве службе безбедности с фокусом на значају обавештајне, контраобавештајне и необавештајне активности. Начин прикупљања података и оперативни рад служби безбедности су сагледани од појмовних, теоретских одређења до практичних делатности у реализацији активности одвраћања. У овом поглављу је анализиран однос политике, дипломатије и служби безбедности. Посебно је анализирана спрега дипломатије и обавештајних активности, као и специфичности које овакве активности носе у концепту одвраћања.

У *трећем поглављу* је направљен посебан осврт на необавештајне активности и информационе операције као врсте активности у којима учествују или које предузимају службе безбедности. Ово поглавље садржи детаљно објашњење појмовног одређења необавештајне активности у научној и стручној литератури у САД и РФ као и у садржајима које обухватају необавештајне активности у Републици Србији, са нагласком на проблему различитих појмовних одређења истих или сличних активности у наведеним државама. Објашњена је веза између необавештајне активности и информационих операција. Такође, описане су и класификоване и друге сфере необавештајне активности: *пропагандне активности, политичке активности, економске активности* и *паравојне активности*. У свакој од наведених сфера необавештајне активности данас значајно место заузима сајбер простор у коме се спроводе информационе операције. У том смислу, сагледано је традиционално схватање необавештајне активности и насупрот њему савремено схватање које посебан нагласак ставља на информационим операцијама као средству за спровођење необавештајних активности. У овом поглављу су представљене и нове теорије које се баве односом информационих операција и необавештајних активности. Оно што је неизбежно у сагледавању ових појава јесу и етичка питања употребе необавештајне активности, како у традиционалном облику, тако и путем информационих операција.

Четврто поглавље даје преглед резултата истраживања о месту и улози служби безбедности у конкретним случајевима сајбер напада, посматраних у парадигми необавештајних активности служби безбедности и то сајбер напада на Естонију спроведеног 2007. године, обмане приликом анексије Крима 2014. и сајбер напада на Украјину 2017.

године. У наведеним студијама случаја су анализиране карактеристике и посебности примене сајбер напада у оквиру извођења акција служби безбедности. У овом поглављу су представљена искуства у примени сајбер напада од стране служби безбедности и анализиране неопходне нове мере безбедносне заштите критичних информационих и комуникационих технологија система држава и савеза.

У *петом поглављу* су сумирани резултати истраживања и дата закључна разматрања о перспективама утицаја стратегија одвраћања великих сила на делатност служби безбедности као и о угрожености националне безбедности држава према којима се примењују необавештајне активности и информационе операције. Анализирањем утицаја нових технологија на концепте одвраћања великих сила истражено је условљавање промена до којих тај утицај доводи. У овом поглављу су дате смернице за ревидирање стратешко – доктринарних докумената Републике Србије, као и предикција очекиваних промена у делокругу и начину рада служби безбедности у будућности.

Већи део планираног истраживања се односио на актуелна схватања и поступања служби безбедности и других учесника у необавештајним активностима САД и РФ, као и на савремена решења по питањима безбедности преточена у стратегијско – доктринарна документа која регулишу одвраћање и необавештајну активност и заштиту од угрожавања безбедности државе.

2.1.2. Циљеви истраживања

Из области необавештајне активности служби безбедности неколико деценија уназад истражен је велики број аспеката необавештајне активности (тајне акције – операције, прикривене акције, тиха опција, трећа опција, специјална операција, специјалне политичке акције, реметилачке акције, активне мере и др.). Један од начина (зло)употребе служби безбедности од стране врха државе је и примена необавештајних активности. Циљ спровођења необавештајних активности је остварење амбиција доносилаца политичких одлука да „чвршће" од обичне дипломатије остваре утицај силе према другој или више других држава, корпорација или друштвених група. Део теоретичара као посебну категорију необавештајних активности сврстава економску акцију која обухвата смањење економске моћи и спутавање економије циљне државе. У овој области постоји литература о студијама случајева већ реализованих операција. Анализирајући доступну литературу, остаје неистражено више питања, а нека укључују различита појмовна одређења необавештајне активности, нормативно уређење предузимања оваквих активности, па самим тим и утицаја на демократију једне државе, квалитет предузетих операција (њихова контрола), материјалне и нематеријалне трошкове, посебне методе које се користе и др. (Kibbe, 2017). Овакав вид деловања је финансијски много исплативији него употреба оружаних снага, улазак у рат са државама, јер некада наизглед тактичко деловање према појединим државама може остварити циљеве стратегијског значаја чиме би се избегавали скупи оружани сукоби. Ангажовање служби безбедности на контраобавештајним и/или обавештајним активностима се најчешће заснива на прикупљању и анализи података, састављању и анализи информација, док су необавештајне активности углавном активни, офанзивни инструмент служби безбедности односно спољне државне политике (Uram, 2005). У истраживању ће бити коришћена класификација необавештајне активности на неколико главних категорија необавештајних активности: пропаганду, политичку акцију, паравојну акцију, информациону

операцију и друго, са намером да држава званично не призна деловање (Lowenthal, 2009). Међутим, овај принцип непризнавања деловања у одређеним необавештајним активностима може понекад да буде запостављен и да чак и председник државе лично призна учешће у одређеним необавештајним активностима.

Научни циљ овог истраживања је проширење фонда постојећих и стицање нових сазнања о концептима одвраћања у стратешко – доктринарним документима великих сила, о деловању служби безбедности и других елемената државног апарата, као и о аспектима необавештајне активности (укључујући и информационе операције) у савременим околностима развијених технологија, друштвене међуповезаности и других услова који доводе до прилагођавања необавештајне активности савременим условима. Научни циљ истраживања јесу научна идентификација, дескрипција и објашњење концепта одвраћања у стратешко – доктринарним документима великих сила у периоду након Хладног рата и објашњење улоге служби безбедности у њиховој реализацији.

Практични (*апликативни*) *циљ* овог истраживања јесте долажење до сазнања о методологији израде безбедносне процене и стратешких докумената САД и РФ у области безбедности и одбране, као и методици рада служби безбедности ових држава. Такви увиди могли би бити од користи руководећим органима у систему безбедности Републике Србије у процесу ревизије или израде нових националних стратешко – доктринарних докумената и унапређењу рада служби безбедности.

Стечена сазнања могу представљати полазни основ за ревидирање и формулисање будућих националних стратегијско – доктринарних докумената с обзиром на стратешке циљеве заштите Републике Србије од нових безбедносних претњи међу којима свакако предњаче необавештајне активности страних служби безбедности, посебно у сајбер простору.

Осим ових, истраживање може допринети и нормирању појмовно – терминолошког корпуса у овој области, будући да је тренутно у синонимној употреби већи број страних техничких термина, што доводи до додатних тешкоћа у разумевању предметне проблематике.

2.2. ИСТРАЖИВАЧКА ПИТАЊА

У епистемолошком смислу, оквирима и у условима напред наведених појмовних, теоријских и нормативних недоречености, поставља се питање како можемо приступити истраживању концепта одвраћања великих сила с посебним освртом на примену необавештајних активности служби безбедности након завршетка Хладног рата.

Досадашња истраживања концепта одвраћања и употребе необавештајних активности служби безбедности, кад се сумирају кључни теоријски налази у овој области, могуће је представити кроз неколико истраживачких питања која су коришћена као смернице за планирано истраживање:

- Који су концепти одвраћања присутни код великих сила у периоду након завршетка Хладног рата и како су они артикулисани кроз стратегијско – доктринарне оквире?
- На који начин је убрзан техничко – технолошки, а посебно развој информационих и телекомуникационих технологија, утицао на промене у стратегијама одвраћања великих сила након завршетка Хладног рата?

- Која су општа, посебна и специфична обележја необавештајних активности у савременим околностима обликованим развојем информационим и телекомуникационим технологијама?
- Како су се трансформисале службе безбедности зарад реализације савременог концепта одвраћања?
- На који ће начин концепт одвраћања утицати на креирање безбедносних политика националних држава у блиској будућности?

Посебну пажњу заслужују претходно наведена питања која се односе на узроке који су довели до промена у стратешко – доктринарном концепту одвраћања код великих сила и настанка нових облика необавештајних активности.

Основни проблем овога можемо представити кроз следећа питања:

- Која стратешко – доктринарна документа великих сила су успоставила и појмовно уобличила концепт одвраћања?
- Шта је узрок промена насталих у стратегијама и доктринама одвраћања након Хладног рата?
- На који начин су промене у природи самог концепта одвраћања која се декларише кроз поменута документа утицале на начин спровођења тих активности?
- Да ли је сајбер нападе спроведене у Естонији, Криму и Украјини могуће одредити као необавештајне активности и које су њихове кључне карактеристике?
- Да ли су државе након завршетка Хладног рата постале изложеније утицају необавештајних активности?
- Каква ће бити методологија одвраћања великих сила у будућности и да ли ће она захтевати већу употребу необавештајних активности?

Сходно претходно наведеном, проблем истраживања одређен је низом питања на која се током истраживања одговарало. Истраживање се руководило показатељима назначеним у стратешко – доктринарним документима великих сила – САД и РФ – као и у обимној савременој научној и стручној литератури.

2.2.1. Кључни појмови

Велике силе или *велесиле*[1] су за потребе овог истраживања дефинисане као државе које имају могућност да изврше утицај на глобалном нивоу. Велике силе поседују карактеристичну војну, економску, дипломатску, политичку, културну и друге врсте моћи које могу употребити над мањим државама и нацијама (Kissinger, 1994; Mearsheimer, 2001; Лукашук, 2005; Муса, 2016; Erickson, 2018). У овом истраживању се пре свега мисли на САД и РФ.

[1] Концепт *велике силе* је први увео немачки историограф Ранке Леополд фон (*Leopold von Ranke*, Берлин) званични историограф Пруске од 1841. године. Истраживачи су користили термин у XIX веку, сходно значењу које му је припадало после Бечког конгреса 1815. године, који је учврстио однос снага између водећих сила тог времена – Русије, Пруске, Аустрије, Француске, Велике Британије, које су имале пресудан утицај на систем међународних односа и њихово правно регулисање. Крајем XX века само 5 држава које су биле сталне чланице Савета безбедности Уједињених нација имале су правни статус *великих сила* – Савез Совјетских Социјалистичких Република, САД, Енглеска, Француска и Кина. Критеријуми за велике силе су се временом мењали. У почетку је главна пажња поклањана војној сили – моћи, касније је економски и научно – технички потенцијал државе, њен *морални и политички ауторитет* почео да игра све значајнију улогу (Лукашук, 2005; Муса, 2016).

Стратегија потиче од грчке речи *стратегос* са значењем вођства, што је као и сам настанак појма стратегија везано за војску, те и тумачење вођства је у војном смислу и тиче се планирања, начина распоређивања ресурса за постизање одређених циљева. Карл фон Клаузевиц (*Carl von Clausewitz,* 1780 – 1831), пруски генерал и војни теоретичар, је изговарањем чувене реченице „Стратегија је економија силе", врло често сврставан међу прве стратеге. Поглед уназад на историју, међутим, открива да су многе војсковође и пре њега, као што су Цезар (*Caesar*), Сун Цу (*Sun Tzu*) и Макијавели (*Machiavelli*), војно дизајнирале и формулисале мотивисане стратегије. Свака од ових војних стратегија, од којих неке потичу из антике, важи и за управљање по аналогији, где концентрација ресурса, изненађење, иновације, организација и комуникација, координација циљева и ресурса, разматрање сопствених снага, представљају кључ тј. решење за данашње доносиоце одлука у свакодневном пословању на тржишту, конкурентне и корпоративне актере (Kotler, Berger & Bickhoff, 2010). Под модерним схватањем стратегије подразумева се „пут којим се ограниченим ресурсима достижу пројектовани дугорочни циљеви односног субјекта (на кога се односи стратегија: држава, војска, предузеће...)" (Форца, 2018, стр. 178). *Стратегија* је и општи план активности којом се спроводе конкретне, јасно дефинисане обавезе.

Одвраћање (енг. *deterrence*) у западној литератури је поступак обесхрабривања или обуздавања некога, у светској политици, најчешће националних држава од предузимања нежељених радњи, између осталих и оружаног напада. Укључује напор (испољавање „јачег утицаја") да се реализује или заустави, односно спречи одређена радња, што је покушај да се актер натера на жељено поступање или непоступање (Schelling, 2008; Buzan & Hansen, 2009; Freedman, 2009; Morgan, 2012; Gray, 2016; Mazarr, 2018). Када се у званичним документима РФ наводи да су стратешки циљеви Русије одбрамбена политика која ће се реализовати применом *стратешког одвраћања,* можемо кроз руски језик да анализирамо два термина за појам *одвраћање* – рус. *сдерживание* (обуздавање, одржавање, суздржавање) и рус. *устрашение* (застрашивање). Први појам је схваћен много шире од западног схватања одвраћања, да обухвати све активности усмерене на превенцију рата, укључујући оно што се у западном лексикону назива *задржавање*. Руско *стратешко одвраћање* је много шири појам од његовог директног западног еквивалента (САД), како због његових језичких корена, тако и због тога што је руски концепт постао експанзивнији последњих година. Други руски термин, *устрашение* је уже повезан са нуклеарним способностима. Овај термин се обично користи да прикаже (нелегитимну) политику одвраћања, по линији „нуклеарне уцене" (National Security Strategy of the Russian Federation, 2009). *Стратешко одвраћање* је описано у војно – енциклопедијском речнику Министарства одбране РФ и представља „координирани систем војних и невојних (политичких, дипломатских, правних, економских, идеолошких, научно – техничких и других) мера предузетих узастопно или истовремено са циљем одвраћања војне акције која за собом повлачи штету стратешког карактера. Стратешко одвраћање је усмерено на стабилизацију војно – политичке ситуације како би се утицало на противника у унапред одређеним оквирима, или за деескалацију војног сукоба. Објекти на које треба утицати кроз стратешко одвраћање могу бити војно – политичко руководство и становништво државе потенцијалног противника (или коалиције држава). Мере стратешког одвраћања се спроводе континуирано, како у мирнодопско тако и у ратно доба" (Bruusgaard, 2016, p. 10, 11). Можемо закључити да је с*тратешко одвраћање* концепт који обухвата оно што други (углавном на Западу) називају доктрином *хибридног ратовања* РФ, руску

способност за принудом (The Russian Federation's National Security Strategy, 2009). Taj концепт, *стратешко одвраћање* је много шири концепт од замишљеног западног концепта одвраћања. Мада му у називу стоји одвраћање, он није потпуно одбрамбени, већ садржи како одбрамбене тако и офанзивне, нуклеарне, ненуклеарне и невојне алате за одвраћање. Карактеристика им је да се они користе и у доба мира и рата. Представља низ поступака, мера суздржавања, одвраћања и принуде. У овим активностима се примењују сва расположива средства за одвраћање или доминирање сукобом.

Безбедност као један од најкомплекснијих појмова има велики број дефиниција. У Републици Србији, најприхватљивије одређење за безбедност (уједно и за ово истраживање) јесте да је безбедност „једна, једина и недељива (интегрална) у времену и простору, било да је схватамо као стање, функцију, организацију, политику, филозофију или нешто слично" (Стајић и Лазић, 2015, стр. 54). Савремено схватање појма безбедности можемо да одредимо и као „својство неког реалног друштвеног, природног или техничког субјекта (бића, творевине или ствари) испољено као успостављено, одржано и унапређено стање и/или 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" (Стајић и Лазић, 2015, стр. 60). Овде теоретичари сагледавају следеће елементе: својство, субјект (реални друштвени, природни, технички), стање и/или вредност, испуњеност минимума безбедносних стандарда и омогућавање опстанка, рада, раста и развоја, док према већини западних теоретичара, безбедност укључује ублажавање претњи драгоценим вредностима. Дефинисана на овај начин, безбедност је неизбежно политичка, игра виталну улогу у одлучивању ко добија шта, када и како у светској политици. Ово укључује тумачење прошлости – како су различите групе размишљале и практиковале безбедност, разумевање садашњости и покушава да утиче на будућност (Williams, 2008). Међутим, битно значење израза *безбедност* дато је у првом руском закону „О безбедности" из 1992. године у којој је дефинисана безбедност – *национална безбедност* (рус. *безопасность – Статья 1*.) као „стање заштите виталних интереса појединца, друштва и државе од унутрашњих и спољашњих претњи" (Закон РФ „О безопасности", 1992, p. 1).

Најстручнији органи који се баве питањима безбедности у свакој држави су службе безбедности и оне спроводе обавештајне, контраобавештајне (негде и безбедносне, прим. аут.) и необавештајне активности.

Службе безбедности на западу се углавном дефинишу као енг. *intelligence*, што подразумева и обавештајне и контраобавештајне службе. Међутим, када се жели нагласити да се ради о служби безбедности која се тежишно бави активностима обавештајне природе, тада се користи термин енг. *foreign intelligence,* а уколико се наглашава да се мисли на службу безбедности која се првенствено бави контраобавештајним активностима, тада се употребљава појам енг. *counterintelligence* (Johnson, 2007b; Gill, 2010). *Службе безбедности* се у значењу често мешају приликом коришћења овог термина. У РФ, службе безбедности (обавештајна – рус. *разведка* и контраобавештајна – рус. *контрразведка* служба) су „управо они елементи политичког система државе преко којих они који су на власти, владајућа елита, спроводи концепт, доктрину државног интереса. Преко њих се спроводе претензије државе на право да не поштује законе које мора да штити, ако то захтевају такозвани виши државни интереси. Ради се о посебним службама које су изнад закона, друштва, морала, универзалних

вредности. Свака контрола и надзор је у суштини формалан, јер активности служби безбедности у суштини представљају скуп тајних, завереничких активности које се међусобно смењују" (Шаваев & Лекарев, 2003, p. 21, 22). Једно од теоретских одређења у Републици Србији је да се под *службом безбедности* подразумева „специјализована организација државног апарата која специфичним методама и средствима спроводи обавештајне, контраобавештајне и безбедносне, субверзивне (необавештајне активности) и друге активности с циљем заштите унутрашње и спољне безбедности и реализације стратешких циљева сопствене државе, као и интереса саме те службе" (Милошевић, 2001, стр. 23). Врло често се синтагма обавештајне службе користи да би се говорило о служби безбедности, али разлог је недовољно познавање безбедносно – обавештајног система, делокруга, надлежности, послова којим се баве и методологије рада. У свим правним документима у Републици Србији је у употреби управо термин службе безбедности, било да се ради о служби мешовитог типа, или безбедносној, или обавештајној. Службе безбедности представљају „специјализоване, релативно самосталне институције државног апарата овлашћене да легалним, јавним, али и тајним начинима и средствима прикупљају одређене безбедносне податке и информације о другим државама или њеним институцијама, као и о могућим непријатељима, а ради вођења државне политике, односно које својим мерама и поступцима делују на осујећивању и пресецању одређене антиуставне делатности усмерене против државе и њених грађана, супротстављање деловању обавештајних служби, тероризма, међународног организованог криминала, тежих облика привредног криминала и корупције" (Стајић, 2013, стр. 221).

Обавештајна активност у земљама енглеског говорног подручја се означава изразом енг. *intelligence*, што је само једно од више различитих значења која се придају овом појму. У коју сврху ће се термин употребити зависи првенствено од тога шта се њиме конкретно жели означити. Појам енг. *intelligence* се може дефинисати као *обавештајна активност*, која „чини јединство више међусобно повезаних фаза (опажање обавештајног проблема, дефинисање потреба и захтева, прикупљање, процењивање и анализа, интерпретација, интеграција, израда завршних докумената, уступање и тумачење обавештајних сазнања). Као знање, енг. *intelligence* је завршни обавештајни производ, синтетизовано обавештајно знање које се у различитим формама обавештајних докумената уступа крајњим корисницима – стварним субјектима процеса спољнополитичког одлучивања, као и онима који непосредно учествују у спровођењу дефинисаних спољнополитичких циљева и утврђених праваца спољнополитичке акције" (Савић и Бајагић, 2003, стр. 37). *Обавештајна активност* (енг. *foreign intelligence*) је нормативно одређена као активност служби безбедности у прикупљању информација које се односе на способности, намере или активности страних влада или њихових елемената, страних организација или страних лица или међународних терористичких активности (National security act of 1947, 2021). Обавештајна активност укључује тајне операције; она је тајна, државна активност о разумевању или утицају на стране субјекте, ентитете. Обавештајна активност укључује и тајне операције које се изводе и изазивају одређене ефекте у туђини, иностранству, другим државама или ентитетима, па и према лицима када они представљају виши државни интерес (Warner, 2002). Обавештајна активност се према њеној сврси види и као активност за предузимање прикривених акција, истрага, а посебно препорука вођама политике тј. државе ради сузбијања претњи. Обухвата тајност, информације, обавештајни циклус, контраобавештајни рад, стратешке претње и

прикривене акције (Gill, 2010). У литератури РФ, обавештајна активност представља прикупљање информација, користећи не само отворене изворе, већ и податке добијене од шпијуна, агената, пребега, након чега следи анализа која се састоји у приказу и поређењу података и у њиховој даљој трансформацији у обавештајне производе који помажу у развоју политичке одлуке, обезбеђујући моћ релевантним и поузданим информацијама, захваљујући којима се сагледавају сложене ситуације и питања (Geneva Centre For The Democratic Control Of Armed Forces, 2006). У нормативним документима РФ за обавештајне активности је дефинисано да се спроводе добијањем и обрадом информација о стварним и потенцијалним могућностима, акцијама, плановима и намерама страних држава, организација и појединаца који утичу на виталне интересе РФ и помоћ у спровођењу мера које држава предузима у интересу обезбеђења безбедности РФ. Потребу за обављањем обавештајних активности у границама својих овлашћења утврђују председник РФ и Савезна скупштина (Федеральный Закон „О Внешней Разведке", 1996). Уопштено, службе безбедности имају три основне функције: прикупљање, анализу и контраобавештајну активност која је кључна за читаву обавештајну активност.

Контраобавештајна активност (енг. *counterintelligence*) означава прикупљање информација и спровођење активности у циљу заштите од шпијунаже, друге обавештајне активности, саботаже или атентата које су планирале стране владе или други елементи у име страних организација, или страних лица, или међународних терористичких активности (National security act of 1947, 2021). Контраобавештајна активност представља прикупљање информација и активности спроведених у циљу идентификовања, обмањивања, експлоатације, ометања или заштите од шпијунаже, других обавештајних активности, саботаже или атентата за или у име страних сила, организација или особа, или њихових агената, или међународних терориста организације или активности (Executive Order 12333, 2008). У нормативима РФ (Савезни закон, члан 9.), контраобавештајне активности су дефинисане као оне које обављају савезни органи, службе безбедности и/или њихове јединице, као и службена лица ових органа и подсектора путем контраобавештајних мера у циљу откривања, спречавања, сузбијања обавештајне и друге активности специјалних служби и организација страних држава, као и појединаца, усмерене на наношење штете безбедности РФ (О федеральной службе безопасности, 2022). Поред горе поменутих активности које спроводе првенствено контраобавештајне службе, део *необавештајних активности* реализују такође и контраобавештајне службе (наведена специфичност је различита од једне до друге контраобавештајне службе, службе безбедности).

Необавештајна активност (често изједначавана са субверзивним активностима, прим. аут.) обавештајних служби, све је чешће четврта функција која је тренутно најспорнија у демократском модерном друштву. Процес обавештајне активности (обавештајни циклус) би се требао обично завршити анализом реализације конкретног обавештајног задатка, обавештајног истраживања – ово је тзв. енг. *feedback* (с обзиром на законска овлашћења обавештајних служби). Међутим, досадашња пракса је показала „да су (амерички) обавештајни руководиоци често учествовали и у даљем току спољнополитичког одлучивања, од предлагања праваца спољнополитичке акције и избора једног правца, избора средстава и спољнополитичких поступака, до планирања и организовања конкретне спољнополитичке акције. У тим ситуацијама службе безбедности се појављују као непосредни и/или посредни учесници, посебно када се ради о планирању и спровођењу *субверзивних* садржаја,

карактеристичних за спољну политику појединих држава. На том нивоу обавештајна активност се комбинује са сродним активностима (*тајне акције*), при чему руководни нивои служби безбедности врше анализу тих активности (праћење успешности акције – енг. *feedback*) и планирају наредне обавештајне и сродне активности с обзиром на потребе спољне политике" (Савић и Бајагић, 2003, стр. 49, 50). Необавештајне активности су привилегија углавном офанзивних служби безбедности, што овде можемо констатовати. Када је реч о *тајним акцијама* и *активним мерама*, у Републици Србији се употребљава појам *необавештајне активности* (термин који користе Милошевић, 2005; Мијалковски и Конатар, 2010; Мијалковић 2011; Бајагић, 2010; 2013; 2015а; Конатар, 2015; Трбојевић, 2017; Лабовић и Марјановић, 2021; Марјановић, 2022; и др.), док је данас готово немогуће говорити о овим активностима служби безбедности, а да то не буде с посебним осврtом на *информационе операције* (Миљковић, 2016). Када је реч о активностима служби безбедности у контексту овог истраживања тада исте сагледавамо кроз конкретне активности служби безбедности у политичким, пропагандним, економским и паравојним активностима. Службе безбедности ове активности реализују кроз необавештајне активности које се могу одредити и као *тајне акције – операције,* тиха опција, трећа опција, специјална политичка акција, *активна мера* итд. Необавештајна активност одређује се као активност службе безбедности која се предузима ради вршења утицаја на друге државе, организације, појединце и друге субјекте, првенствено у иностранству и ради остварења националних интереса матичне државе, а између осталих и на одвраћање од намера које нису у складу са интересима матичне земље. Необавештајне активности подразумевају тајне методе реализације спољне и безбедносне политике, мање гласне и наметљиве од примене отворене оружане силе. Представљају активност која се налази између дипломатије и отвореног рата где службе безбедности директно или индиректно организују и/или реализују те активности (Uram, 2005; Lowenthal, 2009; Kibbe, 2017). Под *субверзијом* подразумевамо активности намењене утицају унутрашње политике циљане земље. Овом термину се нуди користан и конкретан начин за разумевање претње руских активности. Велика је флуктуација различитих термина који се користе за исту или сличну активност, а то су: *хибридно ратовање, активне мере, тајне акције, непријатељске мере, сива зона, политички рат* или *оштра моћ* (Radin, Demus & Marcinek, 2020).

Сива зона (енг. *gray zone*) је врло често описивана као борба дуга 45 година током Хладног рата. Западне државе (првенствено САД) су развиле нове приступе за одвраћање и супротстављање тада Савезу Совјетских Социјалистичких Република и њеним *активним мерама* и другим мерама осим рата током тог периода (Monaghan, 2022). *Сива зона* је одређена као део спектра сукоба која не укључује оружана непријатељства, постојање ратног сукоба. Даље, у одређењу сиве зоне, наглашавају се руске *активне мере* (необавештајне активности) против западних грађана, између осталих. У једном смислу, то је зона мира, с обзиром на одсуство рата. Али није мирно, утолико што је сукоб у току, укључујући и разне врсте војних (паравојних) акција. У извесном смислу, термин *сива зона* обухвата стару идеју: тражење предности без трошкова и ризика рата. Каталог активности руске сиве зоне је импресиван и алармантан. Укључује, на пример, *активне мере* (необавештајне активности) против циљева утицаја, са циљем убиства такозваних државних непријатеља, мешање у западне изборне процесе, стратегију информационе конфронтације, акције за замрзавање сукоба око његове периферије и (поновно) потврђивање утицаја у регионима под утицајем

САД. Москва и Пекинг очигледно желе да се регулишу регионални проблеми, корак по корак, али увек на начин који пада испод прага војног одговора од стране САД и/или њихових савезника. Ово је стратегија „скуване жабе" која настоји да избегне „кулминацијске тачке" и уместо тога се ослања на ометање и поделу унутар демократија ради промене чињеница на терену (Roberts, 2020).

Информациона операција по својој суштини и пореклу је војне природе, дефиниције информационих операција пре свега су присутне у војним и безбедносним доктринарним документима западних земаља. Информационе операције у САД подразумевају предузимање потеза да би се деловало на непријатељске информације и информационе системе (са намером да утиче на процесе који су засновани на информацијама, били они аутоматски или их водио човек), док се у исто време штите сопствене информације и информациони системи (Joint Publication 3–13, 2016). Теоретичари РФ дефинишу и користе појам *информациона дејства* (рус. *информационная война*) или *информациона борба* за сукоб у информационом простору. Таква дејства се спроводе информационо – техничким средствима (сајбер нападима и сл.) и информационо – перцептивним средствима, пропагандом, управљањем перцепцијом противника, обманом, дезинформисањем, психолошким операцијама (Timothy, 2019; Расторгуев & Литвиненко 2014). *Информационе операције* су радње које се предузимају ради постизања информационе супериорности у обезбеђивању националне војне стратегије утицајем на информационе и информатичке системе непријатеља уз јачање и заштиту сопствених информација и информационих система и инфраструктуре. Утицај током информационих операција се испољава на: „органе управљања државом и њеним оружаним снагама; информациони и контролни систем цивилне инфраструктуре (телекомуникације, укључујући масовне медије, транспорт, енергетски комплекс, финансијски и индустријски сектор); информационе и контролне елементе војне инфраструктуре (комуникације, обавештајне службе, борбену контролу, логистику, системе контроле наоружања); линије, комуникационе канале и пренос података; информације које круже или се чувају у контролним системима; друштво у целини (и цивилно становништво и особље оружаних снага), његове државне, економске и друштвене институције; масовне медије (првенствено електронске); менаџмент и особље аутоматизованих контролних система укључених у процес доношења одлука" (Макаренко, 2017, стр. 241). У овом истраживању је прихваћен термин *информационе операције* (Миљковић, 2016).

Сајбер напади су такође добро прилагођени као оруђе хибридне агресије (хибрид – третира сајбер и као средство и као домен претње). Не дешавају се у контекстуалном вакууму, тако да могу бити повезани (у извесној мери) са починиоцима (Monaghan, 2022). *Сајбер напади* су посебна врста информационе, субверзивне активности која нуди флексибилан алат за прикривено постизање низа циљева. У западним војскама кибернетичка средства се често схватају као посебно поље, док руска доктрина тежи да ову област третира као један елемент међу многима у оквиру ширег концепта информационих операција. *Сајбер напади* су се обично користили за класичне шпијунске операције, али такође може да се користи да допринесе различитим напорима за обликовање страног мишљења и поступака (Radin, Demus & Marcinek, 2020). *Сајбер напад* начелно представља акте агресије унутар сајбер простора или кроз сајбер простор на информациони систем другог ентитета. Он је облик војног дејства еквивалентан примени оружане силе, па се може предузимати и у офанзивном и у дефанзивном смислу. Сајбер напади су везани за сајбер простор. Кључни садржај сајбер

простора су подаци и информације у електронском облику, а фактор који га омогућава јесу информационо – телекомуникационе технологије (Младеновић, 2016; Путник, 2012). Дакле, сајбер напад је део или један од облика информационе операције.

2.2.2. Индикатори

У првом и другом истраживачком питању можемо констатовати да постоји један концепт одвраћања у САД, а други у РФ. Ови концепти утврђени су стратешко – доктринарним документима који услед брзог развоја информационих и телекомуникационих технологија врло често су доводили до промена у одвраћању што је неминовно захтевало измену докумената (стратегија, доктрина и др. докумената) и њихово ажурирање, ради прилагођавања новонасталим околностима. Тако су САД, од краја Хладног рата па до данас, донеле велики број стратегијских докумената који се на посредан и директан начин односе на одвраћање. Ради се о следећим документима: доктрине председника (1992, 2001, 2009, 2017, 2021), стратегије националне безбедности (1999, 2006, 2017), национална одбрамбена стратегија (2018), националне војне стратегије (1989, 1992, 1995, 2004, 2011, 2015, 2018). У истом периоду, РФ је усвојила следећа документа: стратегију националне безбедности (2009), војну доктрину (2010, 2014), Закон РФ о безбедности (1992, 1993, 2002, 2005, 2006, 2007, 2008). Конфронтација ове две силе уз избегавање директног оружаног сукоба изискује редефинисање постојећих стратегија, доктрина и других докумената који треба да пруже одговор о новом начину одвраћања. Повећана друштвена зависност од нових технологија, доводи до увећања претњи по безбедност држава новим формама, изворима претњи. Насиље неће бити ограничено, већ ће бити присутно свугде и на било којој тачки планете.

У трећем, четвртом и петом истраживачком питању, на основу истраживања промена које су настале од периода Хладног рата до сада, у погледу развоја информационих и телекомуникационих технологија, људског друштва и међународних односа, сагледано је како су ове промене утицале на начин одвраћања држава, организација, појединаца и описане су опште карактеристике савремених начина употребе служби безбедности. Службе безбедности су сагледане кроз необавештајне активности у зонама где су се догађале информационе операције и друге необавештајне активности, о чему сведочи велики број научних истраживања насталих на овим темама. Сагледана су општа, посебна и специфична обележја необавештајних активности и константна присутност (број, интензитет присутности) служби безбедности у спровођењу стратегија одвраћања, студија случаја информационих операција у Естонији, Криму и Украјини. Наведено нам даје одговор на питање каква је била улога служби безбедности у реализацији савременог концепта одвраћања, а каква је данас улога служби безбедности. Долазимо до закључка на који начин концепт одвраћања утиче на креирање безбедносне политике националних држава и на глобалну безбедност уопште. Велика активност офанзивних служби безбедности кроз пропагандне, политичке, економске и паравојне активности условила је промене у стратешко – доктринарним документима националних држава и дат је нови правац у одвраћању. Феномен садашњости и будућности, сајбер напад и сајбер простор диктирају и диригују промене у стратегијама и доводе до израде нових стратегија.

У (*Табели 1*) груписани су кључни индикатори који су коришћени у истраживању. Истраживање је фокусирано у две групе индикатора. Прву групу су чинили одвраћање у постхладноратовском периоду, које је истраживано кроз идентификацију стратегијских

докумената који регулишу одвраћање, и промене које доводе до нових концепата у одвраћању, као и поступци, па и промене делова система безбедности услед развоја нових технологија и билатералних односа држава након интервенција служби безбедности. Другу групу индикатора су чиниле активности служби безбедности у одвраћању, посматране кроз политичке, пропагандне, паравојне, економске као и информационе активности (операције). Поред табеларно приказаних извора података, у овом научном истраживању је коришћен и велики број научних истраживања насталих у овој области, као и горе наведених других база података (обрађено у наредном поглављу).

Табела 1. Табеларни приказ посматраних кључних индикатора коришћених у истраживању.

ЗАВИСНА ВАРИЈАБЛА		**ОПЕРАЦИОНАЛИЗАЦИЈА**	**ИЗВОР ПОДАТАКА**
ОДВРАЋАЊЕ У ПОСТХЛАДНОРАТОВСКОМ ПЕРИОДУ	Промена стратегијских докумената	Идентификација докумената која прописују одвраћање на стратегијском нивоу у САД и РФ, број, врста докумената која регулишу одвраћање и установљавање сегмената у њима који прописују одвраћање и на који начин. Компарацијом ових сегмената, насталих после Хладног рата до данас констатовати које су то промене у концептима одвраћања САД и РФ.	*defense.gov* *usa.gov* *army.mil* *fas.org* *agentura.ru* *government.ru* *mil.ru*
	Поступци делова система безбедности	Услед повећане друштвене зависности од нових технологија, долази до увећања претњи по безбедност држава новим формама, изворима претњи што условљава трансформације служби безбедности (као и др. целина система безбедности) и нове начине примене различитих концепата одвраћања у САД и РФ. Стварање/оспособљавање организација, агенција, институција за предузимање необавештајних активности и регистровање нових обележја у активностима државе у одвраћању, првенствено активности служби безбедности. Сагледавање ефикасности државних институција у одвраћању.	*carnegieendowment.org* *ohchr.org* *connections–qj.org* *cia.gov* *nps.edu* *nps.primo* *roe.ru* *fsb.ru* *svr.gov.ru*

ЗАВИСНА ВАРИЈАБЛА		ОПЕРАЦИОНАЛИЗАЦИЈА	ИЗВОР ПОДАТАКА
	Билатерални односи држава након интервенција	Врста и број докумената насталих између државе која интервенише и државе где ће бити испољене необавештајне активности. Интензитет остварених притисака политичара државе која интервенише према политичарима нападајуће државе. Колико пута је ангажовање у необавештајним активностима било противно међународном праву. Интензитет политичких, дипломатских веза између државе која интервенише и државе према којој ће бити испољена необавештајна активност.	*mid.ru* *fam.state.gov* *fas.org* *usa.gov* *rsf.org* *cia.gov* *government.ru* *svr.gov.ru* *privacyinternacional.org* *un.org*
	Промене настале развојем нових технологија	Број нових система наоружања и војне опреме (хиперсоничне ракете, авиони, дронови, ПВО системи и др.) до каквих промена је довело. Промене регистроване од периода Хладног рата па све до сада, у погледу развоја нових технологија, дипломатских односа, људског друштва, покушаћемо да констатујемо како су оне утицале на начин одвраћања држава, организација, лица (правних и физичких) и да опишемо опште карактеристике савремених начина употребе служби безбедности. Службе безбедности би сагледали кроз необавештајне активности у зонама где су се догађале информационе операције и друге необавештајне активности у тзв. *сивој зони*.	*rand.org* *defense.gov* *csis.org* *nps.edu* *nsa.gov* *dcsa.mil* *agentura.ru* *roe.ru* *soldat.ru* *rusarmy.com*

НЕЗАВИСНА ВАРИЈАБЛА		ОПЕРАЦИОНАЛИЗАЦИЈА	ИЗВОР ПОДАТАКА
АКТИВНОСТИ СЛУЖБИ БЕЗБЕДНОСТИ У ОДВРАЋАЊУ	Политичке активности	На који начин се користе политичке активности у држави и иностранству ради обезбеђења адекватне употребе силе од служби безбедности. Интензитет остварених притисака политичара према политичарима нападајуће државе, организације, групе, лица (правног, физичког). У којој мери је у овим активностима присутно (не)поштовање људских права. Утицај одвраћања на креирање безбедносне политике у будућности.	*nature.com* *state.gov* *nps.primo* *carnegieendowment.org* *neweurope.org.ua* *politico.com* *rsf.org* *government.ru* *mid.ru* *fam.state.gov*
	Пропагандне активности	Степен учесталости употребе дезинформација ради отпочињања или правдања одређене интервенције према некој држави, организацији, групи, лицу (правном или физичком). Број започетих интервенција, војних или невојних, које су правдане на основу пласираних дезинформација.	*state.gov* *bbc.com* *nps.primo* *connections–qj.org* *cia.gov* *svr.gov.ru* *soldat.ru*
	Економске активности	Штета нанета интервенцијом од стране интервенишуће државе. Интензитет условљавања економским уступцима. Сагледати до интервенције државе, интензитет економске сарадње. Количина економске размене, након интервенције. Број изазваних криза, затим дестабилизација. Трошак који је наступио услед економских активности од интервенишуће државе, а ради *јачег утицаја* на циљну државу, организацију, групу, лице (правно, физичко). Присуство САД пре и после интервенције у трговини наоружањем тамо где је испољена њена интервенција (активност).	*rand.org* *neweurope.org.ua* *carnegieendowment.org* *connections–qj.org* *lse.ac.uk*

НЕЗАВИСНА ВАРИЈАБЛА		ОПЕРАЦИОНАЛИЗАЦИЈА	ИЗВОР ПОДАТАКА
	Паравојне активности	Број активног учешћа регуларних припадника оружаних снага агресора на територији друге суверене државе ради *јачег утицаја* на лице, групу, организацију, државу. Број жртава наступио услед предузимања паравојне активности као и настале последице након паравојне активности. Трајање активности и директни трошкови (пара) војних интервенција у доларима с тим да уз наведено је неопходно и да буде присутно да на ове трошкове треба додати и ангажовање, трошкове служби безбедности. Жртве настале оваквим интервенцијама, војне и цивилне.	*war–memorial.net/ /index.asp* *ucdp.uu.se* *ap.ohchr.org* *nps.primo* *cia.gov* *svr.gov.ru* *soldat.ru* *rusarmy.com* Годишњи буџет САД. Извештаји владиних и невладиних организација.
	Информационе операције	Број активних учествовања техничких средстава на територији друге државе ради испољавања *јачег утицаја* на одвраћање. Број сајбер напада упућених према држави, организацији, групи, лицу (правном или физичком) ради остваривања одвраћања. Трајање сајбер напада на институције у једној држави или друге ентитете. Установљавање критичних објеката на које се врше сајбер напади. Интензитет развоја нових технологија и њихов утицај на одвраћање као и регистровања нових обележја необавештајних активности услед техничко – технолошког развоја, кроз студије случаја информационих операција у Естонији, Криму и Украјини. Идентификација посебности *сиве зоне* са свим својим карактеристикама.	*citizenlab.ca* *csis.org* *nps.primo* *ohchr.org* *carnegieendowment.org* *politico.com* *bbc.com* *nsa.gov* *dia.mil* *disa.mil* *dcsa.mil* *dodcio.defense.gov* *fsb.ru* *neweurope.org.ua* *sbu.gov.ua* *mbo.gov.ua* *valisluureamet.ee* *rand.org*

Извор: Аутор.

2.3. ТИП И МЕТОД ИСТРАЖИВАЊА

Избор метода одређен је проблемом истраживања, теоријским и операционализованим предметом истраживања као и истраживачким питањима. Поред наведеног, сложеност предмета истраживања утиче на избор метода.

Истраживање овог типа захтева коришћење већег броја метода и врло опрезну и селективну анализу доступних релевантних извора података. Комплексност овог феномена је наметнула мултиметодски приступ.

Ради се о доминантно квалитативном истраживачком приступу. Недовољна теоријска изграђеност као и усклађеност је довела до претежно експлораторне природе успостављених истраживачких захтева.

Стратегије одвраћања, необавештајне активности служби безбедности и информационе операције као један од феномена рада савремених служби безбедности јесу изузетно комплексне области за истраживање. Наведени облик деловања је врло сложен за изучавање, те је неопходно користити различите истраживачке методе и теоријска знања из више научних дисциплина.

2.4. ВРЕМЕНСКО – ПРОСТОРНИ ОКВИР ИСТРАЖИВАЊА И ИЗВОРИ ПОДАТАКА

Предмет истраживања се односио на *простор* испољеног деловања служби безбедности (велики број држава, јер се деловање првенствено односи на активности у иностранству, не само у САД и РФ) и других државних органа (дипломата, дела политичара као и другог особља укљученог у спровођење ових активности) током планирања и реализације необавештајних активности и информационих операција у обављању својих редовних задатака у остваривању интереса државе кроз међународне односе, тако да је истраживање лимитирано на простор где се налазе САД, РФ, Естонија, Крим и Украјина.

Временски оквир предмета истраживања се односио на период после Хладног рата па до данас. Проблем истраживања спада у домен научних дисциплина наука безбедности, политикологије, међународних односа, права и др.

Извори података који су коришћени у овом истраживању су разноврсни, превасходно због специфичности и комплексности предмета истраживања. Следећи извори података (поред оних приказаних у *Табели 1*) су послужили за истраживање:

- велики број научних резултата и стручних радова који су се бавили истраживањем необавештајне активности, односно радом служби безбедности;
- позитивноправни прописи (међународни, национални);
- искуствена грађа стварана за потребе претходних истраживања (која се може секундарно анализирати);
- међународни документи, споразуми и др., који су директно или индиректно везани за необавештајне активности служби безбедности;
- евиденције државних и међународних тела која се баве праћењем и анализом безбедносних питања на глобалном плану;
- једна од „база података у академским истраживањима оружаних сукоба јесте *Correlates of War– Non–, Intra–, Inter–, Extra – State Wars* (Корелати рата – недржавни, унутардржавни, међудржавни и вандржавни ратови" (Стојановић Такић, 2022, стр. 28);

- једна од најобухватнијих каталогизација база података представљена је у публикацији *Индикатори и индекси сукоба и безбедности*: *преглед и класификација отворених база података*, у којој су Павловићева и сарадници из Агенције за истраживање и развој у области одбране (*Recherche et développement pour la défense Canada*) канадског Министарства националне одбране, пружили свеобухватан списак са детаљним описима 126 база података о сукобима и безбедности, које су разврстали у 16 категорија" (Стојановић Такић, 2022, стр. 28);
- један од каталога је и Каталог база података за истраживања у области безбедности, Факултет безбедности, Димитријевић и Параушић, 2017. и др. базе података).

Основу су чинили извори података везани за предмет истраживања, али и интернет (као све значајнији извор секундарних података). То су страна и домаћа документа, стручни и уско специјализовани радови домаћих и страних аутора, доступна документа и извештаји. Извори података су и експерти.

2.5. ТЕХНИКЕ ЗА ПРИКУПЉАЊЕ ПОДАТАКА

Ради поштовања основних епистемолошких принципа, пре свега прецизности и поузданости, ово истраживање је обухватило како анализу различитих извора података, тако и интердисциплинарно коришћење различитих истраживачких метода и то:

- анализа правних докумената;
- метод секундарне анализе;
- метод анализе садржаја;
- компаративна метода;
- метод студије случаја.

Анализа правних докумената

Анализа правних докумената у овом истраживању је била правно – догматска. На овај начин је спроведено тумачење правних норми у циљу разумевања значења симбола којима су оне изражене. Правне науке примењују овај метод, а у овом истраживању су упоредно анализирани позитивноправни прописи којима се уређује ова област. Нормативна акта која су анализирана у овом истраживању односила су се првенствено на иностранo законодавство, пре свега на нормативу САД и РФ. За потребе истраживања, САД и РФ су узете као пример држава које најинтензивније примењују необавештајне активности и информационе операције у реализацији својих или савезничких спољнополитичких циљева и те активности се више не третирају као тајне.

Метод секундарне анализе

Велики број истраживачких радова и докумената који су настали из разних потреба су искоришћени као извори података о теми која је истраживана. Ради се о специфичној области, а секундарну анализу података неопходно је било спровести да би на тај начин била анализирана доступна грађа из досад спроведених научних истраживања у области необавештајних активности. Поред тога, кроз употребу метода секундарне анализе су

проучаване и доступне евиденције релевантних цивилних и војних институција, различити јавно доступни извештаји, текстови из новина и др. што би довело до бољег појмовног и класификационог одређења необавештајног деловања служби безбедности. Посебно је значајна и због немогућности спровођења истраживања у којем би учесници били актери неких од необавештајних активности. Овде се као проблем могла појавити веродостојност података који се анализирају, што је захтевало посебну обазривост приликом одабира извора података. Уз ову констатацију било је потребно редовно вредновати и оцењивати квалитет доступних корпуса знања који су одабрани за секундарну анализу.

Метод анализе садржаја

Сви јавно доступни садржаји, садржаји медија и комуникације за широку употребу, сагледани су методом анализе садржаја које емитују масовни медији. Сва сазнања добијена у истраживању су сакупљана систематично, а преко различитих медијских садржаја (интернет сајтови, ТВ емисије, филмови, снимци, друштвене мреже, новине, часописи и сл.).

Компаративна метода

Компаративна метода (поређење) је примењена у овом истраживању, јер без ње није могућ ниједан облик закључивања. Применом компаративне методе је вршено доказивање или одбацивање претпоставки о одређењу појма одвраћање у највишим стратешко – доктринарним документима где су сагледаване доктрине председника, стратегије националне безбедности, одбрамбене стратегије, војне доктрине и други документи уз сагледавање одређених појава и тражења њихових сличности или супротности. Применом ове методе у истраживању идентификоване су сличности и разлике између активности које примењују службе безбедности Запада и Истока. Ова метода је примењена приликом упоређивања истих чинилаца (политичких, економских, пропагандних, паравојних и других). У циљу свеобухватног сагледавања предмета истраживања, овај метод је омогућио проверу и допуну података добијених разноврсним методским приступима, што умањује пропусте примене других метода. Компарацијом обавештајних, контраобавештајних и необавештајних активности служби безбедности великих сила идентификоване су разлике и сличности у раду и предузимању делатности на одвраћању. Кроз детаљно поређење стратешко – доктринарних докумената, сагледано је појмовно одређење модерног наоружања и војне опреме, врсте, тип и констатоване сличности и разлике, као и евентуално испољен утицај на одвраћање његовим истицањем.

Метод студије случаја

Студија случаја се на „најопштијем нивоу одређује као дубинско проучавање једног или више одабраних случајева, односно примера, који се у односу на истраживачки дизајн сматра адекватним. Адекватност одабране студије је нужан предуслов уопштавања добијених налаза и извучених закључака" (Стојановић Такић, 2022, стр. 32). Студијом случаја је обухваћен конкретан проблем/случај, као што су информационе операције у Естонији, Криму, Украјини и сличне необавештајне активности. Ова метода је погодна за

истраживање оних појава које до момента истраживања нису биле довољно сагледаване као предмет научног истраживања. Ради се управо о таквим појавама, необавештајним активностима и информационим операцијама служби безбедности што се може делимично оправдати вишедеценијским сакривањем. Тема овог истраживања је необавештајна активност служби безбедности у одвраћању. На основу ранијих студија случаја може се закључити колико су необавештајне активности генерално коришћене и у којој мери од стране САД и РФ у склопу нових облика политичке, економске, пропагандне и паравојне активности ради остварења националних интереса. Један од случајева, који припада новијем међународном сукобу у којима је учествовала РФ, представља сајбер напад у Естонији 2007. године. Руске власти су такође званично признале да су умешане у овај сукоб. Ово истраживање тако испуњава два неопходна услова за студије случаја. Прво, главно истраживачко питање је типично питање „како" су руске власти користиле сајбер напад у реализацији националних, државних интереса (којим средствима и којим методама). Друго, пронађено је и више догађаја у којима су руске власти примениле активности које спадају у домен необавештајне активности: руска анексија Крима, 2014. године, утицај на америчке председничке изборе 2016. године итд. С обзиром на чињеницу да су се ови сукоби догодили у блиској прошлости и да су сагледаване активности служби безбедности које су део предмета истраживања, овде препознајемо оригиналност у догађајима. Једна од најактуелнијих тема је управо савремене акције служби безбедности у сајбер простору и необавештајне активности које спроводе. Необавештајне активности и сајбер напад су по својој специфичности јединствени. Ове јединствености могу бити констатоване у времену и простору као активности које су се дешавале у друштву како у блиској прошлости, тако и данас, са великом вероватноћом да ће се дешавати и у блиској будућности. У том смислу, ова метода је коришћена за истраживање и сагледавање јединствености примене необавештајних активности у раду служби безбедности. За ово истраживање су анализиране конкретне акције, као и студије које могу бити репрезентативне за истраживање јединствености активности служби безбедности у необавештајним активностима примењене у пракси и обрађене у теорији (необавештајној, обавештајној и контраобавештајној активности служби безбедности). Јединственост анализираних случајева у истраживању се огледала у генерализацији, јер су изучавани случајеви који су слични у примени метода рада служби безбедности. Јединственост је сагледавана кроз постављене циљеве, методе које су примењене у акцијама које су извођене, начин реализације, ангажоване снаге и средства у припреми и реализацији акција, место и улога дипломатије и политике у припреми и реализацији акција, које су активности пратиле реализацију акција, простор, условљеност временом у смислу: годишње доба, метео услови, доба дана и ноћи, трајање акције, структура ангажована у акцији, примењени начин спровођења акције, резултати на терену (у пракси), као и друге специфичности и обележја овог типа активности.

2.6. НАУЧНИ ДОПРИНОС ИСТРАЖИВАЊА

Предложена тема је недовољно обрађивана у домаћој научној литератури, а на различите и методолошки неуједначене начине тематизована у страној научној литератури, што овако постављено истраживање чини јединственим. Осим тога, реализацијом планираног истраживања проширен је фонд постојећих и стечена су нова сазнања о концептима одвраћања у стратешко – доктринарним документима великих сила, као и о

деловању служби безбедности и других елемената државног апарата, али и о аспектима необавештајне активности (укључујући и информационе операције) у савременим околностима развијених технологија, друштвене међуповезаности и других услова који доводе до прилагођавања необавештајне активности савременим условима. Такође, опис одвраћања у стратешко – доктринарним документима великих сила у периоду након Хладног рата и објашњење улоге служби безбедности у њиховој реализацији је допринело да овај истраживачки рад буде јединствен. Истраживање је наговестило будуће видове одвраћања сходно примењиваним необавештајним активностима како би довело до правовремене превенције у будућим активностима и нормативно кориговање докумената који регулишу ову област.

Истраживање је, осим претходно наведеног, допринело и појашњењу појмовне и терминолошке суштине ове специфичне области. Различита употреба наизглед сличних или истих појмова, затим употреба појма необавештајне активности који указује на нови концепт у одвраћању који није само дефанзивни, већ има и офанзивне елементе, добија ново значење, те је сада потпуно познато да ли се необавештајне активности односе само на концепт или и на неки нови тип одвраћања, претњу или све то скупа. Када су присутне теоријске нејасноће, проучавање феномена необавештајних активности захтева темељан приступ који се усредсређује како на домаће, тако и на стране изворе научног сазнања. Научно проучавање феномена необавештајне активности представљало је прикладан оквир за испитивање природе проблема необавештајних активности и информационих операција, као и добру прилику за процену и измену постојећих концептуалних оквира у разматрању необавештајних активности и информационих операција као савремених безбедносних феномена.

3. КОНЦЕПТ ОДВРАЋАЊА У СТРАТЕГИЈСКО – ДОКТРИНАРНИМ ДОКУМЕНТИМА ВЕЛИКИХ СИЛА НАКОН ХЛАДНОГ РАТА

У овом поглављу, представљен је теоријски оквир на ком је базирано даље истраживање, које обухвата одвраћање као концепт великих сила и друге кључне појмове везане за необавештајне активности служби безбедности у постхладноратовском периоду. Када говоримо о службама безбедности, говоримо о специјализованим организацијама које се баве обавештајним, контраобавештајним, безбедносним и необавештајним активностима. Необавештајне активности служби безбедности (познате и као *тајне акције, тиха опција, трећа опција, специјална политичка акција, активна мера* итд.) у смислу овог истраживања сагледавамо првенствено кроз конкретне активности служби безбедности у политичким, пропагандним, економским и паравојним активностима које се користе ради одвраћања других држава. Теоријски домен овог истраживања је базиран на објашњењу употребе служби безбедности, односно примене силе и моћи у међународним односима, како би се приморала друга држава (или неки други ентитет или појединац) на поступање у складу са намером матичне државе. Након приказа научних дебата о концептима одвраћања великих сила, истраживачко тежиште је усмерено на образлагање коришћења служби безбедности у међународним односима и њихових активности на којима се заснива одвраћање.

3.1. КОНЦЕПТ ОДВРАЋАЊА СЈЕДИЊЕНИХ АМЕРИЧКИХ ДРЖАВА

3.1.1. Теорија одвраћања

Према *Речнику војних и њима сродних израза* оружаних снага САД, одвраћање има следеће значење: „спречавање деловања постојањем веродостојне претње од неприхватљивог противљења и/или уверење да су трошкови акције већи од перципиране користи". У поменутом речнику је одвраћање (енг. *deterrence*) стављено у исту раван са термином стратешког ефекта када се дефинишу задаци и мисије (одвраћање, стабилизација, итд.), где је „листа појмова стратешког ефекта: унапредити, осигурати, присилити, такмичити се, приморати, садржати, обманути, поразити, деградирати, одложити, делегитимизирати, порећи, уништити, одвратити, дискредитовати, онемогућити, обесхрабрити, пореметити, преусмерити, ангажовати, побољшати, интегрисати, изоловати, убити, одржавати, управљати, неутралисати, спречити, заштитити, стабилизовати, потиснути, синхронизовати" (Department of Defense Dictionary of Military and Associated Terms, 2021, p. 2, 63).

Одвраћање које постоји више од три четвртине века је еволуирало заједно са променама стратешких услова за решавање претњи. Када се говори о одвраћању, тада морамо поменути неколико теоретичара.

Шелинг (*Thomas Schelling*) као један од првих теоретичара који је одредио значење овог термина, исти види као спречавање или обесхрабривање од деловања путем страха, сумње или слично. Такође, одвраћање види и као скретање у страну или обесхрабривање путем страха, чиме долазимо до спречавања акције страхујући од последица. Одвраћање је било у популарној употреби не само у војној стратегији већ и у кривичном праву. Одвраћање је пасивно, представља одговор на нешто неприхватљиво, где у миру представља одсуство провокације. То је нешто попут „одбране" за разлику од „увреде". Шелинг пореди наведено са називом Министарства одбране, а не Ратно одељење, а „одбрана" описује мирољубиву страну војне акције (Schelling, 2008). Тако је Шелинг, у књизи *Оружје и утицај* описао да су Американци традиционално на рат гледали као на алтернативу дипломатији, а на војну стратегију као на науку о победи. Шелинг даље каже да је преговарачка моћ и искоришћавање те моћи, за добро или зло, ради очувања мира или претње рату, дипломатија, и то дипломатија насиља. У овој књизи Шелинг се концентрише на начин на који се војна моћ – стварна или измишљена – користи, вешто или неспретно, као преговарачка моћ за одвраћање. Извештаје сопствених војних служби безбедности о противнику, аутор види као најважнију дипломатску комуникацију (Schelling, 2008).

Мазар (*Michael Mazarr*) одвраћање види као поступак обесхрабривања или обуздавања некога у међународној политици. Најчешће се ради о националној држави, где се наведена активност предузима како би се иста обуздала од нежељених акција. Када се помињу нежељене акције, тада најчешће мислимо на оружану агресију, оружани напад. Представља напор да се заустави или спречи наведена радња. Одвраћање држава да предузимају нежељене акције, посебно оружану агресију, иако већ дуго присутно у америчкој одбрамбеној политици, поново је постало главна тема у америчкој одбрамбеној политици. Ово се првенствено односи на политички дијалог о одвраћању који карактеришу врло често неутемељене тврдње, тврдње које су у супротности са емпиријом и мало упућује на квалитетне анализе. Одвраћање мора бити замишљено као напор да се обликује мишљење о потенцијалном агресору. Свака стратегија за спречавање агресије мора почети са проценом

интереса и мотива потенцијала агресора, укључујући и његову теорију одвраћања. Одвраћање је много више од обичног претећег тона упућеног потенцијалном непријатељу – противнику тј. захтева нијансирано прилагођавање перцепција, па у тим варијантама непријатељ – противник види алтернативу агресији као атрактивнију од самог рата. Мазар кроз синтезу одвраћања нуди концепт који је импресиван и својом свеобухватношћу и својом краткоћом. Одвраћање представља обесхрабривање или обуздавање некога – у светској политици, обично националне државе – од предузимања нежељених радњи, као што је оружани напад или други вид насиља. Укључује напор да се заустави или спречи нека радња, што је покушај да се актер примора на наше захтеве (Mazarr, 2018). Према Мазару, три су основна услова за успех у одвраћању: први, ниво мотивације агресора, затим други, колика је јасноћа о предмету одвраћања и акцијама које ће бранилац предузети и трећи, да агресор мора бити уверен да држава која врши одвраћање има способност и вољу да изврши претње. Када се говори о нивоу мотивације агресора, за успех или неуспех одвраћања, тада кажемо да ако претње одвраћања буду констатоване као општа политика непријатељства, они могу изгубити способност да буду примењени за одвраћање конкретне радње. Јасноћа о предмету одвраћања и акцијама које ће бранилац предузети можемо да сврстамо у други услов за успех одвраћања када бранилац треба да на што је могуће јаснији начин презентује шта покушава да одврати, као и шта ће урадити ако се претња игнорише. Трећи услов је да агресор мора бити уверен да држава која врши одвраћање има способност и вољу да изврши упућене претње с тим што у овом услову морамо нагласити да је он у ствари чисто перцептивне природе, јер није у питању да ли бранилац заправо има такве способности или вољу, већ да ли агресор верује да јесте. Мазар је разматрајући улогу одвраћања у стратегији националне безбедности САД констатовао три фактора која утичу на одвраћање: први, да се спречавање агресије не своди само на присилу, претње већ и на нуђење уверавања, а одвраћа се потенцијални агресор како би увидео потребу или прилику за агресију; други фактор су перцепције које САД морају да посматрају кроз уверења и предубеђења потенцијалног агресора; и трећи фактор, који укључује комбинацију хватања озбиљности агресорове мотивације, јасноће шта бранилац жели да одврати и шта ће учинити ако претња буде оспорена као и шта ће предузети, које кораке, да се испуни претња. Мазар закључује да је у случајевима после Другог светског рата, где су САД испуниле ова три критеријума, генерално постигнут успех у одвраћању (Mazarr, 2018). Посебно је на одвраћање утицало повећање и одржавање војне моћи у циљу обесхрабривања непријатеља – противника од неког утицаја или напада. Нуклеарно оружје у војном развоју водећих држава је довело до многих промена. Перцепција да неко може потпуно да уништи (државу или више држава) непријатеља са једном или неколико ракета за масовно уништење је довела до тога да су државе почеле да то узимају у обзир као један од кључних параметара у процени својих непријатеља односно њихових савезника. Само сазнање о постојању толике количине нуклеарног потенцијала код неке државе из корена мења процену о предузимању било каквог акта агресије према таквој држави или њиховим савезницима.

Да бисмо разумели и правилно проценили како ће САД одвратити евентуалну руску агресију, неопходно је основно схватање одвраћања. Многи уважени теоретичари пружају широк теоријски оквир одвраћања неопходног за ово истраживање. Посебно је важна литература која узима у обзир веродостојност одвраћања претње које су руске акције довеле

у питање, док нису за занемаривање ни аутори који су са историјског аспекта сагледавали разумевање теорије одвраћања.

Базан и Хансен (*Barry Buzan & Lene Hansen*) се у књизи *Еволуција међународних студија безбедности* фокусирају на рат и војску, политичке, технолошке и стратешке аспекте ривалства великих сила. Једна од тема књиге је како је нуклеарно оружје утицало на ривалство између САД и Совјетског Савеза и стратегију одвраћања. Док је постојао општи договор да је друга сила непријатељ САД и такозване слободе у свету, водиле су се расправе о међусобној интеракцији технологије и непријатељства које је имало утицаја како на хладноратовска такмичења стратешких студија, тако и на постхладноратовске расправе о улогама државе и војне технологије. Са својим језгром усредсређеним на игру теорија и нуклеарно одвраћање, па због експлицитне везе са јавном политиком, биполарност је такође издашно финансирана годинама. До краја хладног рата биполарност је изгледала као опште кадрирање за готово све стратешке теоретизације, па било да се ради о теорији одвраћања, тркама у наоружању, контроли наоружања или савезима, основна претпоставка стратешких студија хладног рата је била биполарност. Ова претпоставка је изузетно истакнута у теорији одвраћања. Оснивач неореалистичке теорије, Валц (*Waltz*), на пример, сматрао је да је Совјетски Савез заузео став пасивног одвраћања према САД, са којим сасвим разумно не жели да се бори. Такође, у истраживању констатује да је питање да ли су Совјети разумели концепте као што је одвраћање на исти начин као теоретичари са запада, односно каква је разлика између руске војске и америчке, као и култура, традиција и др. Греј даље износи да је руски национални политички карактер обележен лукавством, бруталношћу и покорношћу, и да је совјетска стратешка култура у корену руска, а не марксистичко – лењинистичка. За одвраћање су Совјети имали да понуде као контра – претњу само своју конвенционалну војну супериорност и нуклеарне претње у Европи. Покретањем *Спутњик* програма 1957. године све се променило, демонстрирајући да је Совјетски Савез савладао ракетне технологије које би омогућиле да брзо нападну САД, где су до тада претње биле углавном нуклеарним америчким снагама заснованим на бомбардерима. Крајем 1950. године па надаље, све више је јачало међусобно нуклеарно одвраћање Совјетског Савеза и САД нуклеарном паритету суперсила. Велике несигурности нису уведене само услед технолошког развоја, већ и погрешним информацијама – дезинформацијама о томе ко је имао и шта распоредити од оружја. *Једни* су мислили да нуклеарно оружје олакшава одвраћање. Другим речима, поседовање нуклеарног арсенала довољног за *сигурно уништавање* у основи би било довољно да доведе до такозване стратегије *минималног одвраћања*. *Други*, узимајући приступ *максималног одвраћања*, срачунато на безобзирног актера (као што је Кенан претпостављао да је Совјетски Савез) то не би захтевало само претњу од велике штете, већ и скоро извесну вероватноћу да би таква одмазда била извршена пре него што би одвраћање могло да буде ефикасно. Логика би могла налагати да је одмазда након удара била ирационалан чин, отварајући тако прилику безобзирном агресору да размисли о нападу на првом месту. Теорија одвраћања постала је прича о успеху у овом контексту из два разлога. С једне стране, произвела је наизглед продуктивност тј. „прогресивни" истраживачки програм, док је са друге стране све ово изгледало веома корисно, јер су теорије у ствари произвеле сопствену стварност апстракција, свет *сигурне друге могућности удара*, *продуженог одвраћања* и *доминацију ескалације*. Када је сам хладни рат почео да се повлачи, повукао је за собом и расправе о осећају хитности који је био везан за теорију одвраћања, политику задржавања и

проширено одвраћање, и чак и велики део страха од нуклеарног оружја. Окончање хладног рата није однело трајни поступак заокупљеност новим војним технологијама, а није уклоњена ни забринутост због нуклеарног оружја (Buzan & Hansen, 2009).

Следећи теоретичар који се бавио одвраћањем је Кнопф (*Jeffrey W. Knopf*) који прави разлику између четири таласа у истраживању одвраћања. Први талас одвраћања у теорији појавио се након Другог светског рата, ради неопходности одговора на проналазак атомске бомбе. Други талас дошао је 1950/1960. и у њему су доминирале формалне теореме које су произашле из дедуктивног закључивања. Трећи талас 1960/1970. користио је статистичке методе и методе студије случаја за емпиријско тестирање теорије одвраћања. Допуњена је перспектива рационалног актера са перспективама из психолошке литературе и литературе о одлучивању. Последњи талас, након завршетка Хладног рата, појавио се након 11/09 и ставио фокус на асиметрично одвраћање. Основни концепти и претпоставке које се тичу улоге кредибилитета и угледа биле су поново процењиване у светлу стварних случајева одвраћања између западних држава и њихових политичких непослушника у неколико држава (Knopf, 2010).

Вирц (*James Wirtz*) је у својој књизи *Разумевање неуспеха обавештајних података Упозорење, одговор и одвраћање* изнео како различите перцепције претњи могу довести до напада стратешког изненађења, неуспеха служби безбедности и неуспеха одвраћања. Наглашава се стратешки поглед на питања изненађења и непостојања обавештајних података. Објашњава подстицаје и перцепције обе стране када постоје значајне неравнотеже војне моћи између потенцијалних бораца. Нападима које су покренули недржавни актери, и нудећи поређење између Перл Харбора и напада 11. септембра 2001. године, аутор истражује феномен неуспеха у одвраћању, конкретно, како слабије стране у сукобу верују да ће претње одвраћања војно јачих антагониста бити поткопане разним ограничењима, повећавајући привлачност коришћења изненадних напада за постизање њихових циљева. Ово истраживање такође нуди стратегије које могу ублажити појаву непостојања обавештајних података, стратешко изненађење и неуспех у одвраћању (Wirtz, 2017).

Крепиневич (*Krepinevich*) у својој књизи *Пад одвраћања* наводи да се од краја Другог светског рата САД ослањају на одвраћање као на централно место у својој одбрамбеној стратегији. Наведено као акцентовано траје и у Стратегији националне безбедности и Стратегији националне одбране Трампове администрације. Кроз ову студију констатоваћемо да се стратешко окружење у којем одвраћање функционише, променило из корена и наставља да се мења; трансформација и даље траје. Одвраћање укључује напоре да се противник (мета) спречи да предузме забрањену активност. Они који користе одвраћање настоје да утичу на циљни прорачун трошкова, користи и ризика повезаних са спровођењем забрањене активности. Начин да се смањи америчка несигурност у погледу ефикасности нових способности је спровођење што реалнијих вежби на свим нивоима. Мада вежбе никада нису у могућности да замене рат, уз високе реалне услове такве вежбе могу значајно побољшати разумевање потенцијалне ефикасности различитих војних доктрина, структура снага и способности. Ово може помоћи у смањењу различитих погледа на војну равнотежу и на тај начин повећати ефикасност стратегија одвраћања (Krepinevich, 2019).

Фридман (*Lawrence Freedman*) у свом истраживању *Уоквиривање стратешког одвраћања* износи како је током хладног рата одвраћање деловало боље у пракси него у теорији. Процена је постојала да рат великих сила није био практично замислив због

последица које је носила таква једна активност. Међутим, када говоримо о овим и сличним проценама до њих се долазило без реално изведених вежби, односно сценарија. Већ дужи низ година у свету постоји све више мањих арсенала моћи и пролиферације малих арсенала; можда се данас и удаљавамо од оног модела који су нам били одличан пример како одвратити непријатеља. То је најбоље регистровано током Хладног рата. Фридман испитује претпоставке које су биле упориште у стратешком одвраћању и баца поглед на двосмисленију нуклеарну будућност (Freedman, 2009).

Морган (*Morgan M. Patrick*) је написао велики број радова на тему одвраћања (*Одвраћање сада; Стање одвраћања у међународној политици данас; Одвраћање: концептуална анализа* и др.) где је током истраживања констатовао следеће стање по питању одвраћања, за период после Хладног рата. Морган запажа, да се сагледавајући систем и даље могу приказати неки трагови Хладног рата. Морган је трагове видео у следећем: „конкурентни су напори служби безбедности великих сила, у истом смеру; кључне су могућности нуклеарног наоружања великих сила, упркос одсуству политичког сукоба који их чине виталним или чак корисним; нуклеарне снаге у основи су конфигурисане какве су биле, али у мањем обиму, са новим оружјем које се још увек појављује, а постојеће се побољшава; нуклеарне снаге одржаване имајући на уму исте снаге бивших противника, упркос томе што је још теже замислити да их користимо; главна глобална политичка линија кривице остала је Москва и Пекинг у односу на Запад по многим питањима, што још увек кочи ефикасност Савета безбедности; амерички савези остају, са више чланова, као и мрежа Американаца, војне базе су нетакнуте, а америчке снаге су распоређене на многим местима где су били плус нове локације; америчке конвенционалне снаге су и даље значајне, неке друге велике силе одржавају прилично велике снаге, трговина оружјем је и даље снажна; америчко продужено одвраћање и даље је широко распрострањено, делимично засновано на истој моћи, ресурси за пројекцију базе, комуникација, одржавања и сродних објеката” (Morgan, 2012, p. 89). Морган је покушао да сагледа одвраћање, у теорији и пракси, и да види како би могло да се поступа у пословима безбедности (Morgan, 2012). Морган је приметио кооперативну природу односа између водећих сила и да су ослобођене дубоких безбедносних забринутости. Поред нуклеарног оружја, истовремено, главне преостале претње, према Моргану, биле су од пропалих, слабих и одметнутих држава поред недржавних актера. Одвраћање је постало више од тактичког ресурса (Morgan, 2012). На одвраћање су утицали и други развоји, како технолошки тако и идеолошки. Повећана прецизност у стратешком оружју с једне стране, и размештање интерконтиненталних балистичких ракета (енг. *intercontinental ballistic missiles*) са конвенционалним бојевим главама, а с друге стране, појава стратешког сајбер напада/способности, представљао је значајан изазов за ново одвраћање. Морган је приметио и да је знатан напредак у размишљању о улози одвраћања у борби против тероризма где је све веће признање смањене корисности нуклеарног одвраћања. Даље истиче потребу за више пажње усмерене на политичке и нормативне димензије одвраћања, а рапидно на проширивање обима учења како би се боље разумела динамика сајбер простора и логика одвраћања у овом контексту (Morgan, 2012). Можемо констатовати одређене везе одвраћања и то према тероризму, затим сајбер безбедности (уопште новим технологијама), принуди, истраживачким центрима, као и одвраћања у контексту хибридног сукоба и конкуренције сивој зони. Ради комбиноване примене војно – стратешких, техничко – технолошких и друштвено – политичких развојних

трендова, савремени актери сукоба користе велики број инструмената принуде (техника) које примењују ради остварења националних интереса. Ти инструменти обухватају нуклеарне и конвенционалне војне капацитете, али и оне невојне инструменте државне власти.

Колин Грај (*Colin S. Gray*) у својој књизи *Стратегија и политика* износи да никад не може бити научно тачно доказано да ли су се неки изазови о безбедности десили или не, због политичких процеса и то остаје у сфери само нагађања. На пример, хоће ли велико повећање количине ракета дугог домета и нуклеарног наоружања добро служити за појачавање одвраћања или уместо тога може ли изазвати контра ефекат, непријатељски напад док он покушава да нападне пре него што повећамо своје снаге? Где год погледамо стратешка питања, перспективно налазимо контрадикторне односе који нам ускраћују безбедност, па и политички и стратешки успех. Тако да није корисно препознати само проблем који би требао бити решен, него је неопходно да се препозна природа стратегије и увек неодређени карактер вредности тако неизвесне појаве као што је безбедност. Нуклеарно оружје је толико различито од других врста војне моћи тако да је тешко створити нешто друго да га ефикасно замени у погледу силе. Грај перципира и могућност да би британски одлазак, укључујући евентуално пребегавање из Европске уније могао имати значајан утицај на критичну политику веродостојног одвраћања Путиновог малтретирања у источној Европи. Дугогодишња истраживања и јавна расправа о нуклеарном одвраћању јасан је пример *црног лабуда*, јер до сада није било билатералног нуклеарног рата. Можемо констатовати ову чињеницу као доказ или да закључимо, још увек. На крају крајева, како ћемо наступити у будућности и када то тачно будемо могли, морамо критички зависити од тренутног стања наших припрема за одвраћање и ратовање; време спровођења често је суштинска спутавајућа идеја (Gray, 2016). Садашњост и будућност нам је управо много везана за ову последњу Грејеву констатацију, али времена као облика трајања неке појаве, односно у овом случају би то било трајање од момента издавања задатка за употребу одређене врсте оружја, оруђа, средстава, до његовог дејства на циљ.

У раду великог броја теоретичара који се баве одвраћањем, Свеијс и Осинга (*Tim Sweijs & Frans Osinga*) су констатовали следеће као битне особине одвраћања. Када стратези говоре о рату, тада углавном кажу да је природа рата непроменљива, али да његов карактер јесте. Тај карактер је у суштини зависио од доба када се спроводио, па су оне носиле са собом одређене ограничавајуће услове и предрасуде. Ефикасност одвраћања не треба узимати олако, посебно не када се сагледавају одређене јединствене ситуације и када се претње одвраћања формулишу под одређеним, за тај период специфичним, притиском. Одвраћање мора бити схваћено првенствено као настојање да се обликује мишљење потенцијалног агресора. Приликом одвраћања неопходно је разумети интересе, мотиве потенцијалног агресора, укључујући шта вреднује и зашто. Да би одвраћање било ефикасно оно није само чиста претња већ представља постепено прилагођавање перцепције потенцијалном агресору тако да види резервну варијанту за агресију и да она буде боља, прихватљивија варијанта од самог рата. Одвраћање не зависи од тога да ли је рат скуп или ризичан у очима мете већ захтева да се изгледи за рат појављују као гора опција од друге опције, што свакако није увек случај. Процена исплативости рата у основи је обликована уверењима о последици поступака, или, другим речима, субјективних очекивања. Конвенционалне стратегије одвраћања могу се сврстати у следеће: пораз у бици, казнени отпор, стратешка одмазда, стратешки пораз. Поред значајне војне силе, ефикасна

конвенционална одвраћања захтевају снажну политичку вољу и издржљивост и неопходност убеђивања потенцијалног преступника да ће се претња на крају стварно реализовати. За САД, успон Кине и оживљавање РФ најавили су нову еру стратешког надметања, у којем се нуклеарно одвраћање вратило на политичку и војну сцену. Одвраћање САД од агресије РФ је довело до суочавања са изазовима везаним за пројекцију снаге, модернизацију снага и поделу обавеза, терета који је важнији. Одвраћање мора бити праћено јасном политичком вољом да би претње одвраћања биле веродостојне. Велике силе у новој ери надметања доводе до нових појмова у литератури и истицања термина као што су хибридни рат, сива зона, нови тотални рат, гранични рат и др. Велике силе користе широку лепезу војних и невојних активности у сврху принуде. Тада мислимо на економски притисак, кампању дезинформисања, подстицање политичке корупције, шпијунажу, обезбеђивање оружја опозиционим групама, поларизујуће домаће дебате у циљним земљама, сајбер нападе и др. Као одговор на ове појаве, а делом на појављивање стратегија ратних борби између различитих домена, аналитичари на Западу су изнедрили још један нови појам и то *одвраћање од више домена* (енг. *cross – domain deterrence*). Традиционални концепти одвраћања казном и порицањем и даље се налазе у званичним терминолошким објашњењима одвраћања, док се у суштини увеличавају фактори успешности одвраћања који укључују и комуникацију (информациони домен), веродостојних претњи наметањем трошкова (економски домен) и снажне политичке воље (Osinga & Sweijs, 2021).

Пре више од седам деценија Џорџ Ф. Кенан[2] (*George F. Kennan*), дипломата из САД, назвао је акције попут саботаже, дезинформација и мере политичке дестабилизације *мере без рата* (енг. *measures short of war*). Други теоретичари тврде да су то мере све које се предузимају у *сивој зони* осим конвенционалног или нуклеарног рата високог реда. *Непријатељске мере* (енг. *hostile measures)* је најприближнији термин, односно обухвата категорије „тајних или прикривених активних мера" (енг. *clandestine or covert active measures*) што би било најприближније делатностима које је Кенан настојао да опише. Овом термину коришћеном на Западу одговарале би *активне мере* (енг. *active measures*) које представљају термин коришћен на Истоку (РФ). У суштини, према Кенану, ове мере можемо одредити као државне активности осим конвенционалног или нуклеарног напада високог реда примењене против других држава у било ком тренутку и у било ком контексту, са непријатељском намером да стекну своју предност и смање способности, стабилности или предности друге државе (Connable et al., 2020). О важности деловања држава у *сивој зони* говори изјава секретара одбране САД, Џејмс Н. Матиса (*James N. Mattis*) који наглашава да су комбиноване претње понашања у *сивој зони* веће него што су претње терориста *Islamic State of Iraq and Syria – ISIS* (ради се о изјави везаној за Стратегију националне одбране САД 2018. године и то некласификованом делу; ово је важно нагласити јер јасно говори да постоји и класификовани – тајни део наведене стратегије одбране, где се сталним наглашавањем да све треба бити јавног карактера друге државе наводе инсистирањем и присилом да упознају јавност о својим тајним активностима, подацима, прим. аут.). Мере које нису ратне се генерално схватају као акције државе на државу, које се обично спроводе у *сивој зони*. Термин *сива зона* популаризован је након интервенције РФ на Крим 2014.

[2] Види шире: George F. Kennan, *Measures Short Of War – MSW*, Lectures At The National War College, 1946–47, September 16, 1946.

године. *Сива зона* је простор између потпуног неангажовања и избијања рата високог реда, при чему се овај други описује као интензиван, проглашен конвенционалним или нуклеарним ратом између оружаних снага две или више националних држава. Хибридни рат (енг. *hybrid warfare*) је термин који се генерално приписује Франку Г. Хофману (*Frank G. Hoffman*) на Универзитету националне одбране САД, а ради се о термину Североатлантског савеза, у непосредном периоду након заузимања Крима од стране РФ. Аналитичка заједница је на крају дошла до неког општег закључка о *сивој зони* и то да непријатељства у *сивој зони* нису ништа ново, посебно не за РФ, затим да ће РФ наставити да примењује ову тактику, али су њени циљеви и средства ограничени, и да је одвраћање, спречавање или сузбијање такозваног понашања у *сивој зони* тешко. У такозваној доктрини Герасимова[3] о отвореној употреби оружаних снага, неретко под плаштом очувања мира и регулисања кризе јесте примена само у одређеној фази, ради постизања крајњег тријумфа у сукобу. За овај Герасимовов чланак руски аналитичар Чарлс К. Бартлс[4] (*Charles K. Bartles*) из Канзаса, САД, закључује да Герасимов не предлаже нови начин ратовања РФ или *хибридни рат*, као што је констатовано на Западу (Connable et al., 2020).

3.1.2. Стратегијска документа која прописују одвраћање у САД

Доношењем доктрина Председника САД у протеклим деценијама, скоро сваки Председник САД је креирао спољну политику државе и давао иницијалну смерницу државним органима за поступање у раду. Поред доктрина Председника, пажњу заслужују и следећи документи који прописују одвраћање у САД: Стратегија националне безбедности САД, Национална одбрамбена стратегија САД, Националне војне стратегије САД.

3.1.2.1. Доктрине председника САД

Према Биркенталовој (*Birkenthal M. Sara*), *Велика стратегија* је велика идеја стране и политике националне безбедности, концепт који свеобухватно повезује циљеве, начине, средства и принципе организовања, који омогућава државама да наменски планирају и дају приоритет употреби свих инструмената националне моћи. Када говоримо о инструментима националне моћи, првенствено мислимо на дипломатске, економске, културне и војне. Велика стратегија не може бити само листа спољнополитичких приоритета, већ морају бити заступљени национални интереси спојени низом оперативних планова за њихову реализацију и напредовање, што представља замисао постављену од председника (Birkenthal, 2013). У свом раду Биркенталова је повукла потпуну једнакост у терминологији и изједначила терминолошки велику стратегију државе и доктрину председника, док поједини, када говоре о председничким доктринама, говоре само о спољној политици САД.

Према домаћим теоретичарима из ове области, Форца и Стојковић (Божидар Форца и Биљана Стојковић) заступају став да би стратегија државе (национална стратегија) као највиши хијерархијски документ у једној држави, требала „да садржи назначене националне вредности које се штите, националне интересе које треба остварити и циљеве које треба досегнути у одређеном периоду" (Форца и Стојковић, 2014, стр. 153). Даље, ови аутори

[3] Валериј Герасимов (*Valery Gerasimov*), Начелник Генералштаба оружаних снага РФ (*Chief of the General Staff RF*) чланак из 2013. године.
[4] Канцеларија за иностране војне студије оружаних снага САД (*U.S. Army Foreign Military Studies Office*).

овакву стратегију виде као полазни документ следећих докумената, који би били хијерархијски нижи документи и следили би након овог документа. Карактеристично уређење докумената ове врсте је у САД где постоји низ стратегијских докумената, који су хијерархијски повезани. Наведено се посебно односи на националну безбедност у оквиру које постоји Национална стратегија безбедности (енг. *National Security Strategy*) из које „проистичу и посебне стратегије, попут стратегије одбране (енг. *National Defense Strategy*) и војне стратегије (енг. *National Military Strategy*) и стратегије појединих видова војске. Нова Војна стратегија усвојена је почетком 2012. године, са основном интенцијом да се у наредној деценији смање оружане снаге те силе, уштеди више стотина милијарди долара и да се тежиште активности пребаце из средње Азије у регион Пацифика. У складу са том стратегијом, оружане снаге САД би биле преобликоване са нагласком на борбу против тероризма, нуклеарну одбрану, заштиту територије САД и на одвраћање од агресије сваког потенцијалног непријатеља. Такође, САД планирају да тежиште развоја дају на авијацији (беспилотне летилице) и на поморским снагама" (Форца и Стојковић, 2014, стр. 156, 157).

Ближе уређење Председничких доктрина на стратегијском нивоу је уређено документима који дају смернице за рад одређеним лицима, организацијама, институцијама, органима у држави, а које се разрађују кроз стратегије, доктрине и друга документа. Сједињене Америчке Државе покушавају да стратегијом одвраћања и другим документима утичу на РФ и покушавају да их одврате од руског сукоба у *сивој зони* (енг. *gray zone*). Када говоримо о сукобу у *сивој зони*, тада мислимо на сукоб који постоји на нивоу испод општег рата, односно континуирано ратовање испод прага великог рата (Mazarr, 2018).

После Хладног рата, у САД су на челу државе били следећи председници по којима су и њихове доктрине за спољну политику добијале назив, тако да ћемо у наредном делу истраживања говорити о доктринама у време администрација Клинтона, Буша, Обаме, Трампа и Бајдена (у току истраживања је трајао мандат).

Клинтонова доктрина, Бил Клинтон (*Bill Clinton*), од 1992. године до 2001. године. У низу доктрина, практичност Клинтонове доктрине највише је личила на Никсонову доктрину, која је ограничавала америчко учешће новца и опреме. Никсонова политика је деловала јасно, са антикомунистичким смерницама. Насупрот томе, са овим ранијим принципима, Клинтонова доктрина нема услова који би аутоматски гарантовали интервенцију САД или укључивање у сукоб. Уместо тога, Клинтонова доктрина чини било коју америчку акцију зависном од средстава и резултата, а САД могу деловати само тамо где је такво поступање практично. Ово је изразито другачији приступ. Каспар Вајнбергер (*Caspar Weinberger*) је био секретар још у време Регана. Такозвана Вајнбергерова доктрина, којом је утврђена јасна листа критеријума за одобравање употребе силе: да ли је стање у виталном националном интересу САД, да ли је могуће обавезати довољно ресурса за успех, да ли ће таква обавеза бити непрекидна, да ли постоје јасно дефинисани циљеви, да ли ће бити подршке од Конгреса и људи из САД, да ли су постојале друге опције које су се могле користити. Ова доктрина је успешно коришћена у Заливском рату, али Клинтонова администрација је вратила на дораду, јер је општи утисак био да је и Вајнбергерова доктрина била рестриктивна и да би војска могла, требало би да се користи у више ситуација. Клинтонов саветник за националну безбедност, Антони Лејк (*Anthony Lake*), на ову тему у говору на Универзитету националне одбране (енг. *National Defense University*) навео је седам ситуација у којој би се сила могла користити: бранити САД, америчке држављанине и

савезнике; супротстављати се агресивним делима; бранити економске интересе; бранити демократију; сузбијати ширење оружја за масовно уништење, тероризам, криминал и наркотике; чувати утисак о поузданости; тежити хуманитарним циљевима. Овом приликом се ипак наглашава да САД не могу да реше сваку кризу на свету, али и да неће седети по страни када су угрожени људски животи. Могло би се рећи да се Клинтонов приступ не може с правом сматрати доктрином зато што му недостају смернице које одређују када треба предузети радњу. Клинтонов приступ предвиђа да САД морају учинити нешто и да буде присутна уздржаност. Тамо где су вредности и интереси САД у питању и где могу, ту се мора бити спреман за деловање (Gendlin, 1998).

Бушова доктрина, Бушова спољна политика (2001 – 2009): „ја одлучујем и одлучујем шта је најбоље" (Birkenthal, 2013, p. 47). Са овом одредницом је Буш заступао своје погледе на спољну политику. Бушова доктрина је фраза која се користи за описивање различитих сродних спољнополитичких принципа бившег председника САД – Џорџа Буша (*George W. Bush*). Фразу је први пут употребио Чарлс Краутхамер (*Charles Krauthammer*) у јуну 2001. године да би описао Бушову администрацију. *Бушова доктрина* након напада 11. септембра је добила смерницу и дан напада је представљао прекретницу за Буша, који је био присиљен да своје тежиште усмери на међународне проблеме. Бушова доктрина покривала је све аспекте спољне политике и одражавала је његово гледиште о томе шта америчка спољна политика треба да постигне. Бушова доктрина постала је снажно повезана са одлуком Бушове администрације да нападне Ирак 2003. године (због чега се Бушова доктрина врло често назива и Чејнова или Рамсфелдова доктрина енг. *Cheney Doctrine or the Rumsfeld Doctrine*, који су најдоминантнији били у утицају да Бушова одлука буде донешена о нападу на Ирак). Стратегија *превентивних удара* као одбрана од непосредне или претпостављене будуће претње безбедности САД је карактеристична за ову доктрину. Овај принцип политике посебно је примењен у средњем Истоку да се супротстави међународним терористичким организацијама и да оправда инвазију на Ирак. Да закључимо, Бушова доктрина је коришћена да скрене пажњу на спремност да једнострано гони америчке војне интересе. Фразу *Бушова доктрина* ретко су користили чланови Бушове администрације. Председник Буш даје примедбе 2006. године током конференција за штампу у Врту ружа о томе како Иран има нуклеарне амбиције и Северна Кореја планира нуклеарни тест (процедуре одвраћања). Према Бушовој доктрини, ради се о два елемента (циља) и то америчком примату и превентивном рату. *Први, амерички примат*, посматрао је политички универзум као једнополаран, при чему САД имају право и одговорност да служе као хегемон. *Други, превентивни рат*, залагао се за први удар против непријатеља који је одлучан да нанесе штету САД. Бушова доктрина настојала је да јавности пружи јасан осећај претњи које су реалне по САД. Избегла је екологизам, националну изградњу и преговоре у корист кризе дипломатија. Редефинисала је војне претње истичући само три државе, Иран, Ирак и Северну Кореју, чији су напори за постизање нуклеарног оружја представљали осу зла (Birkenthal, 2013).

Обамина доктрина. Обамина спољна политика (2009–2017) тражила је редефинисање америчког лидерства у све глобализованијем свету и интеракцију са мноштвом држава и недржавних актера попут невладиних организација и других транснационалних група у међународном систему. То је поставило велику вредност за рад са савезницима и у оквиру мултилатералних институција. Обама је био снажни заговорник уверења да САД морају

прихватити ограничења рада унутар ових институција да би постигле своје међународне циљеве и да морају да траже легитимитет у покушајима да заштите своје виталне интересе. Обама у својој великој стратегији замишља свет не као мултиполарни, већ као мултипартнерски и покушава да ефикасно ресетује, чак и трансформише спољну политику САД. Сходно томе, најпознатија фраза која артикулише Обамину велику стратегију је „водећа с леђа". На основу ове парадигме залагао се за избегавање међународних конфликта осим ако нису били од апсолутно виталног значаја за америчке националне интересе (Birkenthal, 2013).

Трампова доктрина. У периоду од 2017. до 2021. председник САД, Доналд Трамп (*Donald Trump*) је био човек који је покушао да промени америчку спољну политику. У САД је владало подељено мишљење о најављеној промени америчке спољне политике, јер је већина фаворизовала тренутну хегемонску стратегију и оне који су се надали да ће Трамп успети да преусмери спољну политику Вашингтона. Врло често је коментарисано да је Доналд Трамп први председник САД у постхладноратовском периоду за којег се чини да није имао велику стратегију. Ово је резултирало извесном инерцијом у спољној политици САД, с обзиром на то да међународни системски фактор, релативни пад америчке моћи, није довољан да произведе такву промену у својој спољној политици која би утицала на идентитет САД, са фаворизовањем хегемонистичког понашања. Немати велику стратегију је корак напред у поређењу са либералном стратегијом хегемоније Трампових претходника (Trapara, 2017).

„Убиство Солејманија је део нове стратегије одвраћања непријатеља", изјавио је у јануару 2020. године амерички државни секретар Мајк Помпео (*Majk Pompeo*) који је рекао да је „Касем Солејмани (*Kasem Solejmani*) убијен у склопу шире стратегије одвраћања претње коју представљају непријатељи САД, која се односи и на Кину и Русију, ублажавајући тиме тврдње да је највиши ирански генерал убијен, јер је планирао нападе на америчка дипломатска представништва. Помпео је одржао говор на Хуверовом институту на Универзитету Стенфорд, у којем није изричито спомињао нападе које је наводно планирао Солејмани. Амерички државни секретар се у свом говору фокусирао на, како је рекао, стратегију администрације да успостави *стварну политику одвраћања* према Ирану после претходних републиканских и демократских политика које су подстицале *злоћудне активности* Ирана. Демократе и републиканци су критиковали Трампову администрацију за оправдавање самоодбране која се заснивала на необјављеним обавештајним подацима о претњи. Председник Доналд Трамп је рекао да су међу потенцијалним циљевима тих напада четири америчке амбасаде, а Министар одбране Марк Еспер (*Mark Esper*) је изјавио да није видео никакве обавештајне податке који би упућивали на могуће нападе на дипломатска представништва. Трамп је поново долио уље на ватру рекавши да *заправо и није битно* да ли је Солејмани представљао претњу. Помпео је рекао да се иза убиства иранског генерала крије *шира стратегија*. Председник Трамп и његов тим за националну безбедност поново успостављају политику одвраћања, стварног одвраћања Ирана, рекао је тада државни секретар. Противник мора да се убеди не само да је САД способна да наметне захтеве, него и да заиста има вољу да их спроведе у дело, рекао је Помпео додавши да је нуклеарни споразум с Ираном из 2015. године, из којега се Трамп повукао 2018. године, само охрабрио Техеран. Према његовим речима, САД сада има велику предност у односу на Иран, а стратегија одвраћања није ограничена само на Иран. „У сваком случају морамо одвраћати

непријатеље како бисмо одбранили слободу. То је сав смисао Трамповог настојања да нашу војску учини јачом него што је икад била", рекао је Помпео (Lamarque, 2020, p. 1). На основу ове Помпеове изјаве, можемо да дођемо до два закључка: први да је Помпео покушао да „исправи" пропусте председника Трампа у обраћању медијима о убиству генерала, а други је да је за време Трампове доктрине (уколико је она уопште постојала) на снази била, како то он назива, „шира стратегија одвраћања", која свима на планети шаље поруку да су у било ком месту на планети доступни снагама САД за одмазду. Можда бисмо и могли констатовати да би ова доктрина представљала модернизацију Бушове доктрине и првенствено њене стратегије *превентивних удара*.

3.1.2.2. Стратегија националне безбедности САД

Стратегија националне безбедности оцртава националну стратегију и њене главне бриге о националној безбедности и како се нација планира бавити њима (Scott, 2018).

У Стратегији националне безбедности САД (за време мандата председника Клинтона) из 1999. године (*The National Security Strategy for a new century, 1999*) се износи да одржавање присуства САД у иностранству промовише регионалну стабилност и доприноси одвраћању, демонстрирајући одлучност у одбрани америчких, савезничких и пријатељских интереса у критичним регијама. Напори да се одврати противник, била то нација, терористичка група или злочиначка организација, могу постати водећа идеја одговора на кризу. Одвраћање од кризе углавном укључује сигнализирајућу посвећеност САД, а одређену државу или интерес унапређењем наше ратне способности на терену. Борба и победа у великим ратовима је врхунски тест оружаних снага САД. За догледну будућност, САД по могућности у договору са савезницима, морају имати способност одвраћања и ако одвраћање не успе, да уследи пораз великих размера, прекогранична агресија (National Security Strategy for a new century, 1999).

У Стратегији националне безбедности САД (за време мандата председника Буша) из 2006. године (*The National Security Strategy of the United States of America, 2006*) наведено је следеће у вези са одвраћањем: „Ново стратешко окружење захтева нове приступе одвраћању и одбрани. Наша стратегија одвраћања више не почива првенствено на мрачној премиси наношења погубних последица потенцијалним непријатељима. Оба приступа, офанзивни, а и дефанзивни су неопходни да би се одвратили државни и недржавни актери, негирањем циљева њихових напада и ако је потребно, одговором са надмоћном снагом." (National Security Strategy, 2006, p. 22). Наглашавање да је неопходан нови приступ одвраћању услед условљености новим окружењем уз присуство како дефанзивне тако и офанзивне компоненте, указује на то да под одвраћањем није циљ само одбрана већ и превентивни напад о чему у овом документу немамо детаљно разрађене поступке. Поред наведеног, није речено ни које снаге би спроводиле ове „офанзивне компоненте", тако да је у сфери промишљања да ли се ради о војној моћи и/или неким другим актерима, можда службама безбедности.

У САД је један врло битан документ одредио претње по националну безбедност САД. Ради се о Стратегији националне безбедности САД (за време мандата председника Трампа) из 2017. године, где је између осталих и РФ одређена као приоритетна претња по националну безбедност САД. У овој стратегији је наведено да Русија користи информационе операције као део својих увредљивих сајбер напора да се утиче на јавно мњење широм света. Њихове

кампање утицаја се мешају кроз прикривене операције служби безбедности и лажне интернетске личности са државним медијима, независним посредницима, и плаћеним корисницима друштвених мрежа или „троловима". Према овој стратегији, РФ користи субверзивне мере за слабљење кредибилитета америчке посвећености Европи, подрива трансатлантско јединство и слаби европске институције и владе. Својим најездама на Грузију и Украјину, РФ је демонстрирала своју спремност да крши суверенитет држава. Руска Федерација наставља да застрашује суседе претећим понашањем, као што су нуклеарно држање и распоред снага за офанзивна дејства (National Security Strategy of the United States of America, 2017).

У октобру 2022. године, за време Бајденове администрације, усвојена је у САД нова Стратегија националне безбедности САД у којој је читав сегмент стратегије посвећен одвраћању, *интегрисаном одвраћању* (нови термин). САД по овој стратегији имају витални интерес да одврате агресију Народне Републике Кине, РФ и других држава. Захтева се способност праћења понашања испод и изнад традиционалног прага сукоба, где САД себи неће да приуште ослањање само на конвенционалне снаге и нуклеарно одвраћање. Одбрамбена стратегија мора да одржи и ојача одвраћање, уз Народну Републику Кину као изазов темпа. Интегрисано одвраћање се ослања на беспрекорну комбинацију способности убеђивања потенцијалних противника да су трошкови њихових непријатељских активности већи од њихове користи. Када се говори о интегрисаном одвраћању, у овој стратегији се мисли на следеће: интеграцију у више домена, широм војних (копнене, ваздушне, поморске, сајбер и свемирске) и невојних (економске, технолошке и информационе) домена ангажовања. Затим следи интеграција широм региона, и у домовини, па интеграција у целом спектру сукоба како би се спречило да конкуренти мењају статус док лебде испод прага оружаних сукоба. Такође, говори се и о интеграцији у Влади САД од *дипломатије, обавештајних и економских алата до безбедносне помоћи и одлуке о држању силе*. Ту је и интеграција са савезницима и партнерима кроз улагања у интероперабилност и заједнички развој способности, кооперативно планирање положаја и координисан дипломатски и економски приступ. Интегрисано одвраћање захтева ефикаснију координацију, умрежавање и иновирање, тако да сваки конкурент који размишља о томе да тежи предности у једном домену разуме да САД могу одговорити и у многим другим доменима (National Security Strategy of the United States of America, 2022).

3.1.2.3. Национална одбрамбена стратегија САД

Национална одбрамбена стратегија САД (*National Defense Strategy*) као трајну мисију Министарства одбране одређује обезбеђење борбено веродостојних војних снага које могу да одврате рат и заштите безбедност нације. Ако одвраћање не успе, оружане снаге морају бити спремне да буду ангажоване и да победе. На овај начин, ојачавају се традиционална америчка оруђа дипломатије, где се стварају могућности да Председник и дипломате САД преговарају са позиције снаге – силе (National Defense Strategy, 2018). Суштину ове стратегије чини концепт активне, слојевите одбране на глобалном нивоу што подразумева интеграцију америчких способности у иностранству, разним регионима света. Поред тога, под глобалним способностима се подразумева и употреба свемира и сајбер простора у одбрани. Укратко, дубинска одбрана је заснована на посматрању стратешког окружења као отвореног система у коме се људи, трговина и информације непрекидно крећу, а за шта

читава Влада САД доприноси одбрани. Да би активна, слојевита одбрана била ефикасна, потребни су врхунско прикупљање, спајање и анализа обавештајних података, прорачунато одвраћање непријатеља, слојевити систем у коме се међусобно подржавају одбрамбене мере које нису ни лат. *ad hoc* ни пасивне, и способност масовног фокусирања довољних средстава за борбу, да би се одбранили од било којег напада (Bartholomees, 2008).

Развојем нових технологија дошло је до груписања компоненти за одвраћање. Званичне, јавне компоненте одвраћања у оружаним снагама САД су: сајбер простор, ракетни балистички одбрамбени систем, интерконтиненталне балистичке ракете, команда и контрола, нуклеарно одвраћање кроз примену науке и технологије (изузев нуклеарног тестирања), флексибилност, способност напредног распоређивања бомбардера и авиона са двоструком способношћу, балистичке ракете на подморницама. У 2022. години, објавом нове Националне стратегије одбране САД (*National Defense Strategy*) дата су четири одбрамбена приоритета од којих су два везана за одвраћање: Одвраћање од стратешких напада на САД, савезнике и партнере и Одвраћање од агресије, уз спремност да превлада у сукобу када је то потребно – давање приоритета изазову Народне Републике Кине у Индо – пацифичком региону, затим изазову РФ у Европи. У овој стратегији је наглашен термин *интегрисано одвраћање* који „подразумева неприметан рад у доменима ратовања, местима сукоба, спектру сукоба, свим инструментима америчке националне моћи и нашој мрежи савеза и партнерстава. Прилагођен специфичним околностима, примењује координиран, вишеструки приступ смањењу перцепције конкурената о чистим користима агресије у односу на суздржаност. Интегрисано одвраћање је омогућено борбено веродостојним снагама које су спремне да се боре и победе, по потреби, уз подршку безбедног и ефикасног нуклеарног одвраћања" (National Defense Strategy, 2022, p. 1). Ова стратегија је донела поред тежишта на одвраћању и одређења везана за *сиву зону* односно енг. *gray zone activities*, где као методе сиве зоне препознаје принудне приступе који могу пасти испод перципираних прагова за америчку војну акцију. Такође, наглашавају се активности Народне Републике Кине против САД у овој зони и то од стране снага које контролише држава, за сајбер и свемирске операције и економске принуде не само против САД већ и против њених савезника и партнера. Када је реч о РФ, они према овој стратегији користе дезинформације, сајбер и свемирске операције против САД и њених савезника и партнера, као и нерегуларне, тзв. *прокси снаге* у више држава. Други, Северна Кореја и Иран, користе сличне активности, само што их тренутна ограниченост количином расположивих средстава спутава у постизању истих или сличних ефеката као што је то случај са РФ. Пролиферација напредних ракета, авионских система без посаде и сајбер алата, све до војних *прокси снага* омогућавају конкурентима да угрозе америчке снаге, савезнике и партнере, на индиректне и порицане начине. Ова стратегија селектује начине одвраћања овим редом: одвраћање порицањем, одвраћање отпорношћу, одвраћање директним и колективним трошковима, као и одвраћање информацијом (National Defense Strategy, 2022). Веома актуелна стратегија где увођењем интегрисаног одвраћања и давањем приоритета у одбрамбеној политици велике силе као што је САД на одвраћању у два приоритета (од само четри која је поставила стратегија одбране САД из 2022.) можемо математички констатовати да тачно пола одбрамбене стратегије САД чини управо одвраћање и ово треба озбиљно схватити. Међутим, поред наведеног, за ову стратегију је изузетно битно нагласити представљање *сиве зоне*, односно како се у стратегији наводи *активности у сивој зони*, где углавном наступа присила ради остварења циљева

постављених од руководства државе, где већи део ових и сличних активности предузимају или учествују у њима службе безбедности државе углавном путем необавештајних активности.

3.1.2.4. Националне војне стратегије (1989, 1992, 1995, 2004, 2011, 2015, 2018)

Национална војна стратегија (*National Military Strategy*) у *Речнику војних и њима сродних израза* оружаних снага САД је дефинисана као „документ који је одобрен од руководства оружаних снага САД, ради дистрибуције и примене војне моћи у спровођењу Стратегије националне безбедности и циљева Одбрамбене стратегије у стратешком вођењу" (Department of Defense Dictionary of Military and Associated Terms, 2021, p. 150).

Национална војна стратегија (*National Military Strategy*) обезбеђује дејство заједничких сила са циљем заштите и напредовања САД, односно њених националних интереса. Одражава колективну мудрост шефа здружених снага и команданата, и представља њихов најбољи војни савет. Национална војна стратегија предвиђа удруживање снага са задатком заштите и унапређења америчких националних интереса. То је стратешки правац за војни допринос у остваривању циљева Стратегије националне безбедности за унапређење националних интереса. Главни фокус заједничке доктрине је војна стратегија, која примењује *уметност и науку* у примени силе и претње силом да би се осигурали циљеви националне политике (Scott, 2018). У последњој реченици већ можемо да констатујемо да поред примене силе као крајње одреднице Националне војне стратегије, други део појма који одређује поменуту стратегију чини претња силом, односно терање, приморавање непријатеља, противника на одвраћање.

Национална војна стратегија из 1989. (*The National Military Strategy Document of the United States of America, 1989*) се фокусирала на хладном рату и Совјетском Савезу и артикулисала војни елемент у многим деловима света, алијансе, попут Северноатлантског савеза. Ова стратегија је била утемељена на снажном нуклеарном одвраћању, укључујући предњу одбрану са много снага распоређених напред, посебно у Европи и Кореји, које су потом подржане брзим појачањем да би се разишле у оперативне базе у многим народима (Bartholomees, 2008).

Национална војна стратегија из 1992. (*National Military Strategy of the United States, 1992*) се заснивала на томе да САД пружају вођство за промоцију глобалног мира и безбедност. Изграђена је на следећа четири темеља: Стратешко одвраћање и одбрана, који се састојао од веродостојног нуклеарног одвраћања састављеног од офанзивних и одбрамбених способности; Присуство, које се састојало од снага које су непрекидно биле стациониране или распоређиване широм света; Кризни одговор, што је била способност брзог одговора на више од једне регионалне кризе; и Реконституција, која је укључивала способност мобилизације особља, опреме и индустријске базе за обнову снаге војске. Одвраћање по овој доктрини захтева да су оружане снаге оспособљене за брзо реаговање и спремне за борбу, као и одговоре на кризе. Захтева се тимски рад на свим нивоима као и са активним саставом и резервним припадницима јединица, затим да су обучени за вештине којима морају да доминирају, затим правовремено доћи до тачних безбедносно интересантних података и одржавати интензивне тренинге (National Military Strategy of the United States, 1992). Закључак је да је за одвраћање по овој стратегији, у миру, технолошка супериорност кључни

елемент. У рату побољшава борбу, ефикасност и смањује губитак особља и опреме. Колективни пораз у Ираку очигледно показује потребу за супериорним службама безбедности и поседовањем најбољег светског оружја и оруђа. Нуклеарно одвраћање је настављено као једна од опција у миру и подршке јединицама у мисијама. Стратегија предвиђа да ће с обзиром на количину нуклеарног Совјетског арсенала, нуклеарно одвраћање још дуго бити актуелна стратегија одвраћања.

Национална војна стратегија из 1995. (*National Military Strategy of the United States of America, 1995*) има активнију употребу војске на глобалном нивоу за промоцију стабилности, уместо да се реагује на случајеве нестабилности. Да би се постигла ова два циља, стратегија из 1995. године је дефинисала три компоненте: мирнодопски ангажман; одвраћање и спречавање сукоба, превенцију; борба и победе у ратовима. У основи се очекивало да војска постане ангажованија у превенцији сукоба, укључујући мисије као што су одржавање мира, спровођење мира и помоћ нацији; мисије које нису поменуте у стратегији из 1992. године (National Military Strategy of the United States of America, 1995).

Рамсфелд (*Donald Rumsfeld*) је у мају 2002. године ставио већи нагласак на нови стратешки концепт, *напред одвраћање*, односно посвећеност нападима на потенцијалне претње у иностранству. Док је пројекција америчке снаге на велике даљине за борбу против нових противника имала смисла. Нагласак је био првенствено на глобалној способности са додатним ангажовањем на прекоморском прикупљању обавештајних података, прикривеним специјалним операцијама, беспилотним ваздушним возилима, сајбер ратовању, хиперсоничним ракетама и способности спречавања противника од ометања америчке комуникационе и обавештајне имовине у свемиру и удара у подземне циљеве (Bartholomees, 2008).

Национална војна стратегија из 2004. године (*The National Military Strategy Document of the United States of America, A Strategy for Today; A Vision for Tomorrow, 2004*) фокусира активности на акције које осигуравају савезнике и пријатеље, а где је неопходно разуверити потенцијалне противнике, одвратити од агресије и супротставити се принуди и поразу. Снажни савези и коалиције доприносе узајамној безбедности, теже одвраћању агресије и помажу у постављању услова за успех у борби ако одвраћање не успе. Одвраћање агресије почива на противнику који схвата да САД имају способност да порекну стратешке циљеве и наметну тешке последице као одговор на непријатељске или потенцијално непријатељске акције. Одвраћање агресије и принуде мора бити антиципативне природе како би се спречила катастрофа, утицај напада употребом биолошког, хемијског или нуклеарног оружја на цивилно становништво популационих центара у САД или у партнерским државама. За ефикасно одвраћање потребан је стратешки план комуникације који наглашава спремност САД да примене силу у одбрани својих интереса. САД захтевају широк скуп могућности да обесхрабре агресију и принуде. Нуклеарне способности и даље играју важну улогу у одвраћању од пружања војних опција за спречавање низа претњи, укључујући употребу оружја за масовно уништење и конвенционалних снага великих размера. Нови модел за стратешко одвраћање укључује ненуклеарне и нуклеарне ударне снаге, активну и пасивну одбрану, као и инфраструктуру за изградњу и одржавање снаге. Побољшање ненуклеарних способности напада, информационе операције, командовање и управљање, обавештајне и свемирске снаге допринеће да робуснија и ефикаснија буде способност одвраћања. Будући

напредак у циљању и прецизности ће пружити способности неопходне за победу ширег низа циљева уз смањење колатералне штете (National Military Strategy of the United States, 2004).

Национална војна стратегија из 2011. (*The National Military Strategy of the United States of America, Redefining America s Military Leadership, 2011*) је предвидела недржавне актере који поред државних такође компликују одвраћање и одговорност ширењем свог досега кроз напредне технологије које су некада биле искључиво домен држава. Принципе одвраћања сходно овој стратегији неопходно је прилагодити напорима у супротстављању екстремистима. Терористе је врло тешко директно одвратити; они врше калкулације трошкова и користи и зависе од држава и других заинтересованих страна на које треба утицати. Такође, неопходно је одржавати конвенционална средства одвраћања. За безбедност је потребна способност брзог и глобалног пројектовања моћи у свим доменима; подржати приступе одвраћања целе нације који комбинују економске, дипломатске и војне алате за утицање на противничко понашање. Неопходно је прилагодити принципе одвраћања безбедносним изазовима XXI века, појачавајући одвраћање у ваздуху, свемиру и сајбер простору. Сајбер простор захтева еластичну архитектуру која користи комбинацију за откривање, одвраћање, порицање и вишеслојну одбрану (National Military Strategy, 2011).

Национална војна стратегија из 2015. (*The National Military Strategy of the United States of America, The United States Military's Contribution To National Security, June 2015*) се на неколико места бави одвраћањем као сегментом битним за поступке оружаних снага САД. Нове технологије утичу на рачун одвраћања и управљања сукобима повећавањем неизвесности и сажимањем простора за доношење одлука. На пример, напади на наше комуникационе и сензорске системе могу се догодити са мало или нимало упозорења. Наведено доводи до проблема евентуалних одговора система у таквим случајевима. Директан је утицај на нашу способност процене, координације, комуникације и реаговања у таквим ситуацијама. Даље у стратегији се наглашава да се у будућности сукоби између држава могу показати непредвидљивим, скупим и тешким за контролу. Стратегија даље предвиђа да ако одвраћање није успешно, оружане снаге САД ће бити способне да поразе регионалног противника у великој, вишефазној кампањи, по потреби намећући неприхватљиве трошкове, другом агресору у другом региону. Такође, америчка војска је спремна да пројектује моћ како би порекла циљеве противника. Други облик пројекције снаге је удруживање са партнерима ради извођења ограничених операција у ванредним ситуацијама. Такве операције могу укључивати проток додатних америчких снага и способности у одређени регион ради јачања одвраћања, спречавања ескалације и уверења савезника. Циљ је ојачати одвраћање, истовремено осигуравајући дугорочну одрживост капацитета САД за пројекцију снаге пуног спектра (National Military Strategy, 2015). Овде региструјемо званичну намеру наношења економских трошкова непријатељу где своју супериорност у економији САД поставља као један од доминантних, чак и војних задатака у одвраћању непријатеља од нежељених намера САД.

Национална војна стратегија из 2018. (The *National Military Strategy of the United States of America, The Joint Staff, June 2018*) у одређењу мисија којима треба да се баве оружане снаге САД, од пет мисија две имају намену одвраћања где можемо да закључимо да се ради о стратегији која је доминантно базирана на одвраћању. Ради се о одвраћању стратешког напада (и ширења оружја за масовно уништење) и одвраћању конвенционалног напада. Стратегија даље истиче да дизајн снага омогућава Здруженим снагама да раде оно што раде

на суштински различите и ометајуће начине како би осигурали да Здружене снаге могу одвратити или поразити будуће противнике (National Military Strategy of the United States of America, 2018). Национална војна стратегија за 2018. годину даје смернице како ће Здружене снаге одбранити САД и задржати своју предност, доминацију, а како би одвратиле конкуренте и победиле противнике, радило се то о великим силама или другим безбедносним изазовима.

Војне доктрине или, како их у САД зову, заједничка (здружена) доктрина (енг. *joint doctrine*) према *Речнику војних и њима сродних израза* оружаних снага САД имају следеће значење: „основни принципи који воде припаднике оружаних снага САД у координираној акцији ка заједничком циљу и могу укључивати појмове, тактике, технике и поступке" (Department of Defense Dictionary of Military and Associated Terms, 2021, p. 114). Војне доктрине се фокусирају на развој планирања употребе војне моћи на националном нивоу и коришћења као инструмента моћи у комбинацији са другим инструментима државе и националне моћи, а све то у трагању за спровођењем циљева политике.

Велики број стратешких докумената у САД је предвидео одвраћање на стратегијском нивоу (горе наведени), вреди поменути и Пословни оперативни план националне одбране (енг. *FY 2018 – FY 2022 National Defense Business Operations Plan*) где је наведено да је трајна мисија Министарства одбране да обезбеди борбено веродостојне војне снаге потребне за *одвраћање* од рата и да заштити безбедност САД. Ако *одвраћање* не успе, Заједничке снаге су спремне за победу. Јачањем америчког традиционалног оруђа дипломатије, пружа се војна опција за обезбеђивање председника САД и дипломате имају могућност да преговарају са позиције силе, снаге. Примена концепта одвраћања захтева континуирани напор како би се прилагодили безбедносном окружењу које се стално развија (National Defense Business Operations Plan, 2022).

С обзиром да је једна од угроженијих држава на свету, а налази се под *менторством* САД, ово истраживање би било ускраћено и непотпуно, ако не бисмо бар у кратким цртама анализирали најбитнији правни документ Израела који регулише одвраћање на стратегијском нивоу. Стратешки документ Израела, Стратегија израелских одбрамбених снага (*Israel Defense Forces Strategy*), који указује да стратешки однос између две државе, односно државе и велике силе, Израела и САД, игра важну двоструку улогу у израелском одвраћању, што се огледа у следећем. Врло блиска сарадња са САД повећава домет Израела за политичке и оперативне маневре при одговору на агресију на Израел, и то побољшава оперативне способности Израела да нанесе штету својим непријатељима помоћу већег јачања снага као и путем претње интервенцијом САД у њено име. Прилагођавање концепта одвраћања од XXI века у политици САД, мењање природе посвећености САД као дела модела проширеног одвраћања, израелско одвраћање у XXI веку и проширење концепта одвраћања укључивањем невојних оруђа у стратегије и јачање везе између одбране и одвраћања су основна обележја која карактеришу ову стратегију (Golov, 2016).

У августу 2015. године је објављена[5] прва икада јавно обелодањена Стратегија израелских одбрамбених снага, преведена на енглески језик у августу 2016. године (*Israel Defense Forces Strategy 2016*). Колико озбиљно једна од угроженијих држава на планети

[5] Аутор стратегије израелских одбрамбених снага (*Israel Defense Forces Strategy*), Начелник Генералштаба оружаних снага Израела, генерал – потпуковник Гади Еизенкот (*Chief of General Staff Lt. Gen. Gadi Eisenkot*).

схвата место и улогу служби безбедности за опстанак једног народа и поштовању њених припадника, ради потреба одвраћања, можемо најбоље закључити по томе чији је издвојен цитат у самој Стратегији израелских одбрамбених снага. У питању је мисао Амоса Јадлина (*Amos Yadlin*), бившег шефа Војне обавештајне службе Израела, која гласи: „Хамас и Хезболах нисмо уништили, али смо били у могућности да се успостави одвраћање. Ово је у суштини зато што смо их јако ударили, и зато што су терористи, на неки начин, постали као непотпуни државни ентитети, али јесу као полудржавни ентитети. Терористи су открили да када су одговорни за своју економију, за образовање, за живот свог народа, одједном се не усуђују да користе терор цео дан" и говори много о ефектима одвраћања у једној држави (Graham, 2016, p. 24). Одвраћање се ствара у перцепцији, али заснива се такође на физичким и конкретним елементима. Израелско одвраћање се ослања на предност система одбране Израела, али са нагласком да је ограниченије него у прошлости зато што се претња променила. Одвраћање мора бити специфично и прилагођено сваком непријатељу. Одвраћање од било ког непријатеља мора бити генерализовано и кумулативно читаво време (у циљу одржавања постојећег стања), да буде у контексту одређене кризе – специфичне и прецизиране, како би непријатељ био присиљен да делује или избегне одређено дејство ради заустављања рата или спречавања погоршања стања, ситуације. Према овој стратегији, компоненте одвраћања су следеће: „веродостојна претња тешким офанзивним операцијама која је заснована на изградњи снага (силе), јавној перцепцији акција које показују нашу спремност на ризик и ограничене офанзивне акције. Неопходно је да оружане снаге одржавају имиџ одвраћања и способности као непредвидивог непријатеља који може да реагује на веома озбиљан начин. Израел периодично спроводи ваздушне ударе у Сирији и Либану да се наметну *црвене линије* против терористичке организације, као нпр. ваздушни напад у децембру 2015. године против Самира Кунтара, самог врха оперативе Хезболаха" (Graham, 2016, p. 25). Акције које треба да одврате непријатеља биће спроведене у оквиру *Кампање између ратова* (енг. *Campaign between wars*). Образложење за употребу силе у кампањи између ратова је ради слабљења компоненте негативне силе, затим ради минимизирања способности непријатеља и јачања својих снага, па стварања оптималних услова за победу у будућем рату и стварања легитимитета за спровођење израелске акције и порицање легитимности у акцији непријатеља. Овакве акције које се воде између ратова захтевају мултидисциплинарни концепт, односно употребу следећих сфера: војну, економску, правну, медијску и политичку, а да идеја о операцијама буде са једним циљем, стратешким. Такве идеје за употребу офанзивне силе обухватају употребу, комбинацију *тајне* (енг. *covert operations*) и *прикривене* операције[6] (енг. *clandestine operations*), акције на свим фронтовима и димензијама ван граница Израела. Важно је нагласити да је ова политика заснована на подацима добијеним ангажовањем служби безбедности и усмерена је на наношење штете непријатељским поступцима или намерама. Овим документом је регулисана *отворена акција* за стварање одвраћања којом се наглашавају границе уздржаности Израела. Водећи принципи за употребу силе у кампањи између ратова у *тајним* и *прикривеним*

[6] *Тајне операције* (енг. *covert operations*) су операције чији су резултати видљиви непријатељу и намењене су и спроведене на начин да се идентитет оних који стоје иза њих сакрију или имају могућност порицања. *Прикривене операције* (енг. *clandestine operations*) су операције које се спроводе на начин који обезбеђује тајност или прикривање. А тајна операција се разликује од прикривене операције по томе што је овде нагласак на прикривању операције, а не на прикривању идентитета, особе која стоји иза ње (Graham, 2016).

акцијама тј. кампањама су да су такве започете, континуиране и контролисане операције оне у којој снаге делују на тајни и прикривен начин у кратким временским периодима, затим да их одликује међуорганизацијска сарадња како оперативне природе, тако и са службама безбедности, међународна сарадња у циљу обављања обавештајних послова и да осујети непријатеља и сачува легитимитет акције Израелске одбране, да умањи легитимитет непријатељске акције, као и деловање у јавној перцепцији, економској и правној области као део напора да се смање способности и легитимитет непријатеља са потребом за приступачним и прецизним обавештајним подацима (Graham, 2016). Како Ајзенкот (*Chief of General Staff Lt. Gen. Gadi Eisenkot*) даје своје виђење о *другачијој ситуацији*: „У прошлости смо имали војску у једној од две ситуације, била је припремљена за рат, или је у рату. Али у овом тренутку ово није стварност. Не спремамо се за рат, а ми нисмо у рату. У другачијој ситуацији смо где држимо да цела кампања са различитим перцепцијама се ослања на службе безбедности и прикривене и отворене могућности да спречи јачање нашег противника, да покуша да ослаби непријатеља на начин који неће донети му убрзање" (Graham, 2016, p. 26). После изношења цитата Амоса Јадлина (*Amos Yadlin*), ово Ајзенкотово виђење (*Gadi Eisenkot*) такође је наглашено у Стратегији израелских одбрамбених снага где се још једном потврђује да је кључ свих активности у периоду *Кампање између ратова* управо активност служби безбедности, одакле би сви аналитичари на планети требали много да науче од државе која има можда и највише искуства по питањима супротстављања претњама по националну безбедност државе.

Са теоретског поимања одвраћања, Израел је можда постигао највише својим радом, где одмах предлаже и изградњу снага за *Кампање између ратова* где је потребно поступити на следећи начин. Потребно је да се „успостави координациони центар за операције кампања између ратова, а који укључује међуорганизацијске и међуминистарске елементе. Затим је потребно да се развију способности за тајне и прикривене операције за *Кампање између ратова*" (Graham, 2016, p. 44). С обзиром да је у операцијама овог типа увек ангажован велики број специјалиста из једне државе који нису запослени у једној организацији, центар који је наведен представља први корак у формирању снага док стварање способности за тајне и прикривене акције представљају класичан „занатски део" из сваке безбедносно интересантне струке, специјалности неопходне за реализацију оваквих операција.

Једна од таквих струка представља и сегмент познавања актуелних трендова информационо – телекомуникационих система. Сајбер сфера је једна од области одбране где се изводе овакве операције[7], офанзивне активности и прикупљање обавештајних података. Изградња снага у овој сфери се заснива на следећим радњама: „успостављање сајбер огранка који ће бити директно подређени штабу Начелника Генералштаба оружаних снага Израела за рад и изградњу сајбер способности. Тај огранак има обавезу планирања, организовања, спровођења сукоба у сајбер простору. Међутим, као посебна обавеза је дато развијање технолошке способности за сајбер одбрану свих оперативних система и одбрамбене способности система подршке – радна снага, логистика" (Graham, 2016, p. 44).

[7] Сајбер офанзивна операција (*STUXNET*) је пример офанзивне сајбер операције коју је спроводио Израел, а која је заједнички развијена са САД и циљано усмерена на иранске нуклеарне потенцијале – постројења, способности и др. (Graham, 2016).

Како би били побољшани услови рада и изградња могућих капацитета, неопходно је развити јединствен заједнички језик за командовање и контролу у свим штабовима израелских одбрамбених снага који делују или функционишу у сферама између ратова што ће бити спроведено кроз основане школе за командовање и управљање. Потребно је развити способност коришћења квалитетних служби безбедности, њених услуга – активности које предузимају, на свим нивоима операција: национална, стратешка и оперативна служба безбедности (њена активност). Изградња снага у области служби безбедности је заснована на следећим радњама: развијање и побољшање способности интегрисања информација, развијање способности држања суседне територије на основу обавештајних података неопходних за стварање циљева са високом прецизношћу у кратком временском периоду, праћење непријатељских доктрина, искоришћавање служби безбедности (њених активности, података), њено анализирање и чињење доступном на свим нивоима од штаба, команде округа, до тактичког нивоа у батаљонима и командама које испољавају силу као и потреба представљања слике стања непријатељских формација и мера ефикасности офанзивних напора израелских одбрамбених снага против њих. Неопходно је одржавање очувања основне приправности ради квалитетног одвраћања, уз очување механизама за убрзање неопходних набавки. Изградња снага у овом контексту ће се заснивати на следећим активностима: јачање стратешког и тактичког одвраћања путем сајбер ратовања, затим доступност података од служби безбедности као раног упозорења за покретање превентивних активности, као и способност превентивног удара у складу са индикацијама раног упозорења како би се осујетио покушај напада на Израел (Graham, 2016). Неопходно је још једном нагласити да основ деловања у кампањи између ратова чине поступање и подаци добијени од служби безбедности где је у једном стратегијском документу, први пут објављеном јавном документу у Израелу, наглашен значај необавештајних активности које предузимају службе безбедности.

3.1.3. Сајбер одвраћање и други инструменти одвраћања у прошлости и садашњости

Творац појма *меке моћи* у спољној политици, Џозеф Ај[8] (*Joseph S. Nye*) „амерички теоретичар, указује на измењено схватање природе моћи у савременом свету" (Путник, 2012, стр. 177). С обзиром на могућност државе да путем утицаја на друге наметне своју вољу путем примењивања демократије (политике унутрашње и спољне) или масовне културе и слично, а не војном и економском силом (што би представљало *тврду моћ*). Ај наглашава да то није могуће постићи искључиво *меком моћи*. Он у теорију међународних односа из тог разлога уводи још један термин – *паметну моћ*, која комбинује присиљавање, економски притисак и убеђивање. Ај наводи „да је информација увек била моћ, а да модерна информациона технологија шири информације много шире и брже него било када раније у историји. Због тога је значај информације као елемента моћи порастао. Ај истиче да се природа моћи променила у последњих педесетак година, а посебно након последње информатичке револуције која је рачунаре и интернет учинила неопходним у свим

[8] Џозеф Ај, професор међународних односа на Харварду у књизи из 1990. године, *Осуђени на вођство: промењива природа америчке моћи*, први помиње термин *мека моћ* (Путник, 2012). У својој књизи из 2004. године, *Мека моћ: пут успеха у светској политици*, Ај је увео појам *паметна моћ* који се односи на комбиновање *тврде и меке моћи* (Арежина, 2011).

областима живота. Нај истиче да ће нуклеарно одвраћање, оружане снаге у држави и стационирање трупа у иностранству бити важне и у информатичком добу, али неће бити довољне да осигурају националну безбедност" (Путник, 2012, стр. 177, 178). Овде видимо да је још 1990. године Нај наговестио трансформацију стратегије одвраћања, што би данас могли упоредити са стратегијом сајбер одвраћања и најавом потраге за другим инструментима одвраћања.

Рининг (*Sten Rynning*) пружа анализу о томе како је обновљено стратешко такмичење са РФ и Северноатлантским савезом, што је довело до развијања стратегија одвраћања у светлу разноликости стратешких перспектива међу државама чланицама Северноатлантског савеза. Северноатлантски савез перципира и реагује на ратовање нове генерације од стране РФ које у суштини представља стратегију принуде, врло често усмерену на информациони простор противника. Сукоби нове генерације користе оруђа у опсегу за убеђивање и одвраћање непожељне политике, а што је најбитније, у овој врсти сукоба се не прави разлика између рата и мира. Северноатлантски савез је констатовао више нових начина размишљања РФ о бројним политичким аспектима и то о отпорности друштва, побољшању сарадње служби безбедности, сајбер безбедности и потреби за брзим доношењем одлука. У Северноатлантском савезу је 2014. године основан Заједнички одсек за обавештајно – безбедносне активности, који представља један од механизама раног сазнавања намера РФ. Међутим, пропуст је што се у политичко – војном штабу Северноатлантског савеза не окупљају службе безбедности држава чланица већ се само координира, и оно што нуде државе чланице интегрише се у колективни преглед политике и деловања РФ. У погледу хибридних претњи ова координација је посебно спорна, јер сеје семе конфузије у савезничким информационим просторима. Северноатлантски савез је унапредио своју сајбер одбрану и побољшао координацију служби безбедности, али посебно је побољшана координација са Европском унијом везано за хибридне претње од 2016. године када је донешена заједничка декларација која води ка заједничком програму рада са Центром за одлучно супротстављање хибридним претњама, који се налази у Хелсинкију (*Centre of Excellence for Countering Hybrid Threats, located in Helsinki*). Северноатлантски савез, као одговор на анексију Крима од стране РФ, у 2014. години уводи комбиновање одвраћања *порицањем* (конфликт сиве зоне, отпорност друштва, реакција и напредовање распоређених снага да се супротставе ограниченом отимању земље) и одвраћање *казнама* (пун ланац реакција и снага које се могу распоредити, од конвенционалних до нуклеарних). Северноатлантски савез се у великој мери обавезао на одвраћање РФ кажњавањем. У Хладном рату, стратегија флексибилног одговора Северноатлантског савеза је одражавала политички компромис (Rynning, 2021).

Национална безбедност тако у садашњем времену „може да буде угрожена не само оружаним снагама, већ нападачи могу да буду владе, групе, појединци и други недржавни актери" (Путник, 2012, стр. 178) или они који се представљају као недржавни актери.

Наиме, у ери развоја нових технологија примат димензије сукоба више нису копно, ваздух, море, већ је то од пре пар година постала димензија сајбер простора. Велике силе (САД и РФ и друге државе) већ одавно имају формиране снаге, центре који се баве заштитом као и сукобима у сајбер простору. Генерални секретар Северноатлантског савеза, Јенс Столтенберг, 2018. године износи своје мишљење о начину тумачења члана 5. Оснивачког уговора Северноатлантског савеза по питањима сајбер напада са територије РФ. Генерални

секретар Североатлантског савеза, за који је свима добро познато да је предвођена САД, тумачи нападе у сајбер простору као нападе на чланице Североатлантског савеза. Зависно од карактера сајбер напада намера Североатлантског савеза је да искористи члан 5. и да све државе буду упознате са тим, што имплицира да овај члан неће бити аутоматски примењиван за сваки сајбер напад. Међутим, генерални секретар није хтео да саопшти конкретне услове при којима ће бити искоришћен овај члан. Оно што је пропратило све сајбер нападе неколико година уназад су биле углавном оптужбе највиших званичника држава САД, Француске и Велике Британије да су починиоци сајбер напада из РФ, као и деманти из РФ (већ дужи низ година у етру су тотално контрадикторна саопштења и на Западу и на Истоку). Само пар година касније, 2021. године, поред наведене четврте димензије сукоба (сајбер простора), Североатлантски савез је додао и пету димензију сукоба (у свемиру), а која би могла да буде проширење члана 5. за његово активирање. Ту се наводи да „би чланице Алијансе биле спремне да одговоре и на нападе у свемиру и из свемира" (Stoltenberg, 2018; 2021, p. 1).

Соесанто и Смитс (*Stefan Soesanto & Max Smeets*) сајбер одвраћање сагледавају у војном концепту и оно према њима има најмање три различита значења. Може се односити на одвраћање од (војног) напада, затим употребу (војних) средстава за одвраћање (војних) сајбер напада и употребу (војних) сајбер средстава за одвраћање као (војни) сајбер напад. Научници се тренутно не слажу у ком степену је то генерално могуће одвратити непријатељски сајбер напад, вероватно полазећи од констатације да сајбер простор садржи обиље учесника који имају приступ офанзивном сајбер оружју. Неки сматрају да је стратешка вредност штете нанете сајбер нападима генерално ограничена. Претње од сајбер напада тако немају довољно могућности за ефикасно одвраћање. Заговорници сајбер одвраћања, углавном говоре о следеће четири логике одвраћања и то: одвраћање порицањем (што је синоним за сајбер безбедност), одвраћање казном (трошкови ће надмашити користи), одвраћање испреплетаношћу (међузависност може дестимулисати државе да покрену сајбер нападе), као и одвраћање делегитимизацијом (смањити бојни простор да само обухвата војне борце). Сајбер простор је можда препознат као нови домен ратовања, али изван војске корисност сајбер напада и сајбер одбране у подршци одвраћању је још увек неизвесна. Политички мотивисани сајбер напади са стратешким утицајем су малобројни, већина докумената јесте високо поверљива, али постоји мали приступ сајбер оператерима и постојеће војне сајбер организације су тек у развоју. Тако, Соесанто и Смитс констатују четири будућа правца истраживања за сајбер одвраћање: сајбер одвраћање у свеобухватнијим ставовима одвраћања у контексту такмичења у више домена, затим већи фокус на техничке аспекте на оперативном и тактичком нивоу, па већи нагласак на компетентности и последње, зауздати и отупити непријатељску агресију у сајбер простору (Soesanto & Smeets, 2021). У овој области нема консензуса између научника.

Студије о борби против тероризма након напада 11. септембра 2001. године фокусирале су се на питање да ли се недржавни актери могу одвраћати. Шамир (*Eitan Shamir*) за спречавање претњи од тероризма проналази везу између одвраћања и насилних недржавних актера. Шамир наводи да је Израел развио концепт одвраћања од насилних недржавних актера. Он укључује аспекте одвраћања чији је циљ обуздавање способности противника. Поред обуздавања, Шамир наводи и да је циљ на едукацији у приступу заснованом на процесу који предвиђа континуирани однос између одвраћајућег и одвраћаног. Ставови да је терористичке групе (нарочито верски мотивисане) тешко

одвратити, садржани су углавном у следећим факторима: оне често нису монолитне организације, састоје се од прикривене мреже аутономних ћелија, не постоји обавезујући вођа/шеф/руководилац, особа са којом би представник државе могао да комуницира, затим када говоримо о идеологијама оне искључују нормалне дипломатске преговоре и сл. Шамир потенцира одвраћање које у овом сегменту није могуће остварити апсолутно, већ да треба рестриктивно приступати одвраћању. Штавише, не очекује се да ће ефекат одвраћања произаћи из симболичних напада, већ од поновљених протеста, одговора, кад год је норма прекршена (тзв. приступ кошења траве). Рестриктивно и кумулативно одвраћање од насиља недржавних актера је више инспирисано криминолошким схватањима појма, а не хладноратовским концептима апсолутног одвраћања (Shamir, 2021). Као и у великом броју животних примера, тако и за овај облик одвраћања можемо рећи да се стратешко искуство и култура (како наглашава Шамир) неће једноставно пресликати са једне државе на другу. Овоме бисмо могли додати и комплетну економску, војну, политичку и друге моћи које имају важан утицај на концепте одвраћања и важно је знати да се одвраћање неће једноставно пресликавати са једне културе на другу. Практично, претња санкцијама економски самосталној држави неће дати резултате какве даје за државе које нису самосталне, а као по одређеној дефиницији никада неће бити употребљавана једна врста активности у одвраћању, већ низ активности у које су укључене или којима руководе службе безбедности ради остварења поличких циљева елите једног друштва – јуче државе, данас и сутра можда искључиво само назови елите одређеног друштва.

Део теоретичара дефинише хибридни рат као брак између конвенционалног одвраћања и тактике побуњеника. Питање је да ли се уопште ради о новом облику ратовања или о стратегији коју државе користе ради остварења првенствено политичких циљева како у миру тако и у рату, а најчешће применом субверзивних активности (необавештајних активности). Хибридни рат експлоатише националистичке идентитете, чиме се прикрива одговорност извршиоца и чак добија политичка подршка међу страним посматрачима. Стратегија РФ има за циљ да ослаби спремност Североатлантског савеза и да следи сопствене претње одвраћања (као и обрнуто). Војни стратези су одавно били свесни како страну у сукобу треба ради постизања победе побунити ради лакшег преовладавања тим противником. Државе избегавају директне војне сукобе, а они би користили само великим силама. Сходно томе, прикладније су суптилније и индиректне технике приступа решавању проблема. Ове технике укључују коришћење пропаганде за мобилизацију подршке побуњеницима и за деморалисање непријатељских снага као и напад на слабе тачке супротстављених снага.

Различите су технике које се могу примењивати у хибридном рату: ту је *пропаганда*, која представља утицај на ставове које имају чланови циљног друштва и служи да се омета способност циљне групе да се ослања на подршку јавности у спровођењу своје политике и мобилисања њених ресурса. Следећа техника је *шпијунажа* којом агенти тајно прикупљају обавештајне податке како би се сукобљеној страни обезбедила предност у принудном преговарању. Поред наведеног, агенти би могли ширити намерно лажне информације међу несумњиво члановима јавности у вези са реалним намерама појединих организација или стварању неспоразума и раздора унутар циљног друштва када га још нема. Следећа техника је *криминални поремећај* при чему агенти страна у сукобу учествују у нападима, сајбер нападима, саботажама или киднаповањима и другим врстама субверзија. Неговање *пете*

колоне, или групе појединаца, које обично делују прикривено, који су уграђени у много већу популацију коју треба да наруше. Употреба пете колоне као *необележених војника* омогућавају да се попуне контролни пунктови, заузму владине зграде и други објекти, лица и сл. од стратешког значаја (до одређеног момента). Страна у сукобу би могла покренути *граничне окршаје* како би узнемирила другу страну и испитала њене слабости, затим наставила са исцрпљивањем снага и ресурса и одвајањем од тежишта дејства кроз употребу гериле. Савез Совјетских Социјалистичких Република је применио ове технике одмах после Другог светског рата, спонзорисањем комунистичких покрета у Европи и на другим локацијама да поткопају капиталистичко уређење. Савремена војна доктрина РФ наглашава потребу да се одговори и на спољне и унутрашње претње, не само других великих сила, већ и субверзивних организација делујући у областима под контролом РФ. Војни теоретичари су још пре више деценија били свесни да су САД стекле предност у прецизном удару и информационо – комуникационим технологијама и да би државе могле постати предмет информационог рата. Почетне фазе рата би укључивале кампање дезинформисања. Информациона супериорност је постала неопходна у савременом ратовању (Lanoszka, 2016). С обзиром да се у теоретском одређењу хибридног рата још увек „лута" и нема свеобухватне дефиниције ове појаве, разлог је више што многи људи користе ово одређење неприлагођено ономе што се стварно догађа око њих. Није искључено да је у току део операција које се тајно споводе или необавештајних активности служби безбедности. Када се догађа наведено, тада треба да га и назовемо правим именом: обавештајним, контраобавештајним или необавештајним активностима служби безбедности које су мање – више присутне од када и постоје службе безбедности, осим техника прилагођених напретком нових технологија. Када употребљавамо појмовно одређење рат, тада треба поћи и од његовог теоретског одређења, па и правног, нормативног и сагледати да ли је овај појам хибридни рат адекватно одређен (Lanoszka, 2016). Професор Кајтез Илија је изнео[9] податак да су још после Другог светског рата започеле припреме за шпијунирање широм планете од стране САД и да су 1970. године службе безбедности САД, Централна обавештајна агенција и Агенција за националну безбедност, као и служба безбедности Немачке, Федерална обавештајна служба (нем. *Bundesnachrichtendienst*) склопиле тајни споразум о незаконитом глобалном прислушкивању већег дела планете (тачније 130 држава и Уједињених нација) и да се операција звала Рубикон – *Rubicon* (кодни назив за Федералну обавештајну службу – прелазак на Рубикон значи још из времена Јулија Цезара предузимање неопозивог корака који почиње у одређеном курсу; симболика имена, мада је операција првобитно имала други кодни назив Ризница – *Theasaurus*) док је тајни назив операције за Централну обавештајну агенцију био *Минерва* и већи део ових активности је реализован преко фирме Крипто АГ – *Kripto AG* у Швајцарској (коју је наводно основао Хагелајн /*Boris Hagelajn*/ који се бавио шифровањем, а где је ова фирма остваривала велику добит у раду те је новац наводно усмераван у црне фондове служби безбедности САД и Немачке, односно економске активности ових служби). Фирму су основале америчка Централна обавештајна агенција и немачка Федерална обавештајна служба, а у њој је своје власништво продала Федерална обавештајна служба тек септембра 1993. године након хапшења Ханс Билера (*Hans Biler*) у Техерану где је провео

[9] У телевизијској емисији на јавном сервису Републике Србије, дана 21. августа 2022. године.

девет месеци када је Федерална обавештајна служба изгубила подршку Владе Немачке за ову операцију, док су САД наводно наставиле недозвољене активности све до 2018. године. Почетком 2020. године Питер Милер (*Piter Miler*) је снимио документарни филм о овој операцији за други програм телевизије у Немачкој где се помиње и Социјалистичка Федеративна Република Југославија као држава која је била купац уређаја за шифровање још 1957. па 1978. године, а и немачки и швајцарски јавни сервиси *ZDF* (Јавни телевизијски канал, Немачка) и *SRF* (швајцарска јавна радио – телевизија), као и амерички Вашингтон пост. Део држава је открио да се ради о уређајима који су читљиви за другу страну, између осталих и Аустрија и Социјалистичка Федеративна Република Југославија. С обзиром да се ради о једној изузетно великој операцији, планетарног нивоа, треба бити опрезан у сагледавању ових података које уступају поново исти актери који су све време и били учесници у низу, између осталих и необавештајних активности САД, Немачке и Швајцарске, те да се не ради о припреми нове или већ зановљене старе операције.

Јакобсен (*Peter Viggo Jakobsen*) одвраћање сагледава у још једном облику, и то оном који обухвата како државне, тако и недржавне актере, а ради се о мултинационалним операцијама. Ову врсту операција Јакобсен сагледава кроз реализацију напада на мировне снаге (оне које су биле сачињене од састава држава са запада) које су биле распоређене на територији бивше Социјалистичке Федеративне Републике Југославије. Мировне снаге делују у променљивом контексту у којем се руше строга разграничења између одвраћања и принуде. Следеће факторе треба узети у обзир, претња у принуди може да покаже способност да победи противника брзо уз малу цену; затим рок за усаглашеност треба да створи осећај хитности; битан фактор је уверавање да неће бити додатних захтева после усаглашености и коначно укључивање позитивних подстицаја за смањење трошкова усклађености. Неопходност одвраћања и приморавања у исто време различитих учесника у и изван бојног поља. Јакобсен тако у мировним операцијама разликује четири групе учесника одвраћања (позитивних и негативних) и то: борци који користе силу на бојном пољу; затим савезници који пружају материјалну подршку борцима; присталице бораца које блокирају деловање у регионалним или глобалним институцијама; као и др. лица, пролазници, на бојном пољу на глобалном нивоу, који не испољавају борбена дејства. Јакобсен закључује, да би било успешно одвраћање, учесници одвраћања не могу се ослањати само на претње и употребу силе то није довољно. Према њему, неопходно је допунити њихово дејство, да употреба принуде буде допуњена са убеђивањем и подстицањем, осмишљавањем, спровођењем стратегије утицаја која би се у потпуности ослонила на све ове три компоненте (Jakobsen, 2021). У овом истраживању, Јакобсен је потврдио да специфичност одређених култура, држава, појава, а посебно у овом случају активности, носи своје карактеристике, факторе који чине јединственим конкретно одвраћање тако да и шаблон примене у другим случајевима није адекватан пут односа према одвраћању.

3.2. КОНЦЕПТ ОДВРАЋАЊА РУСКЕ ФЕДЕРАЦИЈЕ

Важно је напоменути да је у некадашњем Савезу Совјетских Социјалистичких Република постојао концепт који је називан *маскировка*[10] и подразумевао је „преварантски

[10] *Маскировка* је термин на руском који је компликовано превести на други језик, јер обухвата велики број енглеских речи и то следеће: камуфлажа, прикривање, обмана, имитација, дезинформација, тајност, лукавство,

концепт у којем учествује цели народ. То није био само термин коришћен у војне сврхе већ се практиковао у читавом руском друштву. Инструменти који су коришћени у овом концепту маскировке су дипломатија, информисање, распоређивање оружаних снага и економске мере" (Bouwmeester, 2020, p. 24). У прошлом веку маскировка је подразумевала да противници са изманипулисаним утисцима и идејама буду наведени да погрешно процене ситуацију, затим сви покушаји маскирања морају бити уверљиви, а понављање обрасца маскировке треба да се избегава и неопходан је континуитет маскировке зато што се ради о активностима које се предузимају не само у рату већ и у миру. Нису само Совјетске власти користиле маскировку у прошлости, већ је и данас користи РФ. Данашња маскировка се наводно спроводи кроз лукаво коришћење перцепција које замагљују слику како би јавно мњење видело овај поглед као исправан, а с циљем да се оправдају политички поступци. У једном периоду је коришћен термин *стратешка маскировка* што је подразумевало средство за примену дезинформација против свих нивоа противника и ширег јавног мњења, политичког, војног. Коришћење, код дела теоретичара, концепта обмане под називом „маскировка 2.0" у РФ (да би се разликовала од *маскировке* за време Савеза Совјетских Социјалистичких Република), која се ослања на тајну дипломатију и велики избор других тајних припрема политичких, војних, економских и информационих. Ова савремена употреба маскировке обухвата пропаганду, медијску манипулацију и употребу обмане како би се остварио утицај РФ на сваки могући начин. Да би могли сумирати напред наведено везано за маскировку, важно је констатовати да модерна маскировка представља маскирање сопствене намере, а да том приликом видљиве активности које се предузимају, често указују на нешто друго и намерно пружају дезинформације за стварање изненађења и стварање перцепција које су изманипулисане (Bouwmeester, 2020). Циљ маскировке је изненадити непријатеља, противника или створити изманипулисане перцепције. Руске власти су дорађивале своју маскировку, па је самим тим концепт неколико пута прилагођаван новим временима. Данашње манифестације маскировке се користе углавном у информационој сфери. У наредном делу истраживања ћемо сагледати концепте одвраћања РФ са освртом на ангажовање у информационој сфери.

3.2.1. Одвраћање у стратегијама председника Руске Федерације

Одвраћање је појам који је врло нејасан и тежак за мерење. Да би се спровело испитивање примене одвраћања од стране САД или РФ, неопходно је применити теоријски оквир одвраћања. У следећем поглављу одредићемо значење појма уз помоћ добро познатих теорија одвраћања. Примењујући ове теорије у емпиријском истраживању, надам се да ћемо успети да сагледамо да ли и у којој мери САД, односно РФ, спроводи одвраћање и попуштање.

У *Речнику српског језика* стратегија је дефинисана као „грана ратне вештине која се бави припремом и вођењем рата у целини. Уопште представља вештину вођења борбе, супротстављања, деловања, наступања. Док стратегијски се односи на стратегију и стратеге, важан за спровођење ратног плана, на начин стратега, како стратег да поступи" (Вујанић и сар., 2011, стр. 1251). У РФ председник доноси Указ о проглашењу Стратегије националне

финте, диверзија и симулација. Мада део ових речи, појмовно се преклапају, совјетски, па касније и руски појам ове речи, речи маскировка, представља више од збира ових енглеских речи – појмова (Bouwmeester, 2020).

безбедности (енг. *National Security Strategy* – рус. *Стратегия национальной безопасности*) који представља основне смернице за поступање свих сегмената друштва и државе.

Стратешко одвраћање описано је у војно – енциклопедијском речнику Министарства одбране РФ и представља координирани систем војних и невојних (политичких, дипломатских, правних, економских, идеолошких, научно – техничких и др.) мера предузетих узастопно или истовремено, све са циљем одвраћања војних акција које повлачи за собом штету стратешког карактера. Стратешко одвраћање је усмерено на стабилизацију војно – политичке ситуације, како би се утицало на противника у унапред одређеном оквиру, или за деескалацију војног сукоба. Предмети на које треба утицати кроз стратешко одвраћање могу бити војно – политичко вођство и становништво потенцијалне противничке државе (или коалиције држава). Стратешке мере одвраћања спроводе се континуирано, како у миру тако и у рату. Концепт стратешког одвраћања се стога заснива на низу различитих извора. Компоненте концепта, односно његове делове чине нуклеарно одвраћање, ненуклеарно одвраћање и невојно одвраћање. Концепт је још увек у фази израде и његова корисност је још увек у употреби о којој се расправљало међу руским теоретичарима. Ипак, оваква комбинација идеја пружа увид у то како РФ може да следи своје стратешке циљеве у будућности (Bruusgaard, 2016).

Стратегијски развој у РФ је јасно уређен, почевши од Устава РФ, преко Федералног закона о безбедности, у коме се, између осталог, дефинише да Председник утврђује Војну доктрину РФ. У РФ се безбедност посматра као предуслов развоја државе и друштва (Форца и Стојковић, 2014). Стратегија националне безбедности РФ усвојена је 12. маја 2009. године и односи се на период до 2020. године. Основна карактеристика ове стратегије је да се сматра покретачким фактором за развој националне моћи (економије, квалитета живота становника, политичке стабилности, јачања одбране и државне безбедности...). Треба имати у виду да РФ велику пажњу у војној стратегији обраћа на државе у блиском окружењу (Форца и Стојковић, 2014). Тако је руска војна интервенција 2008. године у Грузији имала за циљ да пошаље поруку САД и свим земљама, бившим чланицама Савеза Совјетских Социјалистичких Република, да РФ није спремна да толерише провокације по својим рубним подручјима, и да је спремна да поврати свој утицај и оружјем, ако то буде било неопходно (Форца и Стојковић, 2014).

У првом Концепту националне безбедности РФ, уведеном указом председника РФ од 17. децембра 1997. године *N 1300*, термин „национална безбедност" није дефинисан. Међутим, битно значење израза „безбедност" дато је у првом руском закону „О безбедности" 1992. године у којој је дефинисана безбедност – национална безбедност (рус. *безопасность – Статья 1*.) као „стање заштите виталних интереса појединца, друштва и државе од унутрашњих и спољашњих претњи" (Закон РФ „О безопасности", 1992, p. 1).

Стратегија националне безбедности РФ (енг. *National Security Strategy* – рус. *Стратегия национальной безопасности*) је „основни документ стратешког планирања који дефинише националне интересе РФ и стратешке националне приоритете, циљеве, задатке и мере у сфери унутрашње и спољне политике усмерене на јачање националне безбедности РФ" (The Russian Federation's National Security Strategy, 2009, p. 2). Стратегија је предвидела дугорочне националне стратешке интересе и то јачање одбране државе, обезбеђивање неповредивости уставног поретка, суверенитета, независности и националног и територијалног интегритета РФ, јачање политичке и друштвене стабилности, развој

демократских институција, подизање животног стандарда, побољшање здравља становништва и осигуравање стабилног демографског развоја државе, очување и развој културе и традиционалних руских духовних и моралних вредности, повећање конкурентности националне економије, учвршћивање статуса РФ као водеће светске силе, чије акције имају за циљ одржавање стратешке стабилности и обострано корисних партнерстава у полицентричном свету. Национални интереси се осигуравају спровођењем следећих стратешких националних приоритета: „национална одбрана, државна и јавна безбедност, економски раст, наука, технологија и образовање, здравствена заштита, култура, екологија живих система и рационално коришћење природних ресурса, стратешка стабилност и равноправно стратешко партнерство" (The Russian Federation's National Security Strategy, 2009, p. 7). Стратешки циљеви националне одбране треба да се постигну у оквиру спровођења војне политике кроз стратешко одвраћање и спречавање оружаних сукоба, побољшање војне организације државе и облика и метода за распоређивање Оружаних снага РФ, других трупа, војних формација и служби, повећавајући спремност РФ за мобилизацију и спремност снага и средстава цивилне одбране. Међусобно повезане политичке, војне, војно – техничке, дипломатске, економске, информационе и друге мере развијају се и спроводе како би се осигурало стратешко одвраћање и спречили оружани сукоби. Ове мере имају за циљ одвраћање употребе оружане силе против РФ и заштиту њеног суверенитета и територијалног интегритета. Стратешко одвраћање и спречавање оружаних сукоба постижу се одржавањем капацитета за нуклеарно одвраћање на довољном нивоу, док Оружане снаге РФ и друге трупе и војне формације и тела наведено постижу одржавајући на потребном нивоу функционалну и борбену оспособљеност. Да би осигурала стратешку стабилност, РФ чини све потребне напоре да одржи на најнижем нивоу потенцијал одвраћања у сфери стратешких офанзивних наоружања (The Russian Federation's National Security Strategy, 2009). Анализом најбитнијих сегмената ове стратегије можемо констатовати да се стратешко одвраћање у РФ поред развоја и опремања нуклеарним и офанзивним наоружањем као тежишним мерама одвраћања, спроводи и неким другим мерама које су само наведене, а које представљају најобимнији, најкомплекснији и можемо рећи најбитнији сегмент стратешког одвраћања. Ради се о политичким, војним, војно – техничким, дипломатским, економским, информационим и другим мерама (што ћемо детаљно истраживати у наредном делу рада).

Стратегија националне безбедности РФ из 2009. године је зановљена 2015. године (*Стратегия национальной безопасности Российской Федерации, 2015*) где је на њене измене из 2009. године утицало више чинилаца. Наиме, у овом периоду се догодио низ битних чинилаца: „повратак Крима РФ 2014. године, унутрашњи сукоби – грађански рат у источној Украјини, у регији Донбас (Доњецк и Луганск), снажно појављивање и утицај Кине на међународној сцени и консолидовање односа са РФ, укљученост западних држава у рат на северу Африке (тзв. Афричко пролеће) од 2011, посебно у сукобе унутар Сирије и Либије од 2014. године, размештање противракетног система од Североатлантског савеза у Европи, криза која је захватила Европску унију од 2015. године, позната као *миграмтска криза*. У Стратегији националне безбедности РФ из 2015. године, изазови, ризици и претње националној безбедности су наведени у оквиру другог и четвртог поглавља, тачке 7 – 29 и посебно тачка 43" (Форца, 2022, стр. 59).

Анализирајући у ова два документа (*Табела 2*) регистроване изазове, ризике и претње од стране РФ, можемо да констатујемо да су исти врло реално евидентирани и достављени

јавности на увид, без сакривања и лажирања истих, што најбоље потврђују актуелна збивања у РФ, Украјини и др. догађаји који су сада актуелни, у суштини су ништа друго него таксативно наведени у овим документима пре пар година. Почев од проблема са Украјином, затим сајбер и војне претње, економске кризе, итд. Када све сагледамо из ове табеле, можемо да закључимо да се ради о великом броју области које су из надлежности служби безбедности, посебно необавештајних активности према којима би требало да се спроводи одвраћање.

Табела 2. Табеларни приказ изазова, ризика и претњи у стратегијама националне безбедности РФ из 2009. и 2015. године.

Стратегија националне безбедности РФ из 2009. године	*Стратегија националне безбедности РФ из 2015. године*
ширење Северноатлантског савеза ка границама РФ	обојене револуције и корупција
глобални тероризам	повећање броја земаља које поседују нуклеарно оружје
деловање транснационалних криминалних организација и група и пораст корупције	пораст биолошког и хемијског оружја
милитаризацији свемира	Северноатлантски савез претња и процес милитаризације у земљама које окружују РФ
екстремистичке делатности националистичких, религиозних, етничких и др. организација	проблем Украјине и пораст нестабилности у Европи
делатности специјалних служби и организација страних држава	суздржавање од производње нуклеарног оружја
сајбер и војне претње	информациони рат
сукоби у окружењу	угроженост економске стабилности
економска криза	пад у развоју напредних технологија
недостатак питке воде	јачање сиве економије
пролиферација конвенционалног оружја и оружја за масовно уништење	пораст корупције и криминалних активности пре свега у неразвијеним земљама
размештања ракетних система	коришћење војне снаге у случајевима када је нарушена безбедност националних интереса
	делатности специјалних служби и организација страних држава

Извор: Миленковић, 2020, стр. 74.

Стратегија националне безбедности РФ из 2021. године (*Стратегия национальной безопасности Российской Федерации, 2021*) је једноставно морала да замени стратегију из 2015. године, јер се догодило доста тога у међународним односима, што је утицало на то да РФ приступи усвајању новог документа. Навешћемо неколико битних догађаја: „у САД је на председничким изборима 2016. године победио Доналд Трамп, који је и у Стратегији националне безбедности САД из 2017. године као главне противнике означио РФ и Кину; затим Европска унија је 2016. године усвојила Глобалну стратегију за заједничку спољну и безбедносну политику и отпочела процес иступања Уједињеног Краљевства из Уније, који је формално завршен 2020. године, па је од Северноатлантског савеза у својим стратешким концептима означио РФ као главни реметилачки фактор безбедности у свету и наставио са јачањем војних ефектива у земљама суседима, као и са јачањем противракетног штита. САД су отпочеле отворене сукобе с Кином у домену економије и РФ по питању утицаја на безбедност Европе и наставиле са увођењем санкција РФ, чему су се придружиле и друге западне државе због сукоба с Украјином, због Крима и из других разлога" (Форца, 2022, стр.

62, 63). Одвраћање у овој стратегији из 2021. године је одређено у тачки 40. која наводи спровођење војне политике *стратешким одвраћањем* где ће поред оружаних снага РФ бити ангажоване и друге трупе, војне формације и органи. Наглашена је потреба одржавања довољног нивоа способности (између осталих) нуклеарног одвраћања. Посебно је интересантан део прописан у тачкама 41–47, *Државна и јавна безбедност,* као и 48–57 тачке *Информациона безбедност* где је децидно, врло детаљно идентификован већи део необавештајних активности и предвиђен начин превентивне заштите од истих, односно мере – задаци које би требало да предузимају надлежни органи ради одвраћања у свом делокругу рада тј. додељеним надлежностима (Стратегия национальной безопасности Российской Федерации, 2021*).*

Војна доктрина РФ (*Военная доктрина Российской Федерации*) је систем ставова званично прихваћених у држави о припреми за оружану одбрану и оружану одбрану РФ. На основу анализе војних опасности и војних претњи РФ и интересима њених савезника, Војна доктрина формулише главне одредбе војне политике и војно – економске подршке за одбрану државе. Војна доктрина прописује војне мере заштите националних интереса земље и интереса својих савезника тек након исцрпљивања могућности коришћења политичких, дипломатских, правних, економских, информативних и других инструмената ненасилне природе. Тачка 8. војне доктрине под параграфом м) дефинише систем ненуклеарног одвраћања – да је то комплекс спољнополитичких, војних и војнотехничких мера усмерених на спречавање агресије на РФ ненуклеарним средствима. У тачки 21. војне доктрине, једна од предвиђених мера је и одржавање глобалне и регионалне стабилности и потенцијала нуклеарног одвраћања на довољном нивоу (Военная доктрина Российской Федерации, 2014). У овом делу истраживања је издвојена само суштина одвраћања према војној доктрини која се у делу сегмената доста поклапа са Стратегијом националне безбедности РФ, али и наглашава ненуклеарно одвраћање, као и друге инструменте ненасилне природе.

3.2.2. Концепти стратешког одвраћања Руске Федерације после Хладног рата

Овај део истраживања бисмо могли започети изјавом генерала Валерија Герасимова (*Valery Gerasimov*), Начелника Генералштаба оружаних снага РФ: „Данас је очигледно да граница између мира и рата се замагљује” (Roberts, 2020, p. 19). Теоретичари дефинишу *сиву зону* (енг. *gray zone*) као део спектра сукоба који не укључује оружана непријатељства. Даље, у одређењу сиве зоне, наглашавају се руске *активне мере* против западних грађана, између осталих. У једном смислу, то је зона мира, с обзиром на одсуство рата. Али није мирно, утолико што је сукоб у току, укључујући и разне врсте војне акције. У извесном смислу, термин сива зона обухвата стару идеју: тражење предности без трошкова и ризика рата. Противници Запада поново су осмислили ратовање и поново је осмишљен сукоб. Каталог активности руске сиве зоне је импресиван и алармантан. Укључује, на пример, *активне мере* против циљева утицаја, са циљем убиства такозваних државних непријатеља, мешање у западне изборне процесе, информациону конфронтацију стратегија, акције за замрзавање сукоба око његове периферије и (поновно) потврђивање утицаја у регионима под утицајем САД. Такве активности се усклађују добро са примарним циљевима велике руске стратегије како је дефинисао Председник Владимир Путин. Москва и Пекинг очигледно желе да регулишу регионалне проблеме унутар којих се следе корак по корак, али увек на начин који пада испод прага војног одговора од стране САД и/или њихових савезника. Ово је стратегија

„скуване жабе” која настоји да избегне „кулминацијске тачке” и уместо тога се ослања на ометање и поделу унутар демократија ради промене чињеница на терену. Стратешки, одозго према доле потребан је приступ. Требало би да се гради на три главне идеје. Прво, САД и њихови савезници могу подржати постојећу регионалну безбедност, наручује, консолидује добитке и селективно проширује и продубљује те налоге одржавајући привржености колективној безбедности, слободној трговини, и заједничке вредности. Друго, они могу временом променити стратешку равнотежу, утицати на снажније конкурентске стратегије у науци, технологију и друге секторе, чиме се нагриза присилни потенцијал противникове војне способности. Треће, САД и њихови савезници могу створити прилику за обнову и побољшање политичких односа (Roberts, 2020). Када читамо овај део написаних необавештајних активности, које износи овај теоретичар са Запада (био у Обаминој администрацији и на још доста државних дужности) о руским мерама, наравно да је све то истог, уколико не и много ширег спектра у службама безбедности, односно необавештајним активностима које је изводио и изводи Запад (САД).

Многи западни аналитичари заокупљени су тиме да РФ планира операције *хибридног ратовања* против чланица Североатлантског савеза. Као што је наведено у претходном делу истраживања о Војној доктрини РФ, сам термин *хибридног рата* није део руске војне доктрине. Када се изјашњавају руски аналитичари, за њих је *хибридни рат* западна конструкција док је у Стратегији националне безбедности и у теоријској расправи у употреби шири концепт, *стратешко одвраћање*. Овај концепт је део званичне стратегије и битан је за анализу садашње и будуће безбедности и одбрамбене политике РФ. Можемо закључити да је стратешко одвраћање концепт који обухвата оно што други називају доктрином *хибридног ратовања* РФ, руском способношћу за принудом (The Russian Federation's National Security Strategy, 2009). Тај концепт, *стратешко одвраћање* је много шири од замишљеног западног концепта одвраћања. Мада у свом називу има одвраћање, он није потпуно одбрамбени, већ садржи како одбрамбене тако и офанзивне, нуклеарне, ненуклеарне и невојне алате за одвраћање. Карактеристика им је да се они користе и у доба мира и рата. Представља низ поступака, мера суздржавања, одвраћања и принуде. У овим активностима се примењују сва расположива средства за одвраћање или доминирање сукобом.

Можемо констатовати на основу ове компарације (*Табела 3*) изазова, ризика и претњи наведених у стратегијским документима САД и РФ, да је анализираним документима заједничко то да су као безбедносне претње код ових великих сила препознати тероризам, организовани криминал, пролиферација оружја за масовно уништење, регионални сукоби и слабе државе које могу бити узрок сукоба ширих размера, сајбер напади, илегалне миграције и биолошке претње (Миленковић, 2020). Поред заједничких претњи, њих карактерише и заједничка оптерећеност једне другом, односно посвећеност једне другој и опасностима које једна за другу представљају (Миленковић, 2020). Наведене појаве су у фокусу интересовања рада служби безбедности САД и РФ те из наведеног разлога није могуће квалитетно сагледавати ова и слична документа без сагледавања места и улоге, односно утицаја који испољавају службе безбедности на поменуте изазове, ризике и претње (како у њиховом стварању и/или установљавању и супротстављању истим).

Табела 3. Табеларни приказ изазова, ризика и претњи у стратегијско – доктринарним документима САД и РФ.

Стратегија националне безбедности САД из 2017. године	*Стратегија националне безбедности РФ из 2016. године*
ревизионистичке силе Кина и РФ	глобалне нестабилности
отпаднички режими Северна Кореја и Иран	нуклеарна безбедност
радикалне исламске терористичке организације	пролиферација конвенционалног оружја и оружја за масовно уништење
криминалне организације	корупција
поседовање нуклеарног оружја од стране *лаких режима*	размештање ракетних система
експанзија тероризма	западна подршка рушењу Украјинске владе
порозне границе САД	обојене револуције
мигрантска криза	биолошко оружје
опасности од сајбер напада	Североатлантски савез претња
пролиферација оружја за масовно уништење	информациони рат
биолошке претње	природне катастрофе

Извор: Миленковић, 2020, стр. 77.

Стање у држави је приморало РФ током 1990. године и касније да се првенствено ослања на одвраћање, а нарочито на нуклеарно одвраћање од претњи безбедности. Велике промене у међународним војскама, политичка ситуација и технолошки развој изнудили су преиспитивање улоге руског стратешког наоружања у глобалном и регионалном одвраћању. Одвраћање је доспело у први план руске стратешке мисли, са употребом доступних алата. Неколико фаза може се идентификовати у еволуцији, после Хладног рата. Можда је размишљање о ратном одвраћању било прво питање које се постављало. Руски теоретичари су након демонстрација ваздухопловних снага САД и способности прецизног удара 1990–их, врло одговорно постављали питање како да нуклеарним оружјем одврате конвенционалне претње. Када се једна сила попут САД или Североатлантског савеза посматрала у том периоду, можемо да констатујемо да је ово стварно био озбиљан проблем, јер је РФ у том периоду озбиљно заостајала у квалитету у конвенционалним способностима. Одговор на овај изазов, према западним научницима, био је настанак теорије о деескалацији 1999. године у покушају да се искористе нуклеарне способности на најефикаснији могући начин против конвенционално надмоћнијег противника. Следеће је надокнађивање конвенционалне инфериорности, што је теоретичаре током 2000–их довело до фокуса на то како се могу користити нуклеарне и конвенционалне способности у комбинацији, ради квалитетнијег одвраћања, како од конвенционалних тако и од нуклеарних претњи. Период од 2009. године и доношења Стратегије националне безбедности РФ уводи нови термин, *стратешко одвраћање* што доводи до ширења размишљања о стратешком одвраћању, да се укључе ненуклеарне и невојне компоненте. Ограничена ефикасност нуклеарног оружја у одвраћању од конвенционалног и све више присутне нетрадиционалне претње безбедности дате су у руским разматрањима. Нуклеарни концепт одвраћања у савременим изазовима и претњама је био приморан да се надогради. Неколико је претњи које РФ потенцира: амерички војно – технолошки напредак – посебно, балистичко – ракетна одбрана. Наведено се доживљава као поткопавање руских стратешких нуклеарних снага. Следеће је све распрострањеније, опасније, невидљивије и делотворније по безбедност државе – невојне претње руској

безбедности; претње руској економској бази ресурса и политичкој кохезији. Ништа мање битне нису претње у информативној и културној сфери (супротстављање дезинформацијама, „фалсификовање историје", подривање историјске, духовне и патриотске традиције на пољу одбране државе и др.), као и информационо – телекомуникационој сфери (сајбер напади и др.). Савремени рат све више бира невојно оруђе за сукобе између држава. Нове претње приморавају РФ да размишља о томе како да се супротстави новим претњама, а сходно захтевима политике, на оспособљеном кадру је да наведено спроведе у дело расположивим савременим средствима; услови пружају огромне могућности у том погледу (Bruusgaard, 2016). Анализирајући велики број истраживања домаћих и страних теоретичара, није могуће на адекватан начин дати прецизан одговор руског стратешког положаја и способности да учествује у операцијама испод прага сукоба. Истраживачи наведено описују на више начина: као хибридни рат, краткотрајну стратегију, нову генерацију ратовања или сукоб у сивој зони. Руска Федерација предузима више нивоа сукоба, али све док не досегну ниво преко којег их надмашују САД и Северноатлантски савез. Интензивна је у руској стратегији примена конвенционалних и невојних средстава како би постигли своје стратешке циљеве. Наравно, све се то догађа и спроводи до оног момента док не иницирају војни одговор САД. Стратешки циљеви РФ укључују слабљење Северноатлантског савеза ради стицања доминације у Европи.

Незападни концепти одвраћања: према Адамском (*Dmitry Adamsky*), званични руски концепт одвраћања је укорењен у много холистичкијим схватањима. Ова холистичка схватања обухватају елементе и одвраћања и принуде, могу се одвијати пре, током и после рата, и прелазити војне и цивилне домене. Одвраћање у РФ значи употребу претњи, понекад праћених употребом силе. Наведено се спроводи ради очувања статуса одвраћања, затим да га промени, примора, па да обликује стратешко окружење у оквиру којег се све то дешава. Разлика од одвраћања на западу је сугерисање реактивног приступа док је на другој страни проактивнији приступ. Схватање одвраћања у РФ је кроз читав спектар стратешке интеракције, укључујући спречавање појаве претње на првом месту у миру или не, коришћење силе у кризи или рату или обликовање стратешког окружења касније. У одвраћању РФ, моћ произилази из могућности употребе и употребе војних и невојних инструмената. Тако концепт одвраћања са више домена укључује нуклеарни, свемирски и информациони. Адамски објашњава да у стратешком мишљењу РФ појам о војној победи није нестао из нуклеарне стратегије. Наведено појачава ефекте одвраћања. Примењујући западни терминолошки оквир за објашњење руског концепта, може се доћи до погрешне перцепције (Adamsky, 2021).

Ротман (*Maarten Rothman*) одвраћање истражује као метод који употребљава председник РФ, Владимир Путин, ради спречавања евентуалних демократских побуна. Ротман додаје да је неопходно сагледавати потенцијал да моћна држава може војним претњама обесхрабрити народне покрете и супротставити се на такав начин својим противницима. Када говори о одвраћању и принуди, Ротман претпоставља да су из Путинове перспективе присутне две стратегије, да сами себе обесхрабре или одврате демократске побуне, и то: гушење од стране власти погођене земље и претње интервенцијом против продемократских демонстраната или потенцијалних демонстраната, било у знак подршке савезничким режимима током устанка или као казна после њиховог свргавања. Разлог одвраћања је уједно и домаћа и спољна претња, истовремено. Успех домаће

репресије зависи од локалних ограничења и симпатија, укључујући и особље безбедносних служби. Недостатак ове врсте одвраћања Ротман види у томе што демократске побуне не спроводи унитарни актер већ тај колектив који је настао, а он се појављује као колектив само током догађаја и након истог губи снагу, нестаје. У закључку Ротман износи да је онда у интересу РФ да повремено пружа медијске приче које подстичу овај однос, стварајући инциденте (Rothman, 2021).

Вештачка интелигенција представља брзо развијајући сегмент технологије са потенцијално значајним утицајима на националну безбедност. САД и друге државе развијају вештачку интелигенцију за велики број војних функција. Вештачка интелигенција је нашла примену у великом броју сегмената нашег друштва, прикупљању и анализи обавештајних података, логистике, сајбер операција, информационих операција, командовања и контроле, и за разна полуаутономна и аутономна возила. Вештачка интелигенција је била укључена у војне операције у Ираку и Сирији. Кина тежишно развија вештачку интелигенцију за доношење бржих и боље информисаних одлука, као и на развој аутономних војних возила. Руска Федерација је активна у развоју војне вештачке интелигенције, првенствено роботике. Вештачка интелигенција има потенцијал да пружи бројне предности у војном контексту, али она може и да доведе до појаве различитих изазова, па и ризика, ако не и претњи (Hoadley & Sayler, 2020).

3.2.3. Перспективни пројекти у стратегијама одвраћања Руске Федерације

У РФ једно од тумачења *информационе безбедности* је да она обухвата „сагледавање стања безбедности информационог простора, обезбеђивање истог, стања инфраструктуре у којој се информације користе и да ли се користе за предвиђену намену, као и стања информација и тежина нарушавања тајности, интегритета и доступности, затим економска и финансијска компонента" (Ясенев, 2017, p. 8).

Претња од сајбер (кибер) рата је присутна. Наведено је потврђено рачунарским нападима на Естонију током априла и маја 2007. године (Путник, 2012). Тип напада је био релативно конвенционалан. Радило се о првом случају да су сви актери у земљи били истовремено на удару – од политичких, медијских и економских – што је довело до колапса државе. Радило се о првом догађају где је сукоб у сајбер (кибер) простору попримио политичку димензију. Овај сукоб је веома лако могао да ескалира у ратни сукоб. Пар дана након овог напада, естонски министар спољних послова је као виновника напада оптужио руску владу захтевајући примену члана 5. Североатлантског савеза који предвиђа колективну одбрану нападнуте државе (Путник, 2012). Многи сматрају овај конфликт првим сајбер (кибер) ратом. Међутим, само годину дана након ових догађаја, РФ је у августу 2008. године поново оптужена за извођење сајбер (кибер) – напада, сада на Грузију (Путник, 2012). Можемо констатовати да се ради о угрожавању суверенитета државе, где је РФ несумњиво показала шта је могуће да се догоди једној држави попут Естоније или Грузије, уколико би се понашала супротно интересима РФ. Ово је један од примера трансформације стратегије одвраћања, односно поред нуклеарног, постоје и други инструменти који могу навести државу на поступке у складу са интересима матичне државе. Стварање новог инструмента који је у једном моменту реактиван (офанзиван), све док не постане довољна опасност по живот и функционисање кључних инфраструктура једне државе, представља прекретницу трансформисања стратегије одвраћања у сајбер одвраћање у XXI веку.

Руска Федерација је најавом 2018. године од стране председника РФ, Владимира Путина, па затим тестирањем и увођењем хиперсоничног оружја у оперативну употребу, само 20 месеци након тог говора, увела нови тип хиперсоничног оружја кодног имена *Авангард*, које лети 20 пута брже од брзине звука „цик – цак" трајекторијом што га чини неухватљивим за противракетну одбрану, што је обесмислило мегаломанске пројекте улагања у ракетну одбрану и стварању непробојних *кишобрана*. Хладноратовски концепти узајамног осигураног уништења и стратегије одвраћања били би доведени у питање. Хиперсонично оружје представља вид гаранције његовог очувања војне моћи. Увођењем хиперсоничног оружја у оперативну употребу, РФ је онемогућила превагу стратешке равнотеже САД са системима противракетне одбране. Ради се о наоружању које се креће пет и више пута брже од брзине звука, што невероватно скраћује време реаговања противника приликом евентуалне интервенције. Хиперсоничне ракете ће пружити нову еру одвраћања што ће дефинитивно бити привилегија најбогатијих држава (Stojanović, 2020). У говору који је одржао 2018. године, Владимир Путин је најавио и нове балистичке ракете *Кинжал*, интерконтиненталну балистичку ракету *Сармат*, прве крстареће ракете на нуклеарни погон неограниченог домета кодног имена *Буревестник*, подводног дрона на нуклеарни погон *Посејдон* и морнаричке хиперсоничне ракете *Циркон* за своје оружане снаге.

Није искључен евентуални развој дронова који би уз масовну (*у облику ројева*) употребу (без могућности супротстављања или уз делимичну могућност супротстављања) извршавали одређене задатке у сврху одвраћања, носећи мале, али у огромном броју експлозивне материје или неке друге агенсе. Развој информационо – телекомуникационог сектора се догађа вртоглавом брзином коју напросто није могуће пропратити у реалном времену, тако да у овим областима поред наведених сајбер напада је очекивати нове алате у супротстављању државама, односно одвраћању и новим операцијама испод прага сукоба (Марјановић, 2022). Ангажовање и могућности прилагођавања великих система попут оружаних снага, па и служби безбедности изузетно тромих институција и усклађивање кадра, средстава и начина рада са новим изазовима и претњама представиће могућност бржег и квалитетнијег одвраћања у будућности. Стратегијско одвраћање великих сила је углавном везано за остваривање дугорочних државних циљева применом одређених облика присиле, јавно и/или тајно. Одвраћање је везано за развој нових технологија што је у многоме утицало директно на еволуцију концепта одвраћања. Развој и поседовање нуклеарног наоружања и других нових технологија, програма везаних за наоружање и војну опрему умногоме одређују концепт стратегијског одвраћања, а поготово револуционарна открића која могу да чак и у потпуности избаце из употребе читаве системе у сврху стратегијског одвраћања једне или више држава, савеза (Марјановић, 2022).

Дорн и Бринкел (*Cees van Doorn & Theo Brinkel*) истражују још једну технику одвраћања, а то је отпорност. Отпорност на моћи хибридних претњи (тада првенствено говоримо о необавештајним активностима) и њиховим могућностима нарушавања интегритета политичких, економских, друштвених и других структура у државама. У теорији, хибридни рат је тај који отвара широки спектар могућности коришћења свих доступних техника, тактика и инструмената осим самог рата. Дезинформације које експлоатишу друштвени медији су врло битна техника тј. инструмент одвраћања. Отпорност представља способност појединца, заједнице, организације или неког другог ентитета да буде спреман за поремећаје, да се прилагођава новонасталим околностима и даље одраста,

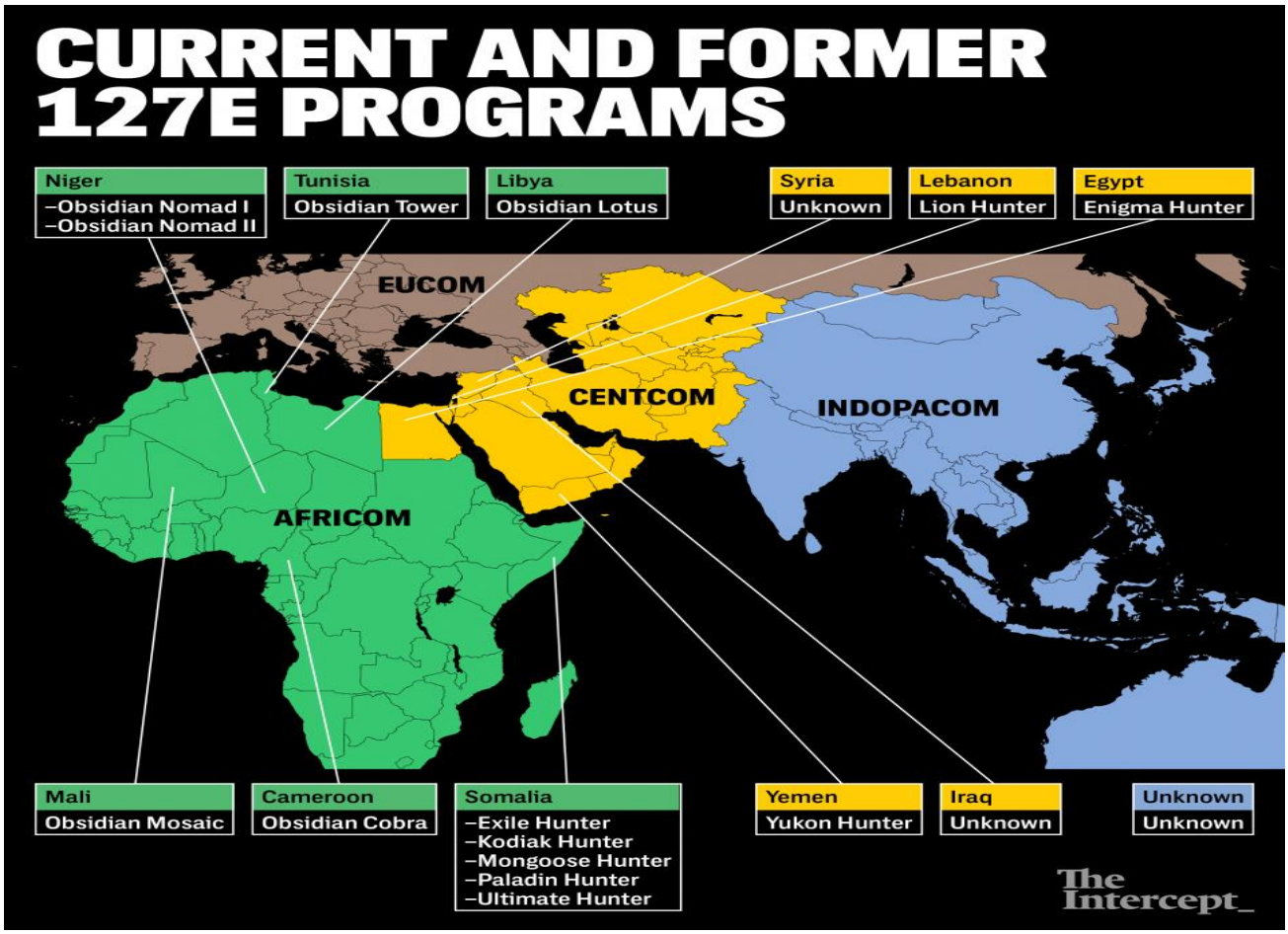
функционише уз њих. Немогуће је одбранити се од свих претњи. Ефикасно одвраћање обично зависи од јаке одбрамбене способности и политичке одлучности да се нешто предузме. Када се говори о информационом рату, одлучујућа способност је порицање употребе оружја. Истинитост, доследност и поштовање договора су тотална супротност кампањама дезинформација (тзв. одвраћање делегитимизацијом). Отпорност се манифестује и у заједничким вредностима и циљевима. Владавина људских права, слобода, поверења у друштво је суштински део који представља отпорност (Doorn & Brinkel, 2021). Када говоримо о отпорности једног друштва тада никако не можемо да не сагледамо све технике које су примењиване у реализацији неког догађаја и да то не проверавамо тако што ћемо потврђивати један исти податак, преко различитих медија, извора (мислећи да смо тако проверили податак) који су на једном платном списку, једне организације, службе безбедности – државе као крајњег неког невидљивог корисника. То су честе замке које се могу врло лако подвести под добро припремљену дезинформацију. Главна одлика сваког друштва у повећању отпорности (енг. *resilience*) би требало да буде повећање знања и борба за што квалитетнијим доласком до знања. Ово је једно од истраживања које је врло дискутабилно, јер се често у медијима поставља питање ко би стварно испланирао да обори авион са ракетом (системом) коју(и) је он лично направио и да то у XXI веку остане сакривено од јавности?

Арбатов (*Alexey Arbatov*) напомиње да су у протеклим деценијама нуклеарне способности РФ и САД значајно смањене, али је ризик од нуклеарног рата већи него што је био на крају Хладног рата. Арбатов описује како увођење нових фактора доводи до великих претњи као што је појава хиперсоничних пројектила, свемирско оружје, сајбер инструменти и интеграција вештачке интелигенције у нуклеарни систем командовања. Системи раног упозоравања могу бити нападнути или извршена обмана, преварен новим свемирским и сајбер способностима. Хиперсоничне ракете чине земаљске радаре неважним и значајно скраћују време за реаговање након детекције сателитских система који нису поуздани у потпуности (Arbatov, 2021).

Успон приватних војних компанија (енг. *Private Military Companies*) из РФ подударио се са развојем војне доктрине и стратегије у РФ у вези са употребом и улогом недржавних актера у сукобу. Евидентно је да оружане снаге РФ верују да се значај информација и политичког утицаја повећао у савременим сукобима, због чега су нетрадиционални облици принуде посебно важни. Ангажовањем приватних војних компанија нуде се четири потенцијалне предности РФ, што представља основу за употребу оваквих компанија, и то: порицање, избегавање незгода, брзо распоређивање (па и повлачење) и јефтинија употреба од употребе конвенционалних оружаних снага. Процене служби безбедности САД су да би се употреба приватних војних компанија могла повећати[11] у будућности (Bowen, 2020). Дана 5. новембра 2022. године велики број прозападних и происточних медија је објавио вест о

[11] Ова процена се подудара и са формирањем приватне војне компаније *Моцарт група* (енг. *Mozart group*) коју је наводно формирао бивши припадник оружаних снага САД – маринаца (*U.S. Marine Corps*) из Лондона, пуковник Ендрју Милбурн (*Andrew Milburn*) који је наводно пензионисан 2019. године, а медији наглашавају његово пензионисање и да је групу формирао приватно (службе безбедности, државе на овај начин избегавају евентуалне последице настале ангажовањем оваквих лица, група и сличних компанија). Наводно је ова група ангажована као пандан *Вагнер групи* у Украјини од стране Уједињеног Краљевства и/или САД, објављен текст у *nytimes.com* дана 1. фебруара 2023. године.

отварању центра приватне војне компаније *Вагнера* у Санкт Петебургу, РФ и да је Јевгениј Пригожин почео да шири спектар активности од чисто паравојног деловања према окупљању проналазача у центру, затим програмера, уопште информационо – телекомуникационог стручњака, разне врсте експерименталних произвођача и других специјалности. Дана 4. децембра 2022. године у великом броју дневних новина[12] у Републици Србији је објављено како је *Интерцепт* (енг. *The Intercept* – америчка непрофитна новинска организација) наводно преко Закона о слободи информација дошла до података да је постојао или још увек постоји тајни програм „127е" где је најмање 14 такозваних „127е" програма било активно на ширем подручју Блиског истока и Азијско – пацифичког региона 2020. године (за остатак држава нема тренутно доступних података – види *Слику 1*). Наводно, према изјави медија, Пентагон, САД је наводно покренуо 23 одвојена програма „127е" на читавој планети у периоду од 2017. до 2020. године. Наводно „127е" програм овлашћује оружане снаге САД да ангажују припаднике оружаних снага САД, специјалне саставе, да под оправдањем *противтерористичких операција* у сарадњи са страним и нерегуларним партнерским снагама спроводе акције широм света. Поред ове врсте акција, Програм наводно омогућава САД да за своје потребе наоружавају, обучавају и обезбеђују обавештајне податке страним снагама, укључујући и нерегуларне снаге.



Слика 1. Приказ ангажовања снага и средстава у оквиру наводног програма *127е*.
Извор: The Intercept – Nick Turse, Alice Speri.

[12] Вечерње новости, Ало, Наслови.нет, Информер, СД.рс, *sputnikportal.rs* и др., а на сајту *theintercept.com* је објављен текст са овом проблематиком 1. јула 2022. године.

4. УЛОГА СЛУЖБИ БЕЗБЕДНОСТИ У РЕАЛИЗАЦИЈИ АКТИВНОСТИ ОДВРАЋАЊА ВЕЛИКИХ СИЛА

Читајући разноврсну домаћу и иностране литературу, врло често наилазимо на термин безбедносно – обавештајни или обавештајно – безбедносни систем, а да као просечан читалац том приликом не уочимо апсолутно никакву разлику у ова два термина. Наиме, почев од основних (хијерархијски најстаријих правних докумената у једној држави) норматива који прописују постојање и рад обавештајно – безбедносног или безбедносно – обавештајног система неке државе у терминолошком одређењу навођења прве речи безбедносно или обавештајно, даје се, одређује, тежиште приликом процена за формирање и/или реорганизације постојећег система, а затим и рада читавог система на безбедносном или обавештајном сегменту као тежишном. Овде долазимо већ до једног неписаног правила, задатка, датог обавештајно – безбедносном или безбедносно – обавештајном систему једне државе који ће бити правац, тежиште рада оваквог система. Тако, уколико назив система почиње са безбедносно наглашава да ће у држави главни део система бити безбедносни апарат, док уколико у називу система прво стоји обавештајни, наведено нам говори да ће у систему главни, тежишни део тог апарата бити обавештајни део система. Ово није крај значења овог термина, већ након одређења тежишта система, у самом називу, термину безбедносно – обавештајни или обавештајно – безбедносни систем ћемо доћи и до тежишта рада, ангажовања тог система односно активности коју ће примењивати делови система. Тако закључујемо да када је прва реч у сложеници безбедносно, тада је тежиште рада (снага) и активности дела система у примени безбедносних и контраобавештајних активности (као и служби које се баве овим активностима) што чини офанзивне активности (снаге), а обавештајне активности су тада у другом плану (као и службе које се баве овим активностима) што би војници или припадници служби безбедности назвали дефанзивним активностима (снагама). Уколико се прво наводи термин обавештајно у сложеници, тада су обавештајне активности (снаге) у тежишту ангажовања (формације), представљају офанзивну компоненту у систему, док безбедносне и контраобавештајне активности (снаге) представљају дефанзивну компоненту ангажовања (формације).

4.1. СЛУЖБЕ БЕЗБЕДНОСТИ

Први међу једнакима или најзначајнији субјекат система националне безбедности модерних држава представља савремени безбедносно – обавештајни или обавештајно – безбедносни систем (који чине службе безбедности). Оправдање за овакву констатацију можемо пронаћи у сталним променама живота и рада које носи данашњица и новим претњама по безбедност коју исте носе са собом. Зато су као одговор система безбедносно – обавештајног на претње које угрожавају националну безбедност присутне сталне реформе њиховог стратешког деловања, делокруга рада и организације. С обзиром на тежишно превентивну улогу оваквих система у смислу обезбеђивања адекватних безбедносних и обавештајних података и информисања надлежних ради предузимања мера на ублажавању, контролисању или отклањању регистроване претње велики број држава покушава пратити корак ових промена. Свако истраживање по питањима савремених безбедносно – обавештајних или обавештајно – безбедносних система данас захтева познавање природе и функционисања политичког система државе чији се систем истражује. Да ли је у питању

председнички, парламентарни, или комбинација ових система, зависи од великог броја питања везаних за функционисање система националне безбедности што доводи до питања ко руководи системом (председник државе или председник владе – премијер), какав је начин координације, контроле и других питања значајних за рад законодавне, извршне и судске власти (Бајагић, 2015b). Брзина промена стратешких праваца у организацији и раду безбедносно – обавештајних система врло често доводи и до промена организација, што је у суштини неопходно, али врло често представља и клопку уколико су те промене честе, не стигне да се заврши потребан циклус формирања и функционисања организације и већ се улази у нове промене, што може бити контрапродуктивно и водити ка урушавању или у најгорем случају нестанку те организације.

Још давне 1776. године, на иницијативу генерала Вашингтона, у оружаним снагама уједињених колонија створена је прва специјализована извиђачко – диверзантска јединица. Ради се о елитном, пробраном саставу америчке војске који је добио назив према свом првом команданту Томасу Нолтону, *Нолтон ренџери*. Нолтон ренџери су имали задатке да решавају такве задатке који су сматрани превише опасним и ризичним за јединице регуларне војске. Већ 1778. године, војска Конфедерације створила је положај шефа војне службе безбедности (обавештајног карактера). Радило се о бригадном генералу Чарлсу Скоту из Вирџиније. Након његовог пензионисања, дужност је преузео пуковник Дејвид Хенли, а затим мајор Бенџамин Талмеџ (Юрьевич, 2014). Поред државних агенција у војсци северњака, обавештајне и контраобавештајне активности обављала је и приватна детективска агенција Алана Пинкертона (1850. године основана у Чикагу). Пред рат, Пинкертон је успео да спречи покушај атентата на председника Линколна. Овим поступком је постао познат. Пикертон је радио под покровитељством Џорџа Меклина (убрзо након почетка рата постављен је за команданта војске Севера), а затим постаје шеф војне обавештајне службе северњака. Ускоро га председник Линколн поставља на место шефа Уједињене обавештајне службе (енг. *Union Intelligence Service*), у којој је радно ангажовао своје детективе. По окончању ратних дејстава, службе безбедности створене током грађанског рата, како у војсци победоносних северњака тако и у војсци поражених јужњака, укинуте су као непотребне. Две деценије након завршетка грађанског рата, потребе за обавештајним подацима у миру поставили су као потребу руководиоци поморских и војних министарстава. Дана 23. марта 1882. године, секретар морнарице Вилијам Хант, у оквиру Бироа за навигацију Поморског одељења својом наредбом створио је Канцеларију за поморске обавештајне службе са задацима „прикупљања и уопштавања поморских информација које могу бити од користи Министарству морнарице у време рата и мира" (Юрьевич, p. 39). Три године касније, 1885. године, слична обавештајна служба, Одсек за војне информације (енг. *Military Information Division*), створена је у оквиру Ратног одељења у оквиру Одсека за војне резерве (енг. *Military Reservation Division*). У скоро три деценије, име одељења се мењало два пута, а у фебруару 1903. године добило је назив Војнообавештајно одељење и формацијски устројено као друго у хијерархији одељење Главног генералштаба у организационој структури Министарства рата. Војнообавештајно одељење обухватало је два одсека: одсек војних информација и одсек војних аташеа (Юрьевич, 2014).

Почевши од 1894. године, Одељење тајне службе почело је да чува америчке председнике, али не као стални задатак ове службе. У лето 1894. године припадници Одељења тајне службе чували су председника Кливленда и чланове његове породице. У

одређеним интервалима, на пример, током шпанско – америчког рата 1898. године, припадници Одељења тајне службе такође су чували председника Вилијама Мекинлија. У септембру 1901. године када је на Мекинлија извршен атентат, није му обезбеђена заштита Одељења тајне службе. Након овог трагичног догађаја, убиства председника Вилијама Мекинлија крајем 1901. године, Конгрес је затражио од Тајне службе да обезбеди трајну заштиту америчким председницима. Да би се САД супротставиле појачаним обавештајним активностима непријатеља у оружаним снагама САД, 1942. године створен је Војни контраобавештајни корпус, који је пружао контраобавештајну подршку оружаним снагама САД како на територији САД, тако и шире. Војна обавештајна служба почела је да обраћа озбиљнију пажњу на пресретање и дешифровање непријатељске кореспонденције у овом периоду (Юрьевич, 2014).

У САД комплетна Обавештајна заједница (енг. *Intelligence community*) је састављена од укупно 17 елемената, почев од савезних агенција као највећих ентитета, па канцеларија, уреда, одељења, бироа и сл. у оквиру извршне власти који су надлежни за прикупљање, анализу и коришћење обавештајних података. Овај састав обавештајне заједнице САД је детаљно обрађен у поднаслову *Значај обавештајне активности за државу*, па неће бити евидентиран у овом делу истраживања.

По правилу, у држави постоји неколико служби безбедности. Основни принцип рада запослених у Мосаду (служба безбедности Израела направљена по моделу служби САД) је да прво сазнају што је могуће више о непријатељу, па тек онда користе силу. Мосад је одговоран за следеће: прикупљање обавештајних података у иностранству, извођење различитих акција, укључујући и терористичке, као и за борбу против палестинског покрета отпора ван државе. Напори службе безбедности усмерени су на добијање политичких, економских и војних информација у свим регионима света како би их користили у интересу Израела (државе). Предмет Мосадових обавештајних активности су и међународне организације, укључујући и Уједињене нације, пошто је ова организација више пута доносила одлуке које су непожељне за Израел. Уз одобрење владе, спроводе се необавештајне активности, *специјалне акције* за елиминисање вођа арапских организација, вођење психолошког рата, дезинформација и др. Истовремено, Мосад активно сарађује са Западним службама безбедности (Шаваев & Лекарев, 2003).

Када говоримо о службама безбедности РФ неопходно је укратко сагледати историјски преглед од првих служби безбедности РФ, њихових задатака још из доба Руског царства, па до данас (види *Табелу 4* и *Табелу 5*).

Табела 4. Преглед руских и совјетских служби безбедности и јединица.

Период	Назив службе – јединице	Задаци
1565 – 1572	Oprichnina	□ Secret police: suppression of Russian citizens. □ Bodyguard of the Russian Czar.
1882 – 1917	Okhrana	□ Secret police: suppression of Russian citizens. □ Foreign and domestic intelligence service.
1917 – 1922	Cheka/VChK (Vserossiyskaya Chrezvychaynaya Komissiya)	□ Secret police: suppression of Russian citizens. □ Fighting against saboteurs and counterrevolutionaries, like any civil or military servicemen loyal to Imperialistic Russia, clergy, and bourgeois.
1922 – 1923	GPU (Gosudartsvennoye Politichekoe Upravelenie)	□ Secret police: suppression of Soviet citizens. □ Foreign and domestic intelligence service.

Период	Назив службе – јединице	Задаци
1923 – 1934	OGPU (Obyedinennoe Gosudartsvennoye Politichekoe Upraveleni)	Secret police: suppression of Soviet citizens. Foreign and domestic intelligence service. Since 1926: anti – state terrorism.
1934 – 1946	NKVD (Narodniy Kommissariat Vnutrennikh del CCCP)	Secret police: suppression of Soviet citizens (known for its role in the Great Purge in 1936 – 1938). Foreign and domestic intelligence service. Anti – state terrorism. Normal police work. Fire fighting. Management of and securing prisons and labour camps. Protection of the borders of the Soviet Union.
1941 – 1953	MGB (Ministerstvo Gosudarstvennoi Bezopasnosti)	Secret police: suppression of Soviet citizens. Foreign and domestic intelligence service. Counterintelligence. Managing Soviet public opinion and loyalty.
1943 – 1946	NKGB (Narodniy Kommissariat Gosudartstvennoi Bezopasnosti)	Secret police: suppression of Soviet citizens. Foreign and domestic intelligence service. Counterintelligence. Penetration and liquidation of anti – Soviet elements in the Soviet Union. Protection of Communist Party and government officials.
1953 – 1991	MVD (Ministerstvo Gosudarstvennoi Bezopasnosti)	Investigating into certain categories of crime and criminality. Supervising Soviet passport system. Maintaining public order. Combating public intoxication. Supervising parolees. Management and securing prisons and labour camps. Fire fighting. Controlling traffic. Management of special psychiatric hospitals.
1954 – 1991	KGB (Komitet Gosudarstvennoi Bezopastnosti)	Secret police: suppression of Soviet citizens. Foreign and domestic intelligence service. Counterintelligence. Operative – investigatory activities. Protection of the borders of the Soviet Union. Protection of Communist Party and government officials. Ensuring government communication. Implement active measures to ensure Soviet Union's security. Running „agents – of – influence" programme. Combating Russian nationalism, opposition, and anti – Soviet activities
1991 – present	Russian Procuracy	Prosecution in court on behalf of the Russian Federation. Investigations into all legal matters. Starting indictment procedures of Russian residents and citizens, which in practice turned out to be an instrument of repression.
1991 – present	SVR (Sluzhba Vneshnei Rezvedki)	Foreign intelligence service. Implement active measures to ensure the Russian federation's security. Running „agents – of – influence" programme.

Период	Назив службе – јединице	Задаци
		Conduct strategic, economic, scientific and technology espionage. Protection of employees of Russian institution outside the Russian Federation. Conduct electronic surveillance in foreign countries. Negotiation of arrangements, like anti – terrorist cooperation and intelligence sharing, with foreign secret services.
1991 – 1994	FSK (Federalnaya Sluzhba Kontrrazvedki)	Domestic intelligence service. Counterintelligence.
1991 – 2003	FAPSI (Federal'noye Agentstvo Pravitel'stvennoy Sviazi i Informatsiy)	Signal Intelligence Security of government communications
1995 – present	FSB (Federalnaya Sluzhba Bezopastnosti)	Domestic intelligence service. Counterintelligence. Cyber security. Investigations into certain grave crimes and law violations. Fight against organised crime, terror and drug smuggling. Intelligence gathering in CIS states. Protection of Russian „compatriots abroad" in CIS states. Export control and economic security. Protection of the borders of the Russian Federation. Information and international relation service.
1996 – present	FSO (Federalnaya Sluzhba Okrany)	Protection of the President and Prime Minister of the Russian Federation, and other highranking state officials. Protection of federal properties.
2003 – present	Spetssviaz (Sluzhba Spetsial'noy Sviazi I Informatsiy)	Main function crypto analysis FSO became parent unit
2003 – present	Unit 71330	Electronic surveillance FSB became the parent unit
2008 – present	Advanced Persistent Threat 29 (APT 29) (Also known as „Cozy Bear")	Offensive Hacker Group. Cyber espionage of embassies (not confirmed). Targeting commercial companies and government organisations in Germany, Uzbekistan, South Korea, Norway, the Netherlands, the United States, the United Kingdom (not confirmed). Related to SVR

Извор: Bouwmeester, 2020, p. 473–475.

Табела 5. Преглед руских и совјетских војних служби безбедности и јединица.

Период	Назив службе – јединице	Задаци
1683 – 1917	Preobazhensky Lifeguard Regiment	Secret police: suppression of Russian citizens. Bodyguard of the Russian Czar. Infantry regiment.

Период	Назив службе – јединице	Задаци
1683 – 1918	Semyonovsky Lifeguard Regiment	Secret police: suppression of Russian citizens. Bodyguard of the Russian Czar. Infantry regiment.
1918 – 1926	Registrupravlenie/Registupr	Military intelligence service.
1926 – 1942	Fourth Department of Soviet Defence Department	Military intelligence service.
1941 – 1945	Razvedchik	Military scouts that stayed behind enemy lines for intelligence and sabotage activities.
1942 – present	GRU (Galvnoye Razvedyvatel'noye Upravleniye)	Main military intelligence service. Now: officially GU (Galvnoye Upravleniye) Conducting offensive cyber activities.
1943 – 1946	SMERSH (Smyert' Shpionam)	Protection of Red Army units against German infiltration. Track down of enemy military spies. Combating anti – Soviet elements, traitors and deserters in the Red Army. Improving discipline in Red Army Track down of Adolf Hitler.
1950 – present	Spetsnaz	Umbrella term for special purpose units, controlled by the GRU.
2005 – present	Advanced Persistent Threat 28 (APT) (Also known as „Fancy Bear")	Conducting offensive cyber activities Unit 26165: Unit 74455:
2016 – present	Rosgvardia	Protection of the borders of the Russian Federation. Take charge of gun control. Combat terrorism and organised crime. Protect public safety and order. Cyber security and cyber intelligence. Guarding important state facilities,like the Kremlin.

Извор: Bouwmeester, 2020, p. 475–476.

Да констатујемо да су према Рихлу (Riehle, 2022) данас најбитније службе безбедности у РФ следеће:

Спољна обавештајна служба (*СВР*), намењена вођењу страних обавештајних активности. Организација потиче директно из Прве главне управе *Комитета државне безбедности* (познатије под акронимом – *КГБ*, рус. *Комитет Государственнои Безопастности*). Бројно стање Спољне обавештајне службе је отприлике 10.000 до 15.000, од чега је отприлике четвртина стационирана у иностранству. Посебно битан за ово истраживање је податак да у Спољној обавештајној служби наводно постоји формацијска целина намењена специјалним операцијама, познатија под називом *Заслон*, која је наводно директно подређена директору Спољне обавештајне службе. Ова целина је директно одговорна за заштиту високих званичника руске амбасаде и других званичника руске владе када путују у иностранство где могу бити изложени одређеним претњама по безбедност лица или активности у којим учествују. На пример, припадници *Заслона* су ангажовани у обезбеђењу када је тадашњи потпредседник Владе РФ Дмитриј Рогозин путовао у Сирију 2014. године, а поред обезбеђења у оваквим срединама, извршава и задатке везане за спровођење тајних акција (необавештајних активности). Мало је података доступно о овој целини Спољне обавештајне службе, али је наводно формирана 1998. године како би

наследила јединице специјалних снага које су биле подређене Првој главној управи Комитета државне безбедности током совјетске ере.

Федерална служба безбедности (*ФСБ*) је наследила већину историјских функција Комитета државне безбедности. Ради се о великој организацији. Велики део њеног особља налази се у граничној служби, која је 2003. године Указом председника РФ препотчињена из Федералне граничне службе у Федералну службу безбедности. Ради се о служби безбедности која је примарна служба надлежна за унутрашњу безбедност државе и народа, тако да има већину ресурса посвећених тој мисији. Одговорна је за борбу против тероризма, екстремизма и етнички заснованих организованих криминалних активности. Спроводи и контраобавештајне активности у министарствима здравља, културе и просвете, у верској сфери и у некомерцијалним организацијама (овде препознајемо могуће наступе за потребе необавештајних активности). Интересантан сегмент за ово истраживање је и Центар за информациону безбедност, који се назива и 18. центар, спроводи и интерни интернет надзор усмерен на руске грађане и прикупљање страних обавештајних података, а 16. центар наводно је био ангажован у циљу напада на украјинску владу, као и органа за спровођење закона и војних ентитета. Федерална служба безбедности је такође наследила два елемента за реализацију тајних акција посебне намене од Комитета државне безбедности, под називом *Алфа* и *Вимпел* (биле су део Првог главног директората Комитета државне безбедности током совјетске ере и имале су улогу прикривених страних акција). Када је Спољна обавештајна служба створена 1991. године, пребачене су на функцију унутрашње безбедности, што је захтевало њихову каснију замену са *Заслоном* у Спољној обавештајној служби. *Алфа* и *Вимпел* су одговорни за сагледавање и евентуално неутралисање терориста или других претећих субјеката унутар РФ.

Следећа војна служба безбедности је *Главна управа Генералштаба* (рус. *Главное управление – ГУ*) која је до 2010. године постојала под називом Главна обавештајна управа (рус. *Гла́вное развéдывательное управлéние – ГРУ)*, па је и даље овај термин у широкој употреби не само у дневној већ и у научној кореспонденцији. Одговорна је за прикупљање обавештајних података у циљу подршке доношењу војних одлука и за тајне операције за подршку спољнополитичким циљевима, као што је био случај од оснивања војне обавештајне службе у совјетско доба.

Поред ове три најбитније службе безбедности у РФ, неопходно је поменути и следеће две службе битне за систем безбедности РФ, а ради се о *Националној гарди РФ* која је скоро формирана, 2016. године под називом *Росгвардија*, са задатком да одговори на оно што руска влада назива „покушајима дестабилизације" или на оно што би се ван РФ назвало незадовољством народа. Намењена је за сузбијање протеста како у физичком, тако и у компјутерском домену. Део мисија гарде се знатно преклапа са Федералном службом безбедности, иако је примарна сврха Националне гарде да остане организационо блиска председнику РФ у случају унутрашњих нереда и неслагања. Следећа служба битна за систем безбедности РФ је *Федерална служба заштите* (*Федеральная служба охраны – ФСО*) чија је најпознатија улога заштита председника РФ и око 40 других високих владиних званичника, укључујући премијера, председнике Савета Федерације и Државне Думе, шефа Председничке администрације, председника Савета безбедности и директора Федералне службе безбедности. Федерална служба заштите је потомак неколико делова бившег Комитета државне безбедности. Намена Федералне службе заштите је заштита виших

руководилаца, обезбеђење објеката који се посебно штите и обезбеђење владиних комуникација, укључујући специјалне шифроване комуникације (Riehle, 2022).

У Републици Србији безбедносно – обавештајни систем је одређен као један од субјеката националне безбедности састављен од три службе безбедности (Безбедносно – информативна агенција, Војнобезбедносна агенција и Војнообавештајна агенција). Безбедносно – обавештајни систем чини део извршног система националне безбедности државе (Стратегија националне безбедности Републике Србије, 2019). Према томе, основне категорије феномена служби безбедности јесу безбедносно – обавештајни систем са активностима које предузимају субјекти система и то обавештајна активност, контраобавештајна активност (укључујући и безбедносну заштиту – активности, прим. аут.) и необавештајна (субверзивна) активност (Мијалковић, 2011). „Безбедносне активности (енг. *Security activities*) обухватају особље (кадрове), физичку, информациону, оперативну, индустријску и техничку заштиту и противмере за заштиту информација, критичне инфраструктуре, мрежа, особља и објеката од свих претњи" (Strategic Plan 2018–2022, 2017, p. 2).

Основни задатак свих служби безбедности је да владама обезбеде проверене и тачне информације о могућим претњама држави. Анализе служби безбедности помажу доносиоцима политичких одлука да могу дефинисати националне интересе, развити квалитетну националну безбедност, одредити доктрине и стратегије, оружане снаге и друге безбедносне институције, припремити државу за националне и глобалне кризе и одговорити на њих, као и спречити претње држави (Harder, 2017). Уколико није могуће спречити одређене претње, онда је неопходно предузети све што је у могућности да се ублаже одређене последице по људе, снаге, имовину, активности и друге битне елементе.

4.1.1. Појам службе безбедности

Ради описа инструмената националне моћи, годинама је коришћен акроним *DIME* (што је представљало скраћеницу на енглеском језику за: *D* – дипломатски, *I* – информативни, *M* – војни и *E* – економски). Упркос томе што је дуги низ година на овај начин описивана национална моћ САД (да ли свесно или несвесно запостављени инструменти), углавном креатори политике и стратези одавно разумеју да је много више инструмената укључених у развој политике националне безбедности, а поготово њено спровођење. Можемо констатовати да нови акроним као што је *MIDFIELD* (*M* – војни, *I* – информативне, *D* – дипломатске, *F* – финансијске, *I* – енг. *intelligence, E* – економија, *L* – право и *D* – развој) представља много шири спектар варијанти за стратешке руководиоце и креаторе државне политике (Scott, 2018). Да би разумели тај спектар, неопходно је да дефинишемо најбитнији инструмент, а то је енг. *intelligenc*e, који обезбеђује адекватну реализацију скоро свих државних стратегија, посебно стратегије одвраћања.

Различито терминолошко поимање термина енг. *intelligence* (уз тумачење обавештајне – контраобавештајне службе разматране као организације, која је организатор и реализатор и/или активности, па чак и података добијених овим активностима) односно служби безбедности или обавештајних и/или контраобавештајних, безбедносних служби, лицима која релативно слабо познају ову материју врло лако уноси неразумевање и доводи до лоше интерпретације одређених појмова, па и самих назива тајних служби. Бивше комунистичке државе су терминима државне безбедности или државне сигурности и сличним, називале

своје тајне службе (неке се још увек тако зову: Федерална служба безбедности – РФ; Министарство Државне Сигурности – Народна Република Кина, итд.). Демократизацијом друштава, ти називи су мењани и прилагођавани модерним називима. Тајне службе се баве обавештајним, контраобавештајним и другим необавештајним активностима, док постоје и тајне службе које се баве првенствено обавештајним или првенствено контраобавештајним активностима или искључиво контраобавештајним активностима и другим безбедносним пословима ради заштите државних, националних интереса, па су неке сходно тежишној активности коју обављају добијале и назив, односно име службе.

Безбедност, према већини западних теоретичара, укључује ублажавање претњи драгоценим вредностима. Дефинисана на овај начин, безбедност је неизбежно политичка, игра виталну улогу у одлучивању о томе ко добија шта, када и како у светској политици. Ово укључује тумачење прошлости како су различите групе размишљале и практиковале безбедност, разумевање садашњости и покушава да утиче на будућност (Williams, 2008). Када говоримо о *ублажавању претњи*, тада морамо говорити о службама безбедности. Службе безбедности на западу се углавном дефинишу као енг. *intelligence*, што подразумева и обавештајне и контраобавештајне службе. Међутим, када се жели нагласити да се ради о службама које су тежишно обавештајног карактера, тада се користи термин енг. *foreign intelligence*, а уколико се наглашава да се мисли на контраобавештајну службу онда се употребљава појам енг. *counterintelligence*. Када говоримо о *CIA* (Централној обавештајној агенцији, једној од тајних служби у Обавештајној заједници САД), говоримо о тајној служби која се тежишно бави прикупљањем и анализом страних обавештајних података и спровођења необавештајних активности. Док се нпр. у Великој Британији тајна служба која се првенствено бави контраобавештајним активностима зове Служба безбедности (енг. *Secret service – MI5*), док би сам превод (енг. *Military Intelligence, Section 5*) гласио Војни обавештајни одељак 5, што повећава конфузију код читаоца. У званичној нормативно – правној терминологији, када говоримо о тајним службама у Републици Србији, употребљавамо термин служба безбедности, што се односи на све три тајне службе у држави (једна централна Безбедносно – информативна агенција која се бави првенствено контраобавештајним и обавештајним активностима и две ресорне, које представљају органе управе у Министарству одбране, а то су Војнобезбедносна агенција која се првенствено бави контраобавештајним активностима и Војнообавештајна агенција која се тежишно бави обавештајним активностима), без обзира на то да ли се ради о обавештајној или контраобавештајној служби. У неформалној комуникацији врло често ће се чути термин безбедносна служба (што би се односило на контраобавештајну службу) или за лице запослено у тајној служби – безбедњак (када је реч о овлашћеном службеном лицу – контраобавештајцу). Тако да ће у даљем делу истраживања бити употребљаван термин служба безбедности (и за обавештајну и контраобавештајну службу тј. организацију како на Западу тако и на Истоку, једнако, без обзира на друга појмовна одређења у САД и РФ), док службе као вршиоца одређене радње, активности, делатности, службовања јасно разликујемо и дефинишемо у српском језику као обавештајну, контраобавештајну, безбедносну, необавештајну активност (што ће бити дефинисано у наредном делу истраживања) коју предузимају службе безбедности и/или друга тела под њиховим ингеренцијама за потребе спровођења заштите државних интереса.

Службе безбедности, као и велики број гломазних државних организација се врло тешко и споро мењају у организационом смислу, али динамика промена у свету је врло брза и натерала је службе да се стално прилагођавају у раду, па и у организацији новим трендовима економске, техничке, информационо – технолошке, политичке, војне, обавештајне, безбедносне и других природа. Стога је тешко формулисати образац или неки модел обавештајних или безбедносних служби.

Такође, поред свих различитости које их одређују, за већину служби безбедности се може одредити следеће. Демократске државе су карактеристичне по раздвајању на унутрашњу и спољну безбедност. Стога, када говоримо о службама безбедности, можемо говорити о интерним (унутрашњим) и екстерним (спољним) службама безбедности. Обавезе, надлежности унутрашњих служби безбедности су углавном да добије, повеже и процени обавештајне податке релевантне за унутрашњу безбедност. Задаци могу варирати у зависности од земље до земље. Велика већина служби безбедности врши подршку полицији, правосудним органима и др. органима у држави ради спровођења законских поступака из њихове надлежности. Службе безбедности имају јасно дефинисан делокруг рада најчешће прописан у самим законима који се односи на откривање, документовање и преко надлежних органа процесуирање следећих активности: шпијунажа, саботажа и субверзија, тероризам, политички, етнички и верски екстремизам, организовани криминал, производња и трговина наркотицима, лажирање новца и прање новца, ширење оружја за масовно уништавање, илегална трговина оружјем, илегална имиграција, кријумчарење оружја, другог наоружања и војне опреме као и електронски напади, хаковање и ширење дечје порнографије и др. Поред свега наведеног, унутрашње службе у својој надлежности имају вршење безбедносних провера за обављање одређених дужности, коришћење тајних података, постављења на више дужности у државним органима и слично. Приликом реализације својих задатака, унутрашње службе у најстрожијој тајности спроводе пресретање комуникација, прислушкивање, тајно надгледање говора мета под истрагом, убацивање агената унутар сагледаване организације и надзор. Задаци и надлежности спољних служби безбедности јесу да прибаве, увежу и процене стране обавештајне податке релевантне за спољну безбедност и у сврху упозорења државног руководства како би предузело адекавтне мере у заштити националних интереса земље. Заједничке обавезе за већину спољних служби безбедности су подршка безбедносној и спољној политици, откривање активности у иностранству које угрожавају безбедност и националне интересе, информационо ратовање, подршка планирању одбране, подршка војним операцијама, економска обавештајна активност, подршка праћењу уговора и других споразума. У извршавању својих мандата, спољне обавештајне службе се ослањају на све могуће доступне изворе и читав спектар техника тајног обавештајног деловања. Контраобавештајна активност је суштински задатак и сваке обавештајне службе како би могла успешно и безбедно реализовати своје обавезе (Geneva Centre For The Democratic Control Of Armed Forces, 2003).

Према Џонсону (*Loch K. Johnson*), контраобавештајно (обавештајно) особље мора бити квалитетно обучено. Постоји тенденција да се било који контраобавештајац (обавештајац) може преместити из службе безбедности без додатне обуке и да обавља контраобавештајне (обавештајне) послове како у својој агенцији, тако и у приватним фирмама. Контраобавештајна служба је посебно добила на значају у САД након што су ухваћени издајници у оквиру службе безбедности. Наиме, радило се о агенту Федералног

истражног бироа, Роберту Хансену (*Robert Hanssen*), као и официру Централне обавештајне агенције, Олдрич Ејмсу (*Aldrich Ames*), који су ухваћени и званичници Федералног истражног бироа и Централне обавештајне агенције су признали њихове активности. Ако се пронађу шпијуни унутар америчких агенција, то се назива контраобавештајни неуспех, а ако се не пронађу, може се такође назвати контраобавештајним неуспехом – одсуство доказа није доказ о одсуству (Johnson, 2007b).

Службе безбедности и обавештајне и контраобавештајне су уско стручно оспособљене државне организације (агенције) задужене за долазак до безбедносних (обавештајних) података битних за националну безбедност једне државе. Државе најчешће имају више служби безбедности специјализованих за одређену област тј. домен безбедности. Изузетно је позитивно поседовање већег броја служби безбедности јер омогућава већи број специјализованих тематских оквира сваке агенције и пружа разноврсност информација, самим тим и анализе претњи. Колико год да је позитивно, поседовање већег броја служби безбедности може створити и нове проблеме у координацији или конкуренцији између служби безбедности, јер услед међусобне „трке" у достављању информација крајњем кориснику, најчешће највишем државном и војном руководству може доћи до непотпуних или неадекватних процена претњи. Иако је одлазак у другу крајност, формирање једне службе безбедности, много исплативији финансијски и смањује проблеме у координацији, што неминовно доводи и до огромног ризика централизовања моћи код једног човека, односно унутар једне службе безбедности и отежава могућност проверљивости података или примене контролних механизама ради провере тачности доступних података. Служба безбедности која је по свом одређењу обавештајна служба у ширем смислу појма представља специјализовану организацију државног апарата која тајним методама и средствима спроводи обавештајне, контраобавештајне (укључујући и безбедносну заштиту – активности, прим. аут.), необавештајне (субверзивне) и друге активности с циљем заштите унутрашње и спољне безбедности државе и реализације стратешких циљева сопствене државе, као и заштите интереса саме службе безбедности (Мијалковић, 2011). Тежишна активност ових служби безбедности је прикупљање ваљаних података ради стварања обавештајних, контраобавештајних, безбедносних информација за надлежне органе (Мијалковић, 2011). Када говоримо о стварању информација, тада мислимо на обликовање сирових података прикупљених радом служби безбедности и затим разним анализама и на друге начине увезивањем са другим чињеницама састављања потпуних сазнања (у облику информације) о некој појави, догађају, активности и врло често са предлозима мера ради спречавања и/или ублажавања последица.

Службе безбедности које су по свом одређењу *контраобавештајне службе*, намењене су спречавању деловања страних обавештајних служби (првенствено шпијунаже, субверзије или саботаже или деловања политичких група под страном контролом), при томе штитећи изворе података службе безбедности и тајне методе рада у држави и иностранству. Рад контраобавештајне службе безбедности можемо поделити на два дела, дефанзивни и офанзивни. Дефанзивни део рада контраобавештајне службе безбедности се ослања првенствено на истраге, провере и надзор, а офанзивни део рада контраобавештајне службе укључује велики број операција у извршењу својих задатака и то следећих: за продирање, обману, ометање и манипулисање другим организацијама (Harder, 2017).

Службе безбедности сагледавају све структуре друштва и све друштвене активности (економске, војне, политичке, научне, информационе и др.) државе која им је интересантна. Поред обавештајне активности, примењују и контраобавештајну активност, усмерену на откривање и сузбијање деловања страних обавештајних служби према сопственој држави, мада све више, поготово офанзивне службе безбедности, примењују и необавештајне активности ради заштите интереса своје државе. Појам службе безбедности не може се поистовећивати само са појмом шпијунаже, јер она представља само део активности коју предузимају службе. Наведени кључни појмови ће бити детаљније описани у наредном делу рада (Гаћиновић, 2019). Службе безбедности представљају „специјализоване, релативно самосталне институције државног апарата овлашћене да легалним, јавним, али и тајним начинима и средствима прикупљају одређене безбедносне податке и информације о другим државама, или њеним институцијама, као и о могућим непријатељима, а ради вођења државне политике, односно које својим мерама и поступцима делују на осујећивању и пресецању одређене антиуставне делатности усмерене против државе и њених грађана, супротстављање деловању обавештајних служби, тероризма, међународног организованог криминала, тежих облика привредног криминала и корупције" (Стајић и Лазић, 2015, стр. 189). С обзиром да је у западној литератури углавном појмовно одређивана служба безбедности која се бави искључиво обавештајним активностима, овде је сублимирано појмовно одређење службе безбедности која се бави обавештајним и контраобавештајним активностима, али како би ово појмовно одређење било прецизније, потпуније, неопходно је придодати и реч *углавном* испред легалним (ради бављења необавештајним активностима служби безбедности које су углавном супротне важећим прописима), избрисати реч *међународно* испред организовани криминал и додати супротстављање екстремизму.

Службе безбедности су специфичне самосталне организације или организацијске целине државних органа, чија се активност (обавештајна, контраобавештајна) огледа у прикупљању, анализи података о другим лицима, групама, државама, субјектима у/и изван државе уз предлог мера државном руководству, ради правовремене заштите виталних интереса државе, док када политика постане немоћна и како би избегла ратни сукоб са другим државама, епилог је укључивање служби безбедности у реализовање необавештајних активности које би присилиле другу страну да поступи у складу са жељом матичне државе (Бајагић, 2015а). Можемо слободно закључити, уз Бајагићево одређење службе безбедности као једно од најобухватнијих, да је служба безбедности „специјализована установа државног апарата (извршне власти) која у складу са законом утврђеним делокругом рада, спроводи обавештајно – (безбедносно, прим. аут.) – информативне, обавештајно – безбедносне и необавештајне активности и субверзивне садржаје (тајне акције) према виталним интересима и вредностима противника, користећи научне методе, поступке, технике и средства у циљу остварења националних интереса и очувања и унапређења националне безбедности сопствене државе" (Бајагић, 2015а, стр. 135). Из ове дефиниције произилази и неколико наредних кључних појмова везаних за активности које обављају службе безбедности.

Службе безбедности САД су прешле дуг пут у развоју док се нису претвориле у моћан и прилично централизован систем служби безбедности које се баве заштитом националне безбедности државе. Посматрано кроз историју стварања САД, формирање и развој служби безбедности дешавали су се истовремено са формирањем и развојем државе. Приликом регистровања првих сукоба већ је постојала потреба за одређеним подацима (подршка

војним операцијама) које војни руководиоци нису имали, како би реализовали задатке додељене војсци, односно нису имали органе, јединице које би се бавиле овим пословима. У периоду настанка првих служби безбедности на тлу данашњих САД, обавештајне активности у САД су биле препознате само као саставни део војних активности, које су по окончању активних непријатељстава укинуте, тако да у миру у првим деценијама после формирања САД обавештајне активности практично нису ни спровођене. Развој привреде и јачање САД у XIX веку довели су до све веће потребе у САД за стварањем служби безбедности које делују не само у ратно, већ и у мирнодопско време. Поред обезбеђивања војних активности службе безбедности, односно њени припадници су почели да добијају све више задатака који нису били у овој категорији, односно да се баве проблемима везаним за дипломатске и полицијске активности државе. Током Првог светског рата, амерички обавештајци нису били у стању да решавају обавештајне задатке широм државе због међуресорне конкуренције и неспремности ресорних обавештајних служби да поделе информације до којих су дошли. Наведени пропусти су отклоњени захваљујући Френклину Д. Рузвелту који је успео да створи централизован и ефикасан систем служби безбедности, што је већ током Другог светског рата довело до значајног побољшања резултата деловања служби безбедности САД и учињен је можда први корак ка трансформацији обавештајне активности у једну од самосталних делатности државе. Главни задатак служби безбедности САД након завршетка Другог светског рата је конфронтација између Савеза Совјетских Социјалистичких Република и светског социјалистичког система. Управо је глобална природа задатака служби безбедности САД у борби против Савеза Совјетских Социјалистичких Република омогућила САД да коначно трансформишу обавештајну активност у независну врсту државне делатности и да се створи таква организациона заједница која обједињује све водеће службе безбедности. Приоритетни развој у првим деценијама након завршетка Другог светског рата био је везан за техничку област обавештајне активности, попут свемирске обавештајне службе или обавештајне службе на комуникационим каналима и каналима за пренос информација. У периоду до задње четвртине двадесетог века, службе безбедности САД су се фокусирале само на постизање максималне ефикасности у својим активностима усмереним на прикупљање и добијање обавештајних информација, а није разматрана потреба за поштовањем грађанских права и слобода. Законска ограничења која су се појавила у овом периоду озбиљно су закомпликовала рад службама безбедности односно обавештајне активности у САД, где је морало доста тога да се регулише, пропише, поштује, као и да се одговара за евентуално непоштовање. Распадом Савеза Совјетских Социјалистичких Република дошло је до озбиљне трансформације спектра задатака које су морали да решавају службе безбедности САД. Поред традиционалних задатака решаваних током година Хладног рата, у постхладноратовском периоду, од последње деценије двадесетог века, приоритети служби безбедности су: борба против тероризма, трговине дрогом, организованог криминала, сузбијање пролиферације оружја за масовно уништење. Тренд ка јачању обавештајне активности САД на информационим каналима (тежишно их спроводи служба безбедности Агенција за националну безбедност), био је резултат развоја информационих технологија, што је отворило невиђене могућности за глобално прикупљање информација (Юрьевич, 2014).

4.1.2. Методе прикупљања података

Безбедност сваке државе, њених националних интереса, представља најбитнији елемент функционисања једног друштва. Остваривање високог степена безбедности једне државе зависи од могућности доласка до податка, информација битних за спречавање угрожавања националне безбедности, чиме се тежишно баве службе безбедности. С обзиром на то да се ради о тајним делатностима лица и организација који планирају да угрозе националну безбедност државе, супротстављање оваквим непријатељима је једино могуће применом тајних метода за прикупљање података (Марјановић, Лабовић и Браковић, 2022). Службе безбедности су надлежне за примену тајних метода у складу са прописима. Карактер тајних метода за прикупљање података се огледа у томе да се за одређено време, у тајности, а на основу одлуке директора службе безбедности или суда, и под условима које је предвидео закон, одступа од појединих, грађанину уставом загарантованих појединачних права (Марјановић, Лабовић и Браковић, 2022). Нормативно упориште за примену тајних метода рада од стране овлашћених службених лица проналазимо у законима и другим актима. Тајно прикупљање података се врши применом посебних поступака и мера, где се применом тајних метода врши прикупљање података до којих није могуће доћи на други начин, односно само прикупљање би носило велики ризик или несразмерне трошкове. Одобрење за примену ових мера и поступака даје директор службе безбедности, односно надлежни суд. Поред посебних поступака и мера, једна од врло битних тајних метода рада је и тајна сарадња са физичким лицем (Марјановић, Лабовић и Браковић, 2022). Примена тајних метода у раду служби безбедности Републике Србије суштински представља реализацију њихових законских овлашћења, применом посебних поступака, мера и активности, које спроводе овлашћена службена лица у циљу прикупљања, анализирања и даље дистрибуције информација и података од значаја за заштиту њених националних интереса (Марјановић, Лабовић и Браковић, 2022).

У зависности од методе која се примењује за добијање обавештајних података, до средине XX века као карактеристичне за модерне обавештајне службе САД издвајају се следеће активности: обавештајне активности које се спроводе уз помоћ појединаца (енг. *Human Intelligence*), обавештајне активности на каналима комуникације и каналима за пренос информација (енг. *Signal Intelligence*), ваздухопловне обавештајне активности (енг. *Geospatial Intelligence*), научно и техничко обавештајне активности, енг. *Measurement and Signature Intelligence* (Юрьевич, 2014).

Тајне методе које су службе безбедности користиле током 70–их година XX века у Социјалистичкој Федеративној Републици Југославији, могу се поделити на две врсте: 1) методе за откривање, праћење и сузбијање делатности унутрашњег и спољног непријатеља; 2) методе за безбедносну заштиту одређених личности и објеката. Прве се спроводе у најстрожој тајности, а друге уз одобрење и знање целина где се спроводе (Цветковић, 2009). У Социјалистичкој Федеративној Републици Југославији, службе безбедности су примењивале велики број тајних метода, и то: врбовање међу грађанима Социјалистичке Федеративне Републике Југославије и странцима, информативне разговоре, тајне контроле телефонског, телепринтерског саобраћаја, поштанских пошиљака, тајна праћења, претресе станова, осматрања, фото и друге врсте документовања (Цветковић, 2009). У суштини, службе безбедности, како цивилне, тако и војне, примењивале су сличне тајне методе рада у документовању тајних делатности усмерених против државе и њених грађана, а радило се о

следећим методама: озвучење, контрола телефона, контрола преписке, тајни претреси, тајно праћење и провере (Цветковић, 2009). У суштини, до почетка деведесетих година прошлог века на простору бивше Социјалистичке Федеративне Републике Југославије нису постојали законски прописи који би ограничавали службе безбедности у тајном прикупљању података и који би системски регулисали наведену област. Међутим, свака служба је имала одређене подзаконске прописе, нормативе, најчешће у облику правила (Правило о раду Службе државне безбедности и др.) којима је регулисан њихов рад (Милосављевић, 2015). Ради се о подзаконским актима, који су тајног карактера, са одговарајућим степеном тајности, а којима су биле предвиђене одговарајуће мере за тајно прикупљање података, као и посебна овлашћења савезним, републичким и покрајинским секретарима унутрашњих послова, као и руководиоцима служби безбедности, да одобравају примену мера и њихово трајање (Милосављевић, 2015).

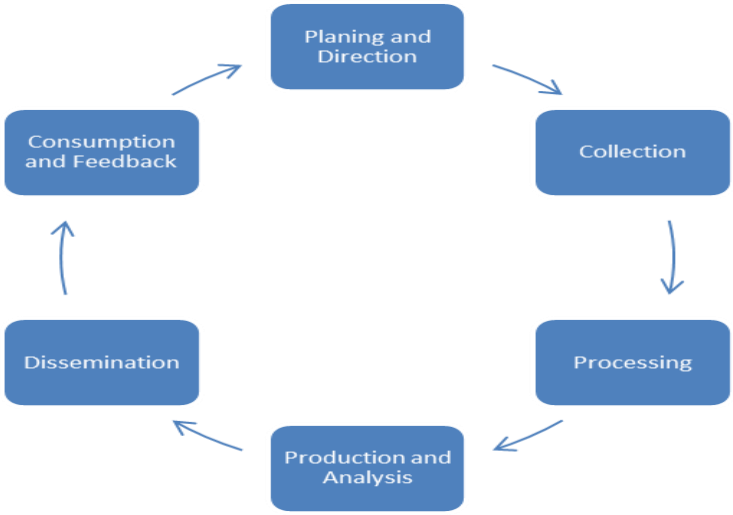
Наиме, када говоримо о тајним методама рада служби безбедности, тада превасходно мислимо на прикупљање безбедносно интересантних информација и података, експлоатацијом следећих техника рада: коришћењем различитих живих извора података (правна и физичка лица и др.), тзв. агентурни метод односно иследни метод рада; коришћењем различитих техничких и електронских средстава, тзв. комбиновани технички метод рада, као и коришћењем различитих јавно доступних отворених извора и сарадње са сродним службама безбедности, тзв. легални метод рада (Милошевић, 2001). Ради превентивне контраобавештајне заштите својих припадника служби безбедности, у РФ је путовање припадника служби безбедности (контраобавештајног карактера) „ограничено и они могу да иду на одмор само унутар граница РФ и не могу напустити РФ десет година након што напусте службу" (Riehle, 2022, p. 285). Наравно, овај вид ограничења они прихватају добровољно, а компензација за наведена одрицања је *повлашћен* статус у друштву (материјални, примање виших плата, обезбеђивање радних места члановима породица и слично, адекватно стамбено збрињавање и друге повластице које могу остварити у држави).

Легални метод рада служби безбедности представља коришћење и обраду података добијених из отворених јавних извора и размене података у односима сарадње са службама безбедности, при чему се такви подаци најчешће користе ради допуне осталим методама рада (Стајић и Лазић, 2015). У свету, један од познатијих таквих начина прикупљања података је уговор о сарадњи на пољу електронских обавештајних активности енг. *United Kingdom – United States Security Agreement* (потписан 1948. године између следећих служби безбедности: САД – Агенција националне безбедности, Канаде – Установа за безбедност комуникација, Велике Британије – Владин штаб за комуникације, Аустралије – Одбрамбени директорат за сигнале и Новог Зеланда – Биро за безбедност владиних комуникација). Централна компонента овог уговора о сарадњи чини пројекат *Ешалон* који врши пресретање свих радио, факс, телефонских и интернет комуникација, односно сателитских и дигиталних веза (Милошевић, 2001). Ангажовање ових пет служби безбедности је називано и *пет очију*.

Узимајући у обзир све наведено, тајне методе рада служби безбедности бисмо могли дефинисати као специјалне технике рада служби безбедности за тајно прикупљање безбедносно интересантних података којима се изузетно, на одређено време и без знања грађана, а на основу одлуке суда и под условима прописаним законом, одступа од појединих уставом зајемчених индивидуалних права (Милосављевић, 2015).

Када говоримо о другим службама безбедности (сличан начин рада како на Западу тако и на Истоку), тада констатујемо да према једном од циклуса настанка главног производа службе безбедности, а то је информација за крајњег корисника, наведено обухвата шест целина (*Шема 1*): Планирање и усмеравање, Прикупљање података (преко отворених и тајних извора), Обраду прикупљених података (где се додаје контекст у припреми за анализу), Обраду и анализу које претварају податке у информације, најбитније производе служби безбедности, Акцију ширења (дељења) информација са доносиоцима одлука, Коришћење и повратне информације политичких доносиоца одлука. Повратна информација служби безбедности укључује смернице државног руководства о будућим потребама служби безбедности, које се уносе у планирање и даје правац којим се поново покреће циклус (Harder, 2017).

Шема 1. The intelligence cycle, енг.



Извор: Harder, 2017, p. 4.

Обавештајни циклус обухвата процес издавања задатака, прикупљања података, обраде података, анализе расположивих података и дистрибуције (коришћења) информација од стране надлежних корисника. Процес обавештајног циклуса покреће дневне активности обавештајне заједнице. Можемо рећи да су „потрошачи" обавештајних података, односно државно и војно руководство и други доносиоци одлука којима су обавештајне информације потребне у обављању редовних дужности и одговорности, покретачи циклуса према обавештајној заједници. Ове потребе тј. захтеви су сортирани по приоритету у оквиру обавештајне заједнице и затим обавештајна заједница прикупља обавештајне податке. По завршеном прикупљању података, следи обрада истих и достављање корисницима информације. За то су задужени аналитичари у агенцијама који коришћењем свих техника, извора података, врше детаљније евалуације и процене прикупљених података интеграцијом података добијених од разних агенција и извора, па како класификованих тако и некласификованих. Таква процена доводи до тога да се обрађен податак, информација доставља надлежном кориснику ових информација. Повратне информације су део циклуса и преко њих се ствара слика степена реализоване претходне обавезе од стране обавештајне заједнице када се утврђује да ли има потребе за даљим прикупљањем података и новим анализама. Зато је графички приказ обавештајног циклуса на слици у наставку приказан у

кружном облику, јер се циркуларно понавља све док се не реализују у потпуности сви захтеви надлежних корисника услуга службе безбедности, обавештајне заједнице или друге организационе целине која се бави овим и сличним пословима (Weapons of Mass Destruction, 2005).

Службе безбедности прикупљају податке из различитих извора података ради могућности провере истих. Део тих извора података је јавно доступан, а део је поверљиве, тајне природе. Једна од подела извора података служби безбедности (*Слика 2*) може се представити на следећи начин:

– (енг. *Open source intelligence – OSINT*): употреба података отвореног извора за службе безбедности,

– (енг. *Human intelligence – HUMINT*): прикупљање података од људи као што су агенти, инсајдери и други доушници,

– (енг. *Signals intelligence – SIGINT*): подаци пресретнути из комуникационих система и електронске емисије, између осталих извора,

– (енг. *Imagery intelligence – IMINT*): снимање слика технологијом са земље, неба или из свемира,

– (енг. *Measurement and signature intelligence – MASINT*): технички и научни подаци добијени нуклеарним, оптичким, радиофреквенцијом, акустиком, сеизмичким или другим начином праћења.

Слика 2. Извори података служби безбедности.
Извор: Аутор.

Сви „сирови" подаци до којих се дође преко било ког од наведених извора података, постају информација за државне кориснике услуга служби безбедности тек када буду обрађени и анализирани што коначно тада добија на значају за евентуално коришћење од стране надлежних (Harder, 2017). У овој подели недостаје бар још један од врло битних извора података служби безбедности, а коју наведени аутор није предвидео – ради се о подацима добијеним сарадњом са партнерским службама безбедности (где треба бити изузетно опрезан услед коришћења наведених података), мада еволуцијом технологија које носи напредак првенствено у сајбер свету, информационих и комуникационих технологија и других, није искључено да се појаве и нове врсте извора података.

4.1.2.1. Јавно доступни извори података

Јавно доступни извори података, употреба података отвореног извора за службе безбедности (енг. *Open source intelligence*), подразумевају коришћење свих јавно расположивих извора података, доступних свима на коришћење, па и служби безбедности. Када говоримо о овој врсти извора података, мислимо конкретно на стручне књиге, научне часописе, зборнике радова, реферате са научних скупова, средства јавног информисања,

друштвене мреже и др. Поред наведених јавних извора, врло битан сегмент података за потребе рада служби безбедности могу бити и разни други извори података, како од државних органа тако и недржавних, који су јавно доступни. Тада мислимо на приступ разним базама података катастра непокретности, фондова, управа, организација и сл. што би користило у раду службе безбедности (Стајић и Лазић, 2015).

Јавно доступни извори података данас не представљају само праћење медија у својој и у другим државама или прикупљање података преко дипломатских представништава. Пренатрпаност интернета информацијама, укључујући и друштвене мреже, достигла је тај ниво да није могуће ручно вршити претраживања, а да у реалном времену дођете до података битних за службе безбедности (Димитријевић, 2022). Наиме, направљени су софтвери који аутоматизују прикупљање, па и селекцију података од значаја за оног ко организује прикупљање (Димитријевић, 2022). Постхладноратовски период карактерише велики број софтверских алата, за употребу података отвореног извора за потребе служби безбедности који се користе и они далеко превазилазе капацитете које су током хладног рата поседовали обавештајно – безбедносни системи великих сила (Димитријевић, 2022).

Комитет за тајну преписку (*кореспонденцију*) у САД је створио сопствену курирску службу и малу аналитичку јединицу, која се бавила аналитичком обрадом информација добијених из отворених извора података (Юрьевич, 2014). У даљем делу истраживања ће бити више речи о овом комитету.

4.1.2.2. Човек – извор података

Прикупљање података од људи (енг. *Human intelligence*), агентурни, односно иследни метод рада служби безбедности представља најстарији метод прикупљања података „још док су уходе и шпијуни били једино средство и начин за прикупљање података о противнику" (Марјановић, Лабовић и Браковић, 2022, стр. 209), коришћењем човека као прикривеног или отвореног извора података, односно инфилтрацијом припадника службе или агентурне мреже у структуре страних држава и организација. Сарадња са човеком као извором података, представља свестан и континуиран однос службе са појединцем помоћу кога се долази до безбедносно интересантних података, а сам поступак ангажовања и коришћења је неизоставан метод рада службе безбедности, с обзиром на то да се ради о непосредном извору безбедносних сазнања (Марјановић, Лабовић и Браковић, 2022).

Операције које реализују људи се не могу одвијати без агената. Врло често коришћена реч, агент, се меша у значењу. Агент није припадник службе безбедности, већ лице које је служба безбедности ангажовала као извор података. То је једна од врста извора података (Riehle, 2022). Припадник службе безбедности може такође да се користи као извор података (ретко), али његов назив није агент, већ се зависно од службе у којој се налази запослен зове најчешће оперативац, овлашћено службено лице, референт или слично, и поред тога има свој чин (уколико се ради о војној служби безбедности) или други назив хијерархијског статуса припадника службе (у цивилним службама безбедности). Службе безбедности углавном траже услуге од агената високо позиционираних у једном друштву и најбитније је да имају приступ битним тајним подацима и утицај на одређене битне активности у друштву како би били што кориснији за потребе служби безбедности. Уколико припадник службе безбедности мора да ангажује агента (извор података), он користи податке којима се идентификују рањивости тог агента, а које се евентуално могу искористити уколико је

неопходно убедити агента да сарађује са службом безбедности, што представља један вид присиле (Riehle, 2022). Овде је битно нагласити да је репресија, присила у раду са људима као изворима података углавном ознака немоћи, неспособности и неадекватне обучености и рада оперативца службе безбедности. Присила за ангажовање извора податка треба да представља изузетак када не постоји могућност за реализацију одређеног ангажовања, а не правило (велики је број разлога и то представља најлакши начин ангажовања извора података).

За потребе реализације задатка спољно – политичке природе где су ангажоване службе безбедности РФ, регрутује се и друго руско особље, које није у саставу службе безбедности нити је агент, а налази се у иностранству. То су представници необавештајних организација, дипломате, као грађани РФ, или понекад као верски представници православне цркве. Службе безбедности у Савезу Совјетских Социјалистичких Република су подразумевале да дипломате подржавају задатке служби безбедности и уступају податке службама безбедности ако им се приближе, што није искључено да је присутно и данас (Riehle, 2022).

Резидентура служби безбедности РФ у иностранству се састоји од различитих улога припадника једне резидентуре. Ту спадају улоге почев од резидента (он је шеф и бира се као врхунски кадар у свом послу и он контактира са службом безбедности у РФ и управља канцеларијом – резидентуром) до службеника за случајеве, који спроводе операције (који су подељени унутар Спољне обавештајне службе у резидентуре у „линије рада" за политичке активности, научне и технолошке, подршка илегалцима, контраобавештајна и безбедносна, надзор руске дипломатске заједнице у иностранству, обавештајни подаци о емигрантима) и помоћног особља које пружа услуге комуникације, шифранти и сличне евиденције о досијеима, електронски мониторинг, радио и други оператери, особље за одржавање рачунара, особље за одржавање моторног возила (поред исправности битно је да нема постављене уређаје за праћење и сл.), као и друге службе и одржавања (Riehle, 2022).

Раније Комитет државне безбедности, а затим Главна обавештајна управа, служба безбедности РФ је била фокусирана на припрему активности за критичне инфраструктурне локације, укључујући детаљне информације о терену, знаменитостима, клими током различитих годишњих доба, преовлађујућим ветровима, насељеним подручјима и локалним обичајима. Те активности би подржавале инфилтрацију диверзионо – обавештајних група (рус. *диверсионноразведывательные группы*), тимова оперативаца који би се тајно инфилтрирали ваздушним или морским путем да би реализовали саботажне активности на критичне инфраструктуре циљане државе. Податке о свом раду на обавештајним и необавештајним активностима тада Тринаестог одељења Комитета државне безбедности (касније преименованог у Одељење В), дао је Олег Љалин[13], официр Комитета државне безбедности, који је пребегао у Уједињено Краљевство у септембру 1971. године. Љалин је наведеном приликом испричао да су његове мете критичне инфраструктуре укључивале железнице, јавна предузећа, владине и војне комуникације, владине канцеларије и локације за континуитет рада, као и хитне залихе хране које би за напад користиле ваздушне и

[13] Олег Љалин, официр Комитета државне безбедности, био је наводно одговоран за идентификацију, прикупљање информација и планирање саботажних акција на критичне инфраструктурне локације (Riehle, 2022).

поморске диверзантске јединице Савеза Совјетских Социјалистичких Република (данас РФ) ако би избио рат са Западом. Посебан задатак Љалина био је да формира мрежу агената који би имали обавезу да, уколико дође до оваквих и сличних интервенција унутар Уједињеног Краљевства, прихвате и подрже оперативце за реализацију саботажне активности када дођу на територију Уједињеног Краљевства. Љалин је нагласио да Комитет државне безбедности није спроводио оно што је он назвао *индустријском саботажом* у миру, већ да су наводно све активности биле припремане искључиво за ратно стање, односно непосредне ратне активности (ванредно стање). Саботажне мере би обухватале деморализацију становништва, војног и цивилног, као и ремећење политичког и економског живота државе. Љалин је у Уједињеном Краљевству идентификовао и свог колегу из Комитета државне безбедности који је обављао послове исте мисије у САД. Олег Калугин, каснији пребег из Комитета државне безбедности, писао је да је свака велика резидентура Комитета државне безбедности широм света имала по једно Одељење В, официра са задатком да се припреми за будући рат. Митрохин је потврдио да се Савез Совјетских Социјалистичких Република (РФ) не спрема само на циљање инфраструктуре у САД и Великој Британији већ и у другим државама, где је поменуо да је планирање необавештајних[14] активности служби безбедности било активније у Ирану него у било којој другој незападној држави (Riehle, 2022). Да се методе рада од хладног до постхладноратовског периода нису много промениле, потврђује и следеће. Наиме, почетком 2020. године полиција у Ирској је ухапсила припаднике служби безбедности РФ које је очигледно мапирало прецизне локације тачака за подморске оптичке каблове у Ирској (Riehle, 2022). Поред пребега, западне службе безбедности су се бавиле офанзивним деловањем, продорима у војну службу безбедности РФ, Главну обавештајну управу током и након Хладног рата, стварањем *двојних агената*, који су пружили вредне информације о службама безбедности других држава и другим организацијама везаним за систем безбедности, а ради се о следећим лицима: „Петр Попов (1953–58), Дмитриј Пољаков (1960–85), Олег Пенковски (1961–62), Сергеј Скрипал (1995–2001) и др.” (Riehle, 2022, p. 181).

4.1.2.3. Употреба техничких средстава

Комбиновани технички метод рада служби безбедности представља тајну опсервацију објекта интересовања (организације и појединци) са истовременом применом и коришћењем различитих техничких и електронских средстава, ради откривања, пресецања и документовања потенцијалних носилаца недозвољене делатности, а чиме се одступа од законом загарантованих права о неповредивости тајне писама и других средстава општења лица (Марјановић, Лабовић и Браковић, 2022).

Службе безбедности имају посебна законска овлашћења. Ове моћи зависе од националног контекста и функција служби безбедности и не би требало да крше међународне и законе о људским правима. Међутим, службама безбедности је законски дозвољено ограничавање људских и грађанских права у одређеним случајевима прописаним законом. Тајне операције усмерене на сузбијање претњи на националну безбедност, понекад

[14] Службе безбедности Савеза Совјетских Социјалистичких Република су шездесетих и седамдесетих година XX века испланирале детаљно нападе на Иран, краљевске палате, главна министарства, главну железничку станицу, седиште полиције и тајне полиције *Савак*, телевизијске и радио зграде, станице за пренос електричне енергије и телефонске централе (Riehle, 2022).

су у супротности са законима (Harder, 2017). Важно је напоменути да су у активностима унутрашњих служби безбедности, што се тиче примене техничких средстава (подаци пресретнути из комуникационих система и електронске емисије енг. *Signals intelligence,* снимање слика технологијом са земље, неба или из свемира енг. *Imagery intelligence,* технички и научни подаци добијени нуклеарним, оптичким, радиофреквенцијом, акустиком, сеизмичким или другим начином праћења енг. *Measurement and Signature Intelligence – MASINT*), прописи веома ригорозни и врло често је неопходно одобрење најчешће надлежних судова и/или надлежних руководилаца служби (само за одређене врсте примене техничких средстава у раду овлашћених службених лица служби безбедности или специфичне ситуације, случајеве ради хитности реаговања) за коришћење и употребу ове врсте средстава, међутим, када се ради о примени техничких средстава у иностранству од стране спољних служби безбедности, односно њених извршилаца, ради се о незаконитим употребама истих на територији и за државу где се примењују.

Дана 4. марта 2018. године, бивши официр војне службе безбедности РФ, Главне управе (некада Главне обавештајне управе), Сергеј Скрипал (енг. *Sergei Skripal*), и његова ћерка били су изложени високо токсичном и потенцијално смртоносном хемијском оружју у Солсберију, Уједињено Краљевство, а РФ и њене службе безбедности, војна служба безбедности Главна управа су убрзо окривљени за напад. Агенти војне службе безбедности Главне управе су на крају идентификовани у Солсберију и оптужени за напад. Британске власти су наводно идентификовале хемијско оружје као новичок, класу нервног агенса развијеног у Савезу Совјетских Социјалистичких Република. Узорци су послати Организацији за забрану хемијског оружја у Хагу, Холандија ради провере налаза. Организација за забрану хемијског оружја је такође истраживала тврдње о наводном гасном нападу у Сирији од стране режима Башара ал Асада на град Дума. Четири агента војне службе безбедности Главне управе су дана 10. априла 2018. године путовали са дипломатским пасошима када су ушли у Холандију. Дана 11. на 12. април, агенти су извршили извиђање подручја око седишта Организације за забрану хемијског оружја у Хагу и резервисали собе у хотелу непосредно поред Организације за забрану хемијског оружја у Хагу. Ангажовањем служби безбедности Велике Британије и Холандије ухапсиле су четворицу мушкараца 13. априла. У аутомобилу агента војне службе безбедности Главне управе откривена је високотехнолошка опрема, која је могла да се користи за хаковање у Организацији за забрану хемијског оружја у Хагу и то енг. *Wi–Fi* мреже. Опрема је заплењена, а агенти протерани из државе. Након тога су Холандија и Велика Британија одржале заједничку конференцију за новинаре 4. октобра 2018. године када је детаљно описана читава операција војне службе безбедности Главне управе и идентификовани агенти. Истовремено, Аустралија, Нови Зеланд, Канада и Североатлантски савез објавили су изјаве у којима подржавају идентификацију злонамерне сајбер активности из РФ и осудиле активности служби безбедности РФ. Реакција на напад на Скрипала и покушај хаковања Организације за забрану хемијског оружја у Хагу је била енергична и удружена (можемо слободно констатовати операција), где је више од 26 држава протерало више од 150 дипломата РФ. Велика Британија је протерала 23 дипломате, САД су протерале 60 званичника и затвориле руски конзулат у Сијетлу и два рекреативна објекта која се наводно користе за прикупљање обавештајних података у Мериленду и Лонг Ајленду (Bowen, 2021).

Економско и научно – технолошко прикупљање података служби безбедности су веома моћни алати које Влада РФ може и користи у одржавању, али и у расту економске и војне снаге РФ. Када су у питању нафта и гас, они представљају битан сегмент у доношењу било какве одлуке о економској и националној безбедности РФ. Интензивирање прикупљања оваквих података за потребе државног руководства РФ полази од темељне претпоставке да је већи део окружења РФ непријатељски расположен, где су економске санкције осмишљене са циљем да промене непријатељско геополитичко понашање РФ према непријатељским државама. У претходним примерима смо могли да констатујемо да су се службе безбедности у политичким активностима углавном ослањале на *техничке методе*, компјутерски засноване методе рада, о чему сведочи операција енг. *SolarWinds* 2020. године, а оно што је до сада присутно у јавности јесте да су операције засноване на човеку као извору података и реализатору одређених задатака преовладале у иностраном економском и научно – технолошком прикупљању података. Чињеница је да унутар РФ (уосталом као и све унутрашње службе безбедности држава), Федерална служба безбедности има скоро потпуну контролу над телекомуникационим окружењем, па у великој мери користе *технички*, па и компјутерски надзор за праћење економских и политичких активности, користећи ресурсе служби безбедности, контраобавештајног карактера (Riehle, 2022).

У XXI веку не можемо да говоримо о сакупљању података и политичким активностима служби безбедности, а да не говоримо о техничкој платформи коју користе службе безбедности РФ том приликом. Техничка платформа обухвата три основна облика (на копну у РФ или на територији под руском контролом, у амбасади, блиски приступ, поморски, ваздушни, сателитски; углавном у надлежности војне службе безбедности, Главне управе, некада Главне обавештајне управе), затим геопросторне обавештајне податке (енг. *Geospatial intelligence*) и активности засноване на компјутеру (често називан сајбер). Све ове техничке платформе подржавају све врсте активности служби безбедности РФ (према подели у РФ ради се о *политичким, економским и научно – технолошким, војним и тајним операцијама*). Веома је важно нагласити да већи део техничких платформи није могуће користити и/или опслуживати без човека као извора података (нпр. ради приступа материјалу кодова и шифрама, или кроз тајна путовања припадника служби безбедности на локације широм света ради спровођења техничких операција блиског приступа, инсталирања средстава и др. опслуживања – *Слика 3*) што говори о неопходности примене више метода рада служби безбедности (Riehle, 2022).

Слика 3. Соба за експлоатацију пресретнутих података из комуникационих система и електронске емисије од стране службе безбедности у хотелу Виру у Талину, Естонија (*Viru in Tallinn, Estonia*).
Извор: Riehle, 2022, p. 261.

Економски раст РФ од 2000. године, довео је до завршетка дуго одлаганих техничких система. Модернизоване верзије сателитских система за прикупљање података почеле су да се појављују око 2010. године, а неколико система је почело са радом од 2015. године. Наводно, на основу истраживања руске председничке академије за националну економију и јавну управу 2018. године, све је већи број образованих држављана РФ који напушта државу из економских и/или политичких разлога, што за област коришћења техничких платформи може дугорочно направити недостатак стручног кадра (Riehle, 2022). Како би након распада Савеза Совјетских Социјалистичких Република, РФ створила независност и што се тиче лансирних локација, од 2005. године, РФ тражи лансирну локацију на истоку РФ како би задржала водећи технолошки статус РФ. Тако је лансирно место Восточниј у Амурској области, РФ, лансирало своје прво беспилотно возило 2015. године и своје прво возило са посадом 2018. године. Други сегмент се односи на интеграцију људских и техничких способности прикупљања података. Сајбер операције од стране РФ порасле су у квантитету и агресивности у протеклој деценији. Инциденти служби безбедности РФ који су до сада јавно откривени указују на комбинацију примена метода рада служби безбедности и то: прикупљање података од људи, техничких операција блиског приступа, података битних за службе безбедности отвореног кода, затим сателитског прикупљања података, ваздушног и прикупљања података на мору и сајбер напада (Riehle, 2022).

Терминолошки и у пракси, за израз тајне методе рада служби безбедности Републике Србије везује се двојако значење. Прво, системским законима којима се уређује рад служби безбедности Србије, за тајне методе рада служби безбедности користи се неколико термина (Марјановић, Лабовић и Браковић, 2022). Војнобезбедносна агенција користи израз *Посебни поступци и мере*, који је као такав предвиђен Законом о Војнобезбедносној агенцији и Војнообавештајној агенцији, а преузет из одредби Закона о основама уређења служби безбедности Републике Србије, док Безбедносно – информативна агенција користи термин *Посебне мере којима се одступа од неповредивости тајне писама и других средстава општења*, предвиђен одредбама Закона о Безбедносно – информативној агенцији, који су садржински исти, а полиција користи термин *Мере циљане потраге*, дефинисан Законом о полицији Републике Србије (Марјановић, Лабовић и Браковић, 2022). Друго, пандан тајним методама рада које су предвиђене системским законима служби безбедности Републике Србије су и *Посебне доказне радње* предвиђене одредбама Закона о кривичном поступку Републике Србије[15], које службе безбедности Републике Србије тајно примењују у документовању и пресецању тешких кривичних дела и дела организованог криминала (Марјановић, Лабовић и Браковић, 2022).

Службе безбедности РФ, посебно Спољна обавештајна служба и војна служба безбедности Главна управа (некада Главна обавештајна управа), у великој мери се ослањају на прикупљање података радом са људима, спроводећи операције широм света. Модерна технологија је учинила тајне операције прикупљања података од људи ризичнијим и тежим, али настављају да истичу битност овог вида активности служби безбедности. У постхладноратовском периоду, а поготово од 2014. године, дипломатски односи РФ претрпели су бројне неуспехе односно службе безбедности страних држава, држава

[15] Види шире: Миодраг Плазинић, Милован Стојковић, Примена посебних доказних радњи и механизми њихове контроле, *Тужилачка реч*, Гласило удружења тужилаца Србије, бр. 28, 2015.

домаћина су предузимале преко руководства својих држава мере за ремећење рада стране службе безбедности на својој територији тако што су периодично вршили протеривања дипломата РФ по разним основама. По овим превентивним поступцима тј. протеривању од стране служби безбедности (преко руководства државе), предњачиле су САД из којих је протерано преко 100 држављана РФ од 2016. године, а овај поступак није стран ни такозваним „пријатељским државама" РФ, као што су Грчка, Аустрија и Мађарска (Riehle, 2022).

4.1.2.4. Сарадња са партнерским службама

Сарадња служби безбедности са страним службама подразумева везу или сарадњу између различитих држава или тела у сврху одбране или заштите националне безбедности. Размена информација може бити важна за спречавање тероризма, потрага за ратним злочинцима, сузбијање организованог, транснационалног криминала и слично. Разлози за наставак такве сарадње су: добијање информација које би иначе било тешко прикупити, прикупљање алтернативних перспектива о претњама; смањење и избегавање високог ризика за активности прикупљања неких података. Може бити корисна у мултилатералним ситуацијама, размене расположивих заједничких процена и стратешке перспективе или ради подршке мултинационалним операцијама (Harder, 2017). Међународна сарадња служби безбедности сама по себи већ укључује одређене ризике уопште такве комуникације, који се огледају у неизвесности у вези са намерама потраживања одређених информација, саме природе могућности провере добијених података који би требало да представљају већ готову информацију (што не мора да значи) или начина (откривања метода) на који су до њих дошле службе безбедности. Код служби безбедности великих сила, говоримо и о репутационим ризицима, мада не треба искључити ни могућност кршења међународног права у неким ситуацијама ради реализације одређених захтева (Harder, 2017).

4.1.3. Облици угрожавања државе из делокруга рада служби безбедности

У највећем броју служби безбедности на планети, њихове надлежности се огледају мање – више у сагледавању сличних активности ради супротстављања (или бављењем истим према другим државама), и то: страним обавештајним службама, екстремизму и тероризму, организованом криминалу и корупцији, као и другим облицима угрожавања безбедности државе.

4.1.3.1. Стране обавештајне службе

Други светски рат је довео Савез Совјетских Социјалистичких Република до критичног момента када је било питање опстанка државе и народа у Савезу Совјетских Социјалистичких Република. Након оваквих поступака, правци деловања служби безбедности су били спајање шпијунаже и саботаже у једну мисију. У Савезу Совјетских Социјалистичких Република, активности службе безбедности (иностраног карактера) су биле подељене на две линије, и то обавештајну и диверзиону. У почетку је обавештајна управа била одговорна за прикупљање обавештајних података о Немачкој и њеним савезницима, док је Дирекција за диверзије слала тимове за „обавештајну саботажу" иза немачких линија. Обавештајна управа је обезбеђивала обавештајне податке за Дирекцију како би могла да реализује задатке и обрнуто, официри из ове Дирекције су сарађивали са Управом. Ово обележје је задржано до данас. Савез Совјетских Социјалистичких Република је оживљавао

мреже агената у Великој Британији и САД док је до 1943. године са својим службама безбедности формирао нове резидентуре агената у Отави у Канади и Канбери у Аустралији. Након Другог светског рата, овај нагласак на ратним савезницима прешао је у оно што је касније постало познато као Хладни рат. Одређење шпијунаже је било одраз сопствене праксе у Савезу Совјетских Социјалистичких Република, које је чинило комбинацију прикупљања обавештајних података и саботажу заједно. До 1970. године, Комитет државне безбедности је створио Пету дирекцију, одговорну за праћење „идеолошке субверзије". Између 1985. и 1991. године, преко 30 совјетских обавештајних службеника је пребегло. У августу 1991. године, директор Комитета државне безбедности, Владимир Крјучков, појавио се као један од вођа покушаја државног удара (неуспелог) против Горбачова, што је довело до негативне репутације Комитета државне безбедности. Хапшењем Крјучкова, Горбачов је именовао Вадима Бакатина, министра унутрашњих послова, за директора Комитета државне безбедности. Бакатин је добио задатак од Горбачова да уништи службу безбедности, Комитет државне безбедности, а Горбачов је то написао на следећи начин: „Традиције чекизма треба искоренити, чекизам као идеологија мора да прекине своје постојање. Морамо се придржавати закона, али не и идеологије" (Riehle, 2022, p. 45, 46). Године које су уследиле указују на то да је Крјучков имао вероватно одличну процену везану за Горбачова, али изузетно лошу за планирање и реализацију специјалне операције, у медијима назване државни удар (Riehle, 2022).

У периоду од 2008. године војна служба безбедности РФ, Главна управа (некада Главна обавештајна управа) је развила значајне сајбер способности, допуњујући своје дугогодишње искуство у извођењу психолошких и информационих операција. Развој сајбер способности Главне обавештајне управе поклопио се са два шира развоја у руском безбедносном и војном размишљању, примени ненасилних средстава у сукобима и информационом рату. Граница између мира и сукоба постаје све нејаснија. Употреба ненасилних средстава је све важнија. Руска Федерација сајбер операције доживљава као ефикасно и релативно јефтино оруђе за подривање. У РФ влада мишљење да су западне владе манипулисале информацијама како би збациле непријатељске режиме. Током протеста у Белорусији против председника Александра Лукашенка 2020. године, шеф службе безбедности РФ, Спољне обавештајне службе, Сергеј Наришкин (*Sergey Naryshkin*), оптужио је Запад да спроводи лоше прикривен, односно, како он каже, покушај организовања друге „обојене револуције" и пуч. РФ је офанзивно врло често користила сајбер операције за постизање циљева руске спољне политике и кажњавање противника. Укључивали су офанзивне нападе на стране електричне мреже, банкарски сектор, владине институције, па чак и спортске догађаје. Федерална служба безбедности се за развој својих сајбер способности, према извештавању медија и на основу савезних оптужница, ослања на метод присиљавања и регрутовања талентованих појединаца из РФ, сајбер – криминалаца, често под претњом кривичног гоњења док је насупрот томе војна служба безбедности РФ, Главна управа (некада Главна обавештајна управа), очигледно настојала да интерно негује таленат и развије вишеструке путеве регрутовања. Због својих поступака рада у овој области, војна служба безбедности Главна управа (некада Главна обавештајна управа) је могла да развије своје способности у сајбер операције (Bowen, 2021).

Деловање страних служби безбедности у Стратегији националне безбедности Републике Србије је одређено на следећи начин: „Обавештајна делатност страних субјеката

који у континуитету делују ка политичким, економским и безбедносним чиниоцима у Републици Србији, поред осталог и кроз субверзивно – пропагандне активности усмерене ка покушајима дестабилизације институција и изазивања тензија у друштву, представља претњу безбедности Републике Србије" (Стратегија националне безбедности Републике Србије, 2019, стр. 27). У суштини, већи део овог одређења у стратегији представља матрицу у супротстављању како обавештајним, тако и необавештајним активностима које такође спроводе службе безбедности, а на западу су првенствено препознате кроз политичке, пропагандне, економске, паравојне активности.

4.1.3.2. Тероризам

Док је „тероризам облик насилног екстремизма, а тероризам је такође често мотивисан идеолошки, концептуална основа тероризма која га разликује од насилног екстремизма је у стварању страха или терора као средства за постизање циља" (United Nations Educational, Scientific and Cultural Organization, 2017, p. 19). Конвенција Већа Европе о спречавању тероризма је одређена као добра међународна пракса за дефинисање кривичних дела „јавно провоцирање извршења терористичког дела", „регрутовање за тероризам" и „обучавање за тероризам". Резолуција Савета безбедности Уједињених нација број 1373 обавезује државе да сузбијају терористичко регрутовање и Резолуција 1624 (2005) позива државе да забране, законом, подстицање на чињење терористичких аката (што је у законодавству Републике Србије и прописано). Посебно, дело подстрекавања на чињење терористичког акта ће бити у складу са људским правима ако се фокусира на директно подстрекавање, са намером да се промовише тероризам, и ако се утврди узрочна веза заснована на доказу, између подстрекавања и вероватне реализације терористичког акта. Подстрекавање на тероризам и регрутовање у тероризам треба да буду инкриминисани и кривично гоњени у складу са међународним стандардима о људским правима. Ставове који се сматрају радикалним или екстремним, као и њихово мирно изражавање, не треба инкриминисати. Природа тероризма као тешког кривичног дела је таква да ће полиција или друге надлежне државне службе безбедности највероватније ради документовања недозвољене делатности морати да примене посебне поступке и мере (Organization for Security and Co–operation in Europe, 2014).

Када се са стратегијског аспекта у РФ посматра тероризам као појава, он се сагледава као политичка претња режиму РФ. Сваки насилни чин који штети утицају или престижу РФ у свету, из њиховог угла представља тероризам. Када наведено поменемо, тада се под оваквом формулацијом може дати тумачење које може укључивати било шта, од исламистичког екстремизма до протеста против Владе РФ на изборима. Када правимо компарацију са тумачењем појмовног одређења у САД где имамо одређење тероризма као незаконите употребе насиља и застрашивања, посебно против цивила, а у остваривању политичких циљева, долазимо и до првог обележја и разлика између РФ и САД где се у РФ било шта може сврстати под ово одређење, док је у САД извршено сужење могућности подвођења одређеног деловања под појмовно одређење тероризма (Riehle, 2022). Директор Спољне обавештајне службе Сергеј Наришкин (*Sergey Naryshkin*) је 2017. године изјавио следеће: „Ви сте добро свесни изазова са којима се Русија суочава. Они укључују покушаје да се обузда наш развој, да се наметне конфронтација, да се дестабилизују региони у близини руских граница, укључујући коришћење терористичких и екстремистичких група као оружја.

Није тајна да су неки од њих пажљиво неговани, па чак и добили директну подршку од специјалних служби бројних земаља" (Riehle, 2022, p. 102). Овде се добро региструје наглашавање утицаја страних служби безбедности у стварању, организацији и деловању тероризма, али с обзиром да је Сергеј директор једне озбиљне службе безбедности, он је у свом обраћању био умерен и прецизан, док су политичари у РФ исту област одредили на следећи начин. Приликом реализације емисије са познатим продуцентом Оливером Стоуном (*Oliver Stone*) 2015. године, председник РФ Владимир Путин је утицај страног фактора (страних служби безбедности) описао следећом реченицом: „Не морате бити велики аналитичар да бисте видели да САД подржавају финансијски, дају информације и политички подржавају чеченске терористе. Они су подржавали сепаратисте и терористе на Северном Кавказу" (Riehle, 2022, p. 102).

Дана 16. септембра 2022. године медији су објавили да су у року од неколико сати терористи убили пет руских званичника на територији коју контролишу снаге РФ у Украјини, а били су стотинама километара удаљени једни од других од Луганска, Херсона, Бердјанска. И сам председник РФ је на питање новинара на телевизији у вези са овим убиствима одговорио да се ради о терористичком акту. Кримски мост је оштећен 8. октобра 2022. године у терористичком акту због којег је као одмазду на овај чин РФ 10. октобра 2022. године учинила велики број напада ракетама високог домета и разорне моћи на Украјину. Такође, терористички акт је забележен у РФ и 15. октобра 2022. године на полигону у Солотију када је погинуло 11 лица, а 15 повређено. Дана 19. октобра 2022. године Федерална служба безбедности је ухапсила агента Службе безбедности Украјине који је покушао да изведе терористичке акте у Подмосковљу са две ракете за противваздухопловну одбрану типа *Игла*. Наведено је само неколико терористичких аката и у све ове акте су уплетене службе безбедности Украјине и других западних држава као организатори или подршка, што је било квалификовано као необавештајна активност ових служби.

У Стратегији националне безбедности Републике Србије тероризам је дефинисан на следећи начин: „Тероризам представља велики ризик и озбиљну претњу безбедности Републике Србије. Извођење терористичких аката на њеној територији може усложити политичко – безбедносну ситуацију. Република Србија и њени грађани, у земљи и иностранству, могу бити објекти терористичког деловања, а њена територија може бити злоупотребљена за транзит, припрему и извођење терористичких акција у другим државама, што је неприхватљиво" (Стратегија националне безбедности Републике Србије, 2019, стр. 26). У Стратегији одбране Републике Србије, тероризам је одређен као „асиметричност претње тероризма и његове повезаности са организованим криминалом имплицирају могућност извођења терористичких аката на територији Републике Србије, првенствено ради остваривања политичких циљева. Осим непосредног испољавања тероризма, безбедност и одбрана Републике Србије могу бити угрожени терористичким деловањем и коришћењем њене територије за транзит, припрему и извођење терористичких акција у другим земљама" (Стратегија одбране Републике Србије, 2019, стр. 21). О озбиљности терористичких аката је сулудо и говорити, зато се ова претња и налази регистрована у највишим стратешким документима једне државе, али је неопходно и констатовати да је извршење у директној вези са политичким циљевима где се опет могу препознати трагови других држава односно њихових служби безбедности.

У Републици Србији Кривичним закоником из 2005. са свим допунама 2009, 2012, 2013, 2014, 2016, 2019. године у члану 391. је одређено Кривично дело, односно дефинисано је шта је то тероризам: поступак лица које „у намери да озбиљно застраши становништво, или да принуди Републику Србију, страну државу или међународну организацију да нешто учини или не учини, или да озбиљно угрози или повреди основне уставне, политичке, економске или друштвене структуре Републике Србије, стране државе или међународне организације: нападне на живот, тело или слободу другог лица, изврши отмицу или узимање талаца, уништи државни или јавни објекат, саобраћајни систем, инфраструктуру укључујући и информационе системе, непокретну платформу у епиконтиненталном појасу, опште добро или приватну имовину на начин који може да угрози животе људи или да проузрокује знатну штету за привреду, изврши отмицу ваздухоплова, брода или других средстава јавног превоза или превоза робе, производи, поседује, набавља, превози, снабдева или употребљава нуклеарно, биолошко, хемијско или друго оружје, експлозив, нуклеарни или радиоактивни материјал или уређај, укључујући и истраживање и развој нуклеарног, биолошког или хемијског оружја, испусти опасне материје или проузрокује пожар, експлозију или поплаву или предузима друге опште опасне радње које могу да угрозе живот људи, омета или обустави снабдевање водом, електричном енергијом или другим основним природним ресурсом које може да угрози живот људи.” Поред овог одређења тероризма у Кривичном законику, дефинисана је последица, санкција и за оног „ко прети извршењем овог Кривичног дела, затим да уколико је при извршењу овог Кривичног дела наступила смрт једног или више лица или су проузрокована велика разарања, па ако је при извршењу овог Кривичног дела учинилац са умишљајем лишио живота једно или више лица, казниће се још вишом казном. Такође, за лица која набављају или оспособљавају средства за извршење овог Кривичног дела или отклањају препреке за његово извршење или са другим договара, планира или организује његово извршење или предузме другу радњу којом се стварају услови за његово непосредно извршење, ко ради извршења овог Кривичног дела упућује или пребацује на територију Републике Србије лица или оружје, експлозив, отрове, опрему, муницију или други материјал.” Као допуне члана 391. су придодата четири параграфа о кривичној одговорности за оног ко: „а) јавно подстиче на извршење терористичких дела где је одређено да ко јавно износи или преноси идеје којима се непосредно или посредно подстиче на вршење кривичног дела из члана 391. овог законика, и параграф б) који прецизира одговорност лица која спроводе врбовање и обучавање за вршење терористичких дела, параграф в) који предвиђа употребу смртоносне направе и параграф г) који предвиђа уништење и оштећење нуклеарног објекта” (Кривични законик, 2005, 2009, 2012, 2013, 2014, 2016, 2019; члан 391). Можемо да констатујемо да, како се практично развијао тероризам у пракси, тако су нормативи покушавали да пропрате наведено кроз одређења у закону, али да се и у овом случају оставља на процени надлежних државних институција шта је то јавно подстицање, шта врбовање и обучавање, шта употреба смртоносне направе и слично, где може да се појави евентуална злоупотреба, намерна или ненамерна.

4.1.3.3. Екстремизам

Заузимање ставова или веровања која се сматрају радикалним или екстремним, као и њихово мирно изражавање не треба сматрати кривичним делима. Екстремизам не би требао бити разлог за предузимање мера од стране службби безбедности или полиције ако нису

повезани са насиљем, или неком другом незаконитом радњом, како је правно дефинисано у складу са међународним правом. Екстремни појединци или групе које не прибегавају потстрекавању и одобравању криминалних активности и/или насиља не треба да буду циљ кривичног правосуђа (Organization for Security and Co–operation in Europe, 2014). Екстремизам значи „веровање и подршка идејама које су веома далеко од онога што већина људи сматра исправним или разумним". Екстремизам се односи на ставове или понашања која се сматрају изван норме. Важно је нагласити субјективну природу овог термина, јер исти може попримити различита значења у зависности од тога ко дефинише норму и одлучује шта је прихватљиво или не у складу са тим. Насилни екстремизам се односи на поступке људи који подржавају или користе насиље за постизање идеолошких, верских или политичких циљева. Ово укључује тероризам и друге облике политички мотивисаног и секташког насиља. Насилни екстремизам идентификује непријатеља, или непријатеље, који су предмет мржње и насиља (United Nations Educational, Scientific and Cultural Organization, 2017, p. 19). Генерално, насилни екстремизам се односи на насиље које се оправдава или је повезано са екстремном религиозном, социјалном или политичком идеологијом (Organization for Security and Co–operation in Europe, 2018). Екстремизам[16] је са теоријског становишта тешко дефинисати. Када говоримо о екстремизму, тада говоримо о понашању које се налази на граници дозвољеног, са тенденцијом да се та граница пређе (те границе су у форми обичаја, закона, религијских и моралних норми, тако да је и поимање екстремизма различито). Тако се у једној средини иста појава може сматрати екстремизмом, док у другој, у којој су другачије норме понашања, то није случај (Ђорић, 2012). Екстремисти су за западноевропске политикологе почетком двадесетог века били бољшевици у Русији који су узели учешће у Октобарској револуцији, па се екстремизам овде везује за левицу. Касније, екстремизам се приписивао и десници у форми фашизма и нацизма. Значајан допринос у теоријском одређењу екстремизма је дао немачки научник Уве Бакес (*Uwe Backes*) који је осамдесетих година двадесетог века заједно са Екхардом Јесеом (*Eckhard Jesse*) истраживао овај феномен унутар академских кругова (Ђорић, 2012). Док се екстремизам сматра понашањем које тежи да пређе границу дозвољеног, радикализам[17] указује на корените промене у друштву које не морају бити негативне (Ђорић, 2012). Препознајемо екстремизам свуда око нас, у политици, култури, спорту, уметности, религији. Када говоримо о академској дефиницији екстремизма, она није још увек прецизно одређена. Екстремизам се препознаје по насилности, односно потенцијалној спремности за вршење насиља као и по веома деструктивном својству уколико пређе у тероризам. Сваки тероризам је потврђени екстремизам на делу. Врло је тешко одредити екстремизам, како теоријски тако и из угла правне регулативе. Ова недореченост ствара проблеме полицији и судовима у извршавању послова из своје надлежности, што доводи до отежаног супротстављања разним екстремним лицима, групама и организацијама које су спремне да почине и најозбиљнија кривична дела. У Кривичном законику Републике Србије се нигде не наводи кривично дело за екстремистичко деловање. И у другим државама је мање – више слична ситуација (Ђорић, 2012). Можда је одличан пример за нормативно одређење ове области РФ, која је 2006. године усвојила закон, рус. *О противодействии*

[16] Екстремизам (лат. *extremus*) и може се превести као крајност, непопустљивост у одређеним идејама, ставовима и поступцима; тако да екстремизам кореспондира са идејом граница тј. ограничавања (Ђорић, 2012).
[17] Латински, *radix* – корен.

экстремистской деятельности, којим се мења одређење екстремизма, па се самим тим и јачају државна овлашћења институција које се баве супротстављањем недозвољеној делатности из ове области. Овом приликом је знатно проширена дефиниција екстремизма, тако да се осим верских, расних и националних злочина, екстремизмом сматрају и многе друге недозвољене делатности, па и оне које се чине из идеолошких, социјалних и политичких разлога, укључујући и хулиганизам, а одређено је и шта су то екстремистичке организације и екстремистички материјали. У овом Закону, *екстремистичка активност* (*екстремизам*) је одређена као „насилна промена у основама уставног система и (или) кршење територијалног интегритета РФ, укључујући отуђење дела територије РФ, са изузетком разграничења, редемаркације државне границе РФ са суседним државама; јавно оправдање тероризма и других терористичких активности; изазивање друштвене, расне, националне или верске мржње; пропаганда искључивости, супериорности или инфериорности особе на основу њене друштвене, расне, националне, верске или језичке припадности или односа према вери; повреда права, слобода и легитимних интереса човека и грађанина, у зависности од његове друштвене, расне, националне, верске или језичке припадности или односа према вери; спречавање грађана у остваривању својих изборних права и права на учешће на референдуму или нарушавање тајности гласања, у комбинацији са насиљем или претњом његовом употребом; ометање законитог рада државних органа, органа локалне самоуправе, изборних комисија, јавних и верских удружења или других организација, у комбинацији са насиљем или претњом његовом употребом; извршење кривичних дела из мотива наведених у ставу „е" првог дела члана 63. Кривичног закона РФ; употреба нацистичких параферналија или симбола, или прибора или симбола који су збуњујуће слични нацистичком прибору или симболима, или прибора или симбола екстремистичких организација, са изузетком случајева употребе нацистичких параферналија или симбола, или прибора или симбола сличних нацистичким прибором или симболима за степен конфузије, односно атрибута или симбола екстремистичких организација, у којима се формира негативан став према идеологији нацизма и екстремизма и нема знакова пропаганде или оправдања нацистичке и екстремистичке идеологије; јавне позиве за спровођење ових аката или масовну дистрибуцију очигледно екстремистичких материјала, као и њихову производњу или складиштење ради масовне дистрибуције; јавна свесно лажна оптужба лица на јавној функцији РФ или на јавној функцији конститутивног субјекта РФ да је извршила, током обављања службене дужности, дела наведена у овом члану и која су злочин; организовање и припремање ових аката, као и подстицање на њихово спровођење; финансирање ових аката или друга помоћ у њиховој организацији, припреми и спровођењу, укључујући обезбеђивање образовне, штампарске и материјално – техничке базе, телефонске и друге видове комуникације или пружање информативних услуга". У истом Закону, *екстремистичка организација* је одређена као „јавно или верско удружење или друга организација за коју је, на основу овог савезног закона, суд донео правоснажну одлуку о ликвидацији или забрани делатности у вези са спровођењем закона, екстремистичких активности." Исти Закон је одредио и *екстремистичке материјале* као „документа или информације намењене за дистрибуцију или јавно приказивање на другим медијима, који позивају на спровођење екстремистичких активности или поткрепљују или оправдавају потребу за тим активностима, укључујући и радове лидера Национал – социјалистичке радничке партије Немачке, Фашистичке партије Италије; говори, слике вођа група,

организација или покрета признатих као злочиначки у складу са пресудом Међународног војног суда за суђење и кажњавање главних ратних злочинаца земаља европске осовине (Нирнбершки трибунал); говоре, слике вођа организација које су сарађивале са овим групама, организацијама или покретима, публикације које поткрепљују или оправдавају националну и (или) расну супериорност или оправдавају праксу чињења војних или других злочина са циљем потпуног или делимичног уништења било које етничке припадности, друштвене, расне, националне или верске групе." (Федеральный закон „О противодействии экстремистской деятельности", 2006, 2014, 2020, 2021). Због свих напред наведених потешкоћа у одређењу, установљавању, па затим и супротстављању овој врсти недозвољених делатности, у надлежност служби безбедности је зато стављено да се бори против екстремизма и тероризма, али колико год да је одлично то што је екстремизам дефинисан у нормативима неке државе (у овом случају анализирамо случај РФ), исувише уопштено, изузетно широко, па и са изменама и допунама прилагођеним актуелним догађајима у држави, то исто тако може бити и извор злоупотребе уколико се овако уопштено, заузимањем ставова или уверења, појмовно одређење екстремизма почне тумачити ради одобравања посебних поступака и мера полицији и службама безбедности према било коме, као и проблема у другим државним институцијама које се баве овим поступцима, под оправдањем идеолошких, социјалних, политичких или других разлога чиме би евентуално могла бити битно угрожена права грађана.

Савезним Законом[18] у РФ, између осталог, предвиђено је спречавање екстремистичке делатности, тако да држава у оквиру своје надлежности предвиђа приоритетно спровођење мера и то превентивне, укључујући образовне, *пропагандне мере* у циљу спречавања екстремистичких активности. Законодавац овде није прописао о којим се конкретно све превентивним мерама ради (вероватно су тајног карактера), али можемо констатовати да је законом предвиђена *пропагандна мера* као посебна мера супротстављања екстремистичким активностима чије је супротстављање у већини држава углавном у надлежности служби безбедности.

У Стратегији националне безбедности Републике Србије предвиђено је „присуство фактора угрожавања безбедности невојним претњама, међу којима су сепаратистичке тежње, етнички, верски и политички екстремизам, економски и социјални проблеми, миграције, организовани криминал, недовољна изграђеност државних институција и елементарне непогоде" (Стратегија националне безбедности Републике Србије, 2019, стр. 17). У Стратегији одбране Републике Србије, екстремизам је одређен као „етнички и верски екстремизам и може се појавити са различитим интензитетом и последицама, са могућношћу испољавања од стране појединаца или организација са територије Републике Србије, као и територија других држава. Тај облик угрожавања безбедности, уз подршку истомишљеника са територија других земаља, истовремено је и генератор сепаратистичких тежњи" (Стратегија одбране Републике Србије, 2019, стр. 21). Навођење невојних претњи у највишим стратегијским документима по питању безбедности једне државе, па између осталих и етничког, верског и политичког екстремизма, говори о озбиљности ове врсте претње, али и аутоматски открива да неко са друге стране, у држави, мора да се

[18] Члан 5, *Федеральный Закон N 114*, О сузбијању екстремистичких активности.

супротставља овим и сличним претњама, што је поред других институција углавном у надлежности служби безбедности.

4.1.3.4. Организовани криминал и корупција

Криминал и нерегуларно ратовање су често повезани. Криминал је често уносно средство за финансирање операција, присиљавање и контролисање становништва и наношење штете владином ауторитету. Неки криминалци се могу противити побунама које угрожавају криминалне циљеве. Најмоћније криминалне организације могу да ангажују паравојне елементе или да се прошире са традиционалних криминалних активности на активности побуне ради својих интереса (Training and Doctrine Command G2 Handbook No. 1.08, 2010).

Да и службе безбедности нису имуне на корупцију, показује и хапшење службеника Федералне службе безбедности по разним оптужбама за корупцију. Почетком 2019. године, у Управи за борбу против корупције ухапшен је пуковник Федералне службе безбедности са неколико колега због примања мита, да би средином године још неколико припадника Федералне службе безбедности било ухапшено и оптужено за пљачку банке и изнуђивање новца од бизнисмена. Отприлике у том периоду, специјални помоћник специјалног изасланика председника за Урал и члан Савета безбедности ухапшен је због велеиздаје због комуникације са Пољском (Riehle, 2022). Следећи су примери припадника служби безбедности који нису били имуни на корупцију. У мају 2019. године пуковник Федералне службе безбедности Кирил Черкалин[19] је ухапшен са великом количином новца и драгоценостима (вредности преко 180 милиона долара) у свом стану. Исте године, убрзо након овог случаја ухапшена су још два официра службе безбедности РФ, Федералне службе безбедности, Дмитриј Фролов и Андреј Васиљев. Одељење К Федералне службе безбедности је наводно истраживало Сергеја Магнитског 2008. године и Алексеја Навањног[20] 2013. године. Черкалин је оптужен да је користио своју регулаторну моћ над банкама како би тражио мито и новац за заштиту коју би им он обезбедио. Такође, у октобру 2019. године, суд у Москви је осудио пуковника из одељења Министарства унутрашњих послова одговорног за регулисање банака на 12 година затвора, због мита и ометања правде; код себе је имао више од 125 милиона долара новца (Riehle, 2022). Ове карактеристичне случајеве смо навели као показатељ да се и у систему безбедности мора стално водити рачуна о корупцији, протежирати квалитетна и што искуснија *унутрашња контрола* запослених у службама безбедности, јер лица која се баве пословима контроле и утицаја на огромне новчане токове у економији чак и мањих, а поготово великих држава, сила, потребно је посебно и чешће

[19] Кирил Черкалин, био припадник Одељења К, Федералне службе безбедности, за коју се предпоставља да се ради о компоненти одговорној за економске контраобавештајне послове у банкарском сектору, а наводно је био и члан међуминистарског комитета за борбу против прања новца, финансирања тероризма и ширења оружја за масовно уништење (Riehle, 2022).

[20] Алексеј Навањни, антикорупцијски активиста ухапшен је 2013. године по оптужби за проневеру. Његов случај је одбачен (што је, анализирајући 6 година касније када је ухапшен због мита Черкапин, пуковник чије је одељење водило истрагу против Навањног, сасвим логичан след догађаја), али је поновљено суђење 2017. године, када је Навањни проглашен кривим. Западни медији су наведено преносили као пресуду којом му је фактички забрањено да се кандидује на председничким изборима 2018. године (Riehle, 2022). Наводно је Навањни добио псеудоним *Fridom* од службе безбедности у Великој Британији, Војног обавештајног одељка 6, са задатком спровођења операције потрес – *Quake* која је представљала промену уставног и политичког уређења у РФ (Факултет за дипломатију и безбедност, 2016).

контролисати и нормативно уредити ову област контроле припадника служби безбедности ангажованих на економским активностима. Наведено је специфично у том сегменту што је велики део тих активности тајне природе, па је врло тешко успоставити контролу токова новца који *званично не постоји* (Лабовић и Марјановић, 2021). Честа је појава да лица која се баве недозвољеним делатностима, а запослени су у служби безбедности, ангажовање унутрашње контроле усмеравају на сагледавање управо оних припадника који су патриоте, поштени, честити официри, па док се установи да је наведено била обмана, потребне су некада и године, док се у том периоду реализују недозвољене делатности од лица која врше обману.

Током 2022. године и у Републици Србији је ухапшено неколико припадника Безбедносно – информативне агенције и Министарства унутрашњих послова Републике Србије, овлашћених службених лица, где им се на терет стављају најозбиљнија кривична дела трговине наркотицима у великим количинама. Пре тога, један од озбиљнијих догађаја који је доспео у јавност, догодио се 26. новембра 2019. године када је ухапшен (поред осталих) део припадника служби безбедности Републике Србије који су се доводили у везу са узгојем и дистрибуцијом наркотика.

4.1.3.5. Други облици угрожавања безбедности државе

Службе безбедности (обавештајног и контраобавештајног карактера) представљају управо оне елементе политичког система државе преко којих власт, односно, да будемо прецизнији, владајућа елита, спроводи концепт тј. доктрину *државног интереса*. Државни интерес је термин који су први користили Макијавели и Ришеље, како би изразили претензије државе на право да када њој (елити) то одговара, игнорише законе које би она требала у суштини да штити, ако то захтевају такозвани виши интереси односно државни интереси. С обзиром да безбедност државе представља кључни државни интерес, лако се долази до констатације да су службе безбедности изнад закона, друштва, морала и универзалних вредности (Шаваев & Лекарев, 2003). Како законодавац никада не може да предвиди све облике угрожавања, тако у већини норматива остаје неодређен део облика угрожавања националне безбедности државе, па самим тим и послова и задатака које обављају службе безбедности. Најчешће се управо под тим окриљем и третира већина необавештајних активности служби безбедности ради реализације виших државних интереса.

Тако Драгишић у свом раду *Национална безбедност – алтернативе и песпективе* наводи да класичне безбедносне претње нису нестале када су настале нове неке претње, већ наведено захтева проширивање списка безбедносних ризика, претњи као и листе начина супротстављања истим (Драгишић, 2020). Ради се о живој проблематици – организму где се нови ризици и претње надовезују на претходне и константно мењају изискујући модификације мера, организација, поступака уз прилагођавање метода супротстављања.

4.2. НАЧИН И ДЕЛОКРУГ РАДА СЛУЖБИ БЕЗБЕДНОСТИ

Америчка тајна служба (енг. *U.S. Secret Service*) наводи да је „уз подршку стотина савезних, државних и локалних организација за спровођење закона и јавне безбедности, сваки од Посебних националних безбедносних догађаја, успешно завршен без већих инцидената" (Reese, 2021, p. 1). Овај цитат говори о комплексности рада служби безбедности као и колико се велики број организација, органа за потребе спровођења активности служби

безбедности на територији САД употребљава ради организовања и спровођења контраобавештајне и безбедносне заштите у оквиру реализације највиших државних активности. Овде је битан елемент употреба целина ван службе безбедности за реализацију послова и задатака из надлежности служби безбедности. Ради разумевања ове врло комплексне материје, ово чини битан сегмент у појашњењу места и улоге сваке, како офанзивне тако и дефанзивне службе безбедности, да неко ко се тек сусреће са овом проблематиком не помисли да су службе безбедности, односно њени припадници једини учесници, реализатори активности служби безбедности. Наиме, циљ политичког – државног врха једне државе кроз своје планове организују службе безбедности и у координацији, сарадњи и садејству са огромним бројем организација и других ентитета спроводе активности које су им додељене ради заштите националне безбедности.

Активности обавештајне заједнице регулисане су Уставом и бројним законима и подзаконским актима. Један од најбитнијих докумената у САД за обавештајне и контраобавештајне активности представља Извршно наређење 12333 (према овом наређењу, 12333, тачка 3.5, параграф /ф/) дефинисано је да енг. *intelligence* укључује и енг. *foreign intelligence* и енг. *counterintelligence* (Executive Order 12333, 2008). Наведено одређење много компликује сагледавање ове проблематике када се две различите и комплексне области, тотално супротне природе називају истим термином. Битно је нагласити да се последњим изменама ове наредбе у 2008. години постављају стратешки циљеви и мисије обавештајне заједнице, мисија се ограничава на прикупљање информација за валидне стране обавештајне сврхе. Овом наредбом се дефинишу и улоге и одговорност унутар међународне заједнице и потврђује посвећеност нације заштити грађанских слобода и права на приватност држављана САД током обављања активности од служби безбедности. Извршно наређење 12333 општим принципима успоставља равнотежу и њима регулише прикупљање обавештајно – безбедносних података. Прецизирано је да се активности обавештајне заједнице које се тичу америчких држављана могу спроводити само у складу са прописаним процедурама које је успоставио (одобрио) руководилац обавештајне заједнице, односно одобрио државни тужилац (за оне активности заједнице за које је неопходно одобрење тужиоца). Основна мисија обавештајне заједнице САД је да прикупља, анализира и доставља информације обавештајне и контраобавештајне природе државном и војном руководству како би правовремено могли да донесу исправне одлуке ради заштите државе. Потрошачи информација од обавештајне заједнице су председник, креатори државне политике, органи за спровођење закона и војска (The Intelligence Community, 2022). Као што смо констатовали недореченост у правним одређењима дефиниција о обавештајној заједници, тако можемо са пуним основом да констатујемо само на основу једног правног акта на који се обавештајна заједница позива као темељним, а то је Извршно наређење 12333, да уколико је само информација мисија обавештајне заједнице, шта је онда то што је прописано у тачки 1.2 параграф (б) тајне акције у истом том извршном наређењу и зашто наведено није обухваћено мисијом иако обухвата велики број мера, радњи и поступака обавештајне заједнице?

Информације као инструмент моћи, гледајући са аспекта доласка до њих преко служби безбедности, могу се схватити на више начина. Наведено укључује вредност извора информација, било физичких, когнитивних или виртуелних. Ове изворе можемо посматрати као људе и/или машине. Контрола над овим структурама се може користити за поседовање моћи. Институције које надгледају, осмишљавају и доприносе току информација, где у својој

понуди имају базе података, такође представљају моћне инструменте (Ducheine & Pijpers, 2021).

Када говоримо о обавештајној активности службе безбедности (војног карактера) тада говоримо о обавезама везаним за прикупљање, обраду и пружање војних, политичких, економских и научно – техничких информација у циљу постизања војне супериорности у региону (за велике силе) и обезбеђивања безбедности у војсци. У организационом смислу, обавештајна активност (војног карактера) обухвата аналитичко – информациони део, обавештајни део, спољне односе, теренску безбедност и војну цензуру са задатком добијања информација о оружаним снагама страних држава (првенствено угрожавајућих), њиховим могућим намерама, степену њихове борбене готовости (односно оперативне и функционалне оспособљености), новим системима наоружања, извођења специјалних операција ван државе, вођење војних научних развојних пројеката, спровођење војне цензуре, укључујући цензуру медија. Мање или више, свака контрола и надзор су у суштини формални, јер саме активности служби безбедности (већи део) су у суштини скуп тајних активности које се међусобно смењују и надовезују, употпуњују. Обавештајна активност у служби безбедности (цивилног карактера) у организационом смислу обухвата следеће: оперативно планирање и координацију, оперативни и технички део, начин прикупљања података, политичко деловање и односе са јавношћу, технички део, војно – научно истраживање, особље, финансије, логистику, безбедност, образовање и обуку (Шаваев & Лекарев, 2003).

Најбитнија начела организовања служби безбедности једне националне заједнице чине: начело координације, законитости, разграничења надлежности, тајност, интеграција резултата, одговарајући распоред снага, технологија рада. Тако државе организују обавештајне, контраобавештајне (безбедносне) и необавештајне – субверзивне и друге активности (Савић, Делић и Бајагић, 2002).

4.2.1. Обавештајна активност

Темељ за одређење обавештајних активности у САД је Закон из 1947. године, праћен реформом обавештајних активности Законом о спречавању тероризма из 2004. године и Законом о овлашћењу за фискалну 1993. годину, којим је Закон из 1947. године измењен, при чему је дефинисано следеће: служба безбедности обухвата обавештајне службе и контраобавештајне службе; страна обавештајна служба (активност) обухвата информације које се односе на способности, намере или активности страних влада или њихове елементе, стране организације или страна лица, а термин контраобавештајна служба (активност) се бави прикупљањем информација и организује и спроводи активности ради заштите од шпијунаже, других обавештајних активности, саботажа или атентата које су извршили или у име страних влада или њихових елемената, стране организације, односно страна лица (Wheaton & Beerbower, 2006). Читава обавештајна заједница се бави доласком до податка, али податак сам по себи не представља крајњу информацију (Wheaton & Beerbower, 2006). Ова одређења (чак и према најстаријим нормативима у САД) контраобавештајне службе (активности) изостављају сегмент припреме за реализацију ових дела, а сама припрема за извршење ових дела представља кривично дело и носи са собом кривичну одговорност за извршиоце, а уз то представља и сегмент који је у надлежности служби безбедности који никако не би смео бити изостављен из овог теоријског одређења. Неопходно је да увек буде присутан проблем разумевања превода страног језика и правог значења речи, где сам превод

са енглеског језика *intelligence*, који се користи вишезначно у терминологији у САД од значења организације (службе безбедности као организације), врсте организације (оне која се бави обавештајним или контраобавештајним пословима), активности (обавештајне активности или контраобавештајне активности), нуди много значења која се често мешају у теорији када вероватно пише неко ко није стручан или има намеру да то пласира на такав начин да буде свима доступно.

Из тајности са новим одређењем обавештајне активности, обавештајна заједница у САД изашла је крајем 2002. године на својој интернет страници обавештајне заједнице. Овде је појмовно одређено (на интернет страници *www.intelligence.gov*) да обавештајна активност представља: „Тело доказа и закључака изведених из њих који се прибављају и достављају као одговор на познате или уочене захтеве потрошача. Често произилазе из информација које су сакривене или нису намењене да буду доступне на коришћење стицаоцу" (Wheaton & Beerbower, 2006, p. 324).

Обавештајна активност (у ширем смислу) је појам који обухвата укупну делатност, све активности коју предузимају обавештајне институције у једној држави (Мијалковић, 2011). У ужем смислу, појам обавештајне активности службе безбедности представља долажење до тајних података који су битни за националну безбедност и заштиту, односно за спровођење стратешких интереса државе (Мијалковић, 2011).

4.2.1.1. Корени обавештајне активности

Корене обавештајних активности (или, како је у првом документу пре формирања САД било одређено, обавештајних делатности) као вида државних активности у САД (говоримо о периоду од краја XVIII века до 1947. године) препознајемо још током Америчког револуционарног[21] рата тј. Америчког рата за независност (1775 – 1783) где су исте обављали обавештајни органи као што је *Тајни комитет* у рату САД за независност од Енглеске, што се одликује посебношћу задатака које су реализовали ови обавештајни органи, да кажемо прве службе безбедности (обавештајног карактера) које су претече служби безбедности које ће бити формиране касније у САД. Само два месеца након што је Континентални конгрес формирао *Тајни комитет*, формиран је још један комитет који се бавио обавештајним активностима са првим именом, називом *Комитет за дописивање* који је врло брзо преименован у *Комитет за тајну преписку – кореспонденцију* (енг. *Committee of Secret Correspondence*). Надлежности *Комитета за тајну преписку* укључивали су

[21] Први пут је разматрање потреба за стварањем независних структура служби безбедности (како контраобавештајног, тако и обавештајног карактера) постављено на Другом континенталном конгресу 1775. године. Џорџ Вашингтон је, као главнокомандујући Команде оружаних снага уједињених колонија, инсистирао да се резолуцијом Конгреса, 18. септембра 1775. године формира *Тајни комитет* (енг. *Secret Committee*) који је између осталих имао и низ задатака како контраобавештајне природе тако и обавештајне. Једна од важних функција комитета била је да организује заштиту трговачких бродова Конфедерације од напада енглеске морнарице. Тајни комитет је морао да своје обавезе реализује у тајности, а радило се првенствено о неопходним набавкама и накнадним расподелама купљене војне муниције, наоружања, барута и других потрепштина где видимо претече тајних активности и државних структура које те обавезе треба да спроведу у дело. Тајни комитет је већ имао људску компоненту за прикупљање података (агенте) са задацима идентификовања локација тајних војних складишта Британаца и потом организовања операција да их ухвате или униште – овде већ идентификујемо део субверзивних активности односно међу првим регистрованим необавештајним активностима служби безбедности, претечама служби безбедности САД (Юрьевич, 2014; In: Journals of the Continental Congress 1774–1789/Volume II/, September 18, 1775. /pp. 253–254./ Washington: Government Printing Office, 1905.).

прикупљање обавештајних података у Енглеској, Ирској и другим европским земљама (у неким случајевима, заједно са *Тајним комитетом*). За реализацију ових задатака обавештајних активности, Комитету је наложено да активно користи агенте[22] из редова становника наведених држава. *Комитет за тајну преписку* (*кореспонденцију*) је две године након оснивања, 17. априла 1777. године променио назив у *Комитет за спољне послове*. Међутим, када говоримо о надлежностима овог новог комитета, оне су остале практично непромењене; наставио је да се бави обавештајним активностима, а сегмент међународне сарадње је највише разматран у другим комитетима Континенталног конгреса, а не у овом. По стварању Министарства иностраних послова (енг. *Department of Foreign Affairs*), 10. јануара 1781. године, претходнице садашњег Стејт департмента САД, већина надлежности *Комитета за тајну преписку* (*кореспонденцију*) пренета је на новостворену институцију. Интересантно је да је Начелнику Одељења за међународне послове наложено да обавезно одржава контакте са свим оним лицима од којих би, на основу његове процене, могао да добије корисне податке тј. информације (Юрьевич, 2014). Генерал Вашингтон, будући први председник САД, већ је на самом почетку ослободилачког рата схватио колико је велика корист коју у рату добија онај који активно користи обавештајне активности. Већ на самом почетку рата за независност формиран је читав обавештајни систем у војсци Конфедерације. Директно на челу овог система био је и сам генерал Вашингтон, који је у неким случајевима чак одржавао и личне састанке са агентима тј. доушницима, како су их у том периоду називали. Убрзо након завршетка рата за независност ове службе безбедности су укинуте, а разлог је разумљиве природе за тај временски период – зато што је обавештајна активност сматрана војном, ратном делатношћу и сходно томе су распуштене и обавештајна и контраобавештајна служба (Юрьевич, 2014).

Даљи развој обавештајних активности у САД везан је тек за крај XIX века јер САД нису имале активне службе безбедности, већ су се тим пословима бавили неспецијализовани органи, намењени углавном извиђачким мисијама. Да нагласимо да обавештајна активност у овом периоду није сматрана за самосталну врсту државне активности, већ да се радило само о једној од врста војних активности. Специјализовани органи, службе безбедности, створене су само за период активних војних чета (током Америчког грађанског рата, 1861–1865). Када су сви сукоби окончани, дошло је и до гашења службе безбедности (обавештајног карактера). Настанком фундаменталних промена у САД, председник Френклин Д. Рузвелт детаљно испитује трансформацију уочи Другог светског рата разнородних обавештајних служби и одељења у јединствени обавештајни систем који је у стању да централно решава националне проблеме. Развој обавештајних активности САД, да кажемо самосталне активности у оквиру државног апарата, настаје у периоду од 1947. године. Говоримо о овој години из разлога што је тада усвојен Закон о националној безбедности САД где је новоосновани Савет Националне

[22] Први агент *Комитета за тајну преписку* (*кореспонденцију*) био је Артур Ли, лекар који се преселио у Лондон, који је добио новчану награду од 200 фунти из првих средстава које је Континентални конгрес доделио за потребе комитета већ у децембру 1775. године (овде препознајемо један од мотива, начина вербовања, одржавања и даљег рада са изворима података служби безбедности, новчана – материјална заинтересованост). У 1776. години као тајни представник северноамеричких колонија, Ли се у Лондону састао са француским обавештајцем и будућим аутором књижевног бестселера *Фигарова женидба* Пјером Огистеном Карон де Бомаршеом. Артур Ли је успео да убеди писца у потребу француске помоћи побуњеним колонијама у Новој Енглеској (Юрьевич, 2014).

безбедности САД главни орган управљања националне безбедности и служби безбедности. Такође, овај процес обухвата и постепено успостављање обавештајне заједнице као јединствене организационе целине која обједињује све водеће службе безбедности САД. Постепено су проширивана овлашћења директора Централне обавештајне агенције у односу на припаднике других служби безбедности из обавештајне заједнице и проширење техника и метода вођења служби безбедности. Обавештајне активности САД показују колико је велики био утицај на активности служби безбедности до којих је довео развој у сфери научно – технолошког напретка, што је опет довело до појаве нових праваца обавештајне активности као што су обавештајне активности у свемиру или извиђање на каналима комуникације и каналима преноса информација (Юрьевич, 2014). У штампи, на основу материјала Едварда Сноудена (*Edward Snowden*), појавио се још један глобални обавештајни програм службе безбедности у САД, Агенције за националну безбедност: рачунарски програм под називом Призма – енг. *Prism,* који се наводно спроводи од 2007. године (наводно на основу Закона о одбрани САД). Овај програм наводно подразумева имплементацију службе безбедности, Агенције националне безбедности, на глобалном нивоу за масовно прикупљање информација о корисницима друштвених мрежа, интернет сервиса, власницима паметних телефона, корисницима услуга претраживања. Ради се о компанијама: *Microsoft, Apple, Google, Facebook, Yahoo!, Paltalk, YouTube, AOL, Skype,* које активно сарађују са Агенцијом националне безбедности и пружају обавештајне податке службама безбедности САД (Юрьевич, 2014). Закон о надзору страних обавештајних служби (енг. *Foreign Intelligence Surveillance Act*) из 1978. године обезбеђује службама безбедности САД обављање обавештајних активности кроз примену овлашћења за прикупљање података о страним обавештајним службама путем електронског надзора, физичке претраге, формирања регистара и хватања и праћења уређајима (који снимају или декодирају бирање, рутирање, адресирање или сигнализирање информација), или производњу одређене пословне евиденције. Службе безбедности обично траже одобрење за такве активности од стране специјализованог суда (енг. *Foreign Intelligence Surveillance Court*), који је створен поменутим Законом, ради постојања неутралног учесника (Foreign Intelligence Surveillance Act, 1978). Закон из 2007. године је овластио обавештајне службе САД да примају (купују) обавештајне податке од комуникационих компанија, интернет провајдера, мобилних оператера, као и од техничког особља и других запослених у тим компанијама (Юрьевич, 2014).

Велике силе, као што су Немачка у периоду од 1933. до 1945. године и Савез Совјетских Социјалистичких Република у периоду од 1920. до 1980. године, важиле су за државе са најмоћнијим и најефикаснијим тајним службама (службама безбедности) када говоримо о XX веку, док када помињемо модерне империје данас, у XXI веку, првенствено мислимо на САД која одговара најмоћнијем систему на свету (по финансијским могућностима, техничкој опремљености и интелектуалном потенцијалу). Брзо растућа је и империја коју представља Кина, која има импресивну историју (обавештајних и контраобавештајних активности). Када говоримо о тајним службама, тада за делатности које оне обављају најчешће кажемо да су тајне активности држава које су увек постојале једна против друге. Враћајући се још даље у прошлост, римски и кинески цареви, египатски фараони, грчки и византијски заповедници, као и други владари у антици, као и наследници њихове суверене власти у наредним историјским епохама, никада нису прекидали да

комбинују војне и политичке активности спречавања деловања, одвраћања и побеђивања спољашњег и унутрашњег непријатеља уз коришћење снага, средстава и метода служби безбедности (обавештајног и контраобавештајног карактера). Службе безбедности тек у XX веку добијају јасно дефинисане структурне и организационе елементе и заузимају битно место у политичком систему државе. Прекид или „ресет" служби безбедности су по два пута доживеле у XX веку Немачка (1918. и 1945. године) и Русија (1917. и 1991. године), када су заједно са државама у потпуности уништене и њихове службе. У XX веку настале службе безбедности у САД развијале су се динамично и без опипљивих шокова, као и службе безбедности Велике Британије. Француска је 1970. и 1990. године стекла заслужени престиж у области економске обавештајне и контраобавештајне активности. Када је реч о Јапану и Кини, ове државе традиционално користе националне карактеристике како би наставиле и развиле доктрину тоталне шпијунаже и контрашпијунаже, а притом су остале најзатвореније службе безбедности на свету (Шаваев & Лекарев, 2003). Руске тајне службе комунистичког доба су званично сматране штитом и мачем партије. Нови политички лидер на Истоку поставља свог руководиоца службе безбедности, док је наводно на Западу систем промене руководства служби безбедности у САД исти такав – новоизабрани председник доводи и поставља новог шефа Централне обавештајне агенције (тежишно обавештајне службе) и Федерални истражни биро [23] (тежишно контраобавештајне службе). Постоје и овде изузеци, а коментари су били да је тајна дуговечности шефова одређених служби безбедности углавном у „озлоглашеним ормарићима" са дуготрајним и смртоносним компромитујућим материјалима о водећим политичарима, бизнисменима и њиховој пратњи, посебно при решавању кадровских проблема. Службе безбедности не би требале бити лидери у политици, већ само следбеници, с тим да се води рачуна да агенти од утицаја страних служби безбедности на челу политичких структура не превазиђу утицај домаће службе безбедности. Није страно да и сами челници служби безбедности постану председници држава, нпр. Централне обавештајне агенције у САД – Џорџ Х. В. Буш; Федералне службе безбедности у РФ – Владимир Путин (Шаваев & Лекарев, 2003).

4.2.1.2. Појмовно одређење обавештајне активности

Један термин, енг. *intelligence*, на Западу има више појмовних одређења и значења. Закон о националној безбедности у САД је врло јасно дефинисао у (енг. *Sec. 3, p. 5*) ове појмове и изразу *intelligence* доделио значење стране обавештајне службе и контраобавештајне службе. Док је енг. *foreign intelligence* најприближнија нашем термину *обавештајна активност* и значи активност у прикупљању информација које се односе на способности, намере или активности страних влада или њихових елемената, страних организација или страних лица или међународних терористичких активности (National security act of 1947, 2021).

[23] Наведени поступци, постављања директора, руководилаца на чело служби безбедности контраобавештајног карактера представља велики проблем, јер наведена лица могу (или морају?) бити политички острашћена и да своје личне (приватне) ставове преносе на задатке у оквиру својих служби безбедности где су постављени на дужност где уз низ, сада потчињених лица запослених у службама безбедности, који морално и квалитетом не заслужују нити да буду припадници служби безбедности реализују одређене незаконите активности. У 2022. години већина медија како у САД тако и изван државе, поступке предузимања репресивних мера припадника служби безбедности САД, Федералног истражног бироа, према сарадницима бившег председника САД, Доналда Трампа и њему лично је окарактерисала као злоупотребу службе безбедности.

Обавештајна активност је у претходном периоду разматрана на великом броју „округлих столова" теоретичара у покушајима научног објашњења овог појма. Резултат је изузетно слаб, што се може делимично правдати тајношћу која прати ову активност. Наведено има смисла ради природе посла коју представља, али врло често иза предузимања мера да неке активности остану тајне природе, долази и до великих могућности за злоупотребе, махинације и друге недозвољене активности. Већина теоретичара на западу који се баве феноменима посвећеним обавештајној активности, раду, активностима, као и обавештајним службама, користе термин на енглеском језику, *intelligence*. Једни теоретичари обавештајну активност тумаче као средство креирања спољне политике, део њих примат даје улози безбедности, неки одбрани земље, док је сагледавање као облика државног органа, организације и механизма за утицај на друге најзаступљеније.

У Извршном наређењу 12333 (енг. *Executive Order 12333*), тачка 3.5, параграф (е) обавештајне активности су дефинисане као „долазак до информација које се односе на способности, намере или активности страних влада или њихових елемената, страних организација, страних лица или међународних терориста" (Executive Order 12333, 2008, p. 15). Службе безбедности реализују обавештајне активности, контраобавештајне активности и необавештајне активности (тајне акције – тачка 3.5, параграф /б/) односно све активности којим су овлашћене службе овим наређењем (Executive Order 12333, 2008).

Процене састављене од обавештајних података служби се обично заснивају како на „тајним" тако и на „јавним – отвореним" изворима података. Јавне изворе често преузимају из материјала који су други сакупили и обрадили (владине целине, медији, невладине агенције…). Све ове активности нећемо дефинисати као обавештајну активност, што указује да се обавештајна активност базира највише на анализи или процени. Да ли би теоретичари требало да прихвате овај ниво непрецизности као коначан? Треба ли и даље настојати да дођемо до дефиниције обавештајне активности која решава ову непрецизност? Затим, даља размишљања о обавештајној активности доводе до следећег питања тј. констатације, о тајном деловању, интервенцијама, необавештајним активностима, у другом или свом друштву (у САД је тек 2008. године ревизијом Извршног наређења 12333 изопштена могућност деловања у земљи, а 2009. године у Извршном наређењу 13491 који се проширио на све запослене у америчкој влади, укључујући оне из Централне обавештајне агенције ограничена је техника испитивања људи, пронађена у Војном теренском приручнику у Операцијама сакупљача обавештајних података, прим. аут.). Теоретичари су игнорисали необавештајне активности у разматрању обавештајне активности, па су одвајали од међународних односа необавештајне активности од „традиционалних" спољнополитичких инструмената (Scott & Jackson, 2004). Један мали део обавештајне активности је „шпијунажа" (дело одређено у нормативима великог броја земаља као кривично дело) и она у најужем смислу подразумева долазак у посед података који су тајне природе и то уз употребу, ангажовање „шпијуна", док врло често обичан човек обавештајну активност препознаје и одређује само као „шпијунажу". О необавештајним активностима служби безбедности ће детаљно бити речи у наредном делу истраживања.

Део теоретичара на западу, попут Варнера (*Michael Warner*), наглашава „информативни" аспект обавештајне активности више од свог „организационог" аспекта, што је ироничан преокрет. Једначина да је обавештајна активност једнака информацији је превише нејасна. Обавештајна активност је неколико ствари: то су информације, процес и

активност, а изводе га државне, законите власти, па оне представљају државне активности. Тајност је битна, јер је обавештајна активност део текуће борбе између нација, ентитета. Обавештајна активност укључује тајне операције. Варнер на крају закључује да је обавештајна активност тајна, државна активност о разумевању или утицају на стране субјекте, ентитете (Warner, 2002). Обавештајна активност укључује и тајне операције које се изводе и изазивају одређене ефекте у туђини, иностранству, другим државама или ентитетима, па и према лицима када они представљају виши државни интерес (Warner, 2002). Џонсон (*Loch K. Johnson*) обавештајну активност сагледава кроз производ, процес, мисију или кроз организацију. Гил (*Peter Gill*) дефинише обавештајну активност према њеној сврси и сходно томе види ту активност као предузимање прикривених акција, истрага, а посебно препорука вођама политике или државе ради сузбијања претњи. Гил закључује да је обавештајна активност кровни појам који обухвата тајност, информације, обавештајни циклус, контраобавештајни рад, стратешке претње и прикривене акције (Gill, 2010).

Обавештајна активност може се посматрати као активност усмерена на активности по питањима безбедности (односи се на унутрашњу безбедност) и активности по питањима страног фактора (односи се на спољну безбедност). Обавештајна активност о безбедности се односи на активности релевантне за унутрашњу безбедност и заштиту државе и друштва од страног деловања (нпр. субверзија, шпијунажа, политички мотивисано насиље и други облици), а како би се наведеним активностима у сарадњи са надлежним државним органима омогућило одржавање мирне, контролисане јавне безбедности и обезбедила унутрашњу безбедност. Долазак до података везаних за активности страних обавештајних активности обухвата активности служби безбедности у сврху упозорења државног руководства о могућем угрожавању државе споља. Податке о намерама, могућностима и активностима других држава, фирми, организација, недржавних група и њихових агената који представљају могуће или реалне ризике или претње држави и државним интересима у иностранству, прикупљају спољне службе безбедности и оне најчешће узимају учешће у супротстављању необавештајним активностима страних служби безбедности и реализацији необавештајних активности за потребе своје службе безбедности – државе. Може се констатовати да су функције и циљеви прикупљања података, као и активности које обављају службе безбедности везане за стране обавештајне и безбедносне активности, различити. Важан је систем контроле и одговорности у току обављања ових активности од стране припадника служби. Констатација специјалиста из ове области током ангажовања радне групе 2003. године (у организацији *Geneva Centre For The Democratic Control Of Armed Forces*) је да због природе моћи унутрашњих служби безбедности, као и примене мера потенцијално против властитих грађана, ова активност служби захтева строге контроле како би се осигурало да унутрашња безбедност буде у сразмери са правима која следују грађанима и становницима (Geneva Centre For The Democratic Control Of Armed Forces, 2003). Контрола наметљиве моћи због поштовања права грађана у држави (својој држави), а према другима, поготово у иностранству, „нема правила", односно није ништа ни констатовано. За сва одређења обавештајне активности заједничко је да све садрже тајност као обавезан део појма. Због тога се слободно може рећи да сазнања која настају обавештајном активношћу представљају велики део историје која ће остати једна непознаница, што обичан свет никада неће сазнати.

Витон и Бирбоуер (*Wheaton and Beerbower*) у свом истраживању о одређењу обавештајне – контраобавештајне активности, закључују да има смисла одвојити активности *информисања политике* (сазнања, разумевање, анализирање и синтезу информација о страном ентитету) и активности које представљају *акт политике* (углавном спроводе државни службеници, покушај утицаја на стране субјекте). Обавештајне – контраобавештајне активности, дакле, представљају процес, фокусиран екстерно (споља) који користи информације из свих доступних извора, а који је дизајниран да смањи ниво неизвесности за доносиоца одлука (Wheaton & Beerbower, 2006).

Мајкл Варнер (*Michael Warner*) је био припадник Централне обавештајне агенције када је дао једну од најсажетијих, а можемо слободно рећи најсвеобухватнијих или најприхватљивијих дефиниција која се односи само на обавештајну активност (логично, јер се Централна обавештајна агенција где је Варнер радио тежишно бави обавештајним, не тежишно контраобавештајним активностима): да обавештајна активност мора бити више од пуке информације и да она представља „тајну, државну делатност за разумевање или утицај на стране субјекте, ентитете" (Warner, 2002, p. 21). Даље Варнер износи да енг. *Intelligence* представља неколико ствари и то: „информацију, процес и активност, а да га врше законите власти" (Warner, 2002, p. 18). Ради приближавања ове Варнерове дефиниције важно је нагласити да одређењем ко врши обавештајне и контраобавештајне активности („законите власти") Варнер тада мисли на организацију, односно на службе безбедности, што представља четврто значење овог термина.

У Републици Србији, велики број теоретичара је терминолошки јасно дефинисао разлику између обавештајне активности и служби безбедности као организације која предузима наведену активност, те је горе поменутих неразумевања много мање. Уопштено, службе безбедности имају три основне функције: прикупљање, анализу и, кључну за читаву обавештајну активност, контраобавештајну активност. Необавештајна активност обавештајних служби је све чешће четврта функција која је тренутно најспорнија у демократском модерном друштву, али врло брзо се може очекивати да и она постане општеприхваћена, попут „шпијунаже" и других активности које су уз адекватне медијске припреме и друге врсте пропаганди постале „свакодневница" иако су законом забрањене, па чак спадају и у кривично дело које не застарева.

4.2.1.3. Значај обавештајне активности за државу

Да би сагледали значај обавештајне активности за једну државу, неопходно је прво сагледати који су то субјекти, односно ентитети који предузимају обавештајне активности за потребе државе. Када кажемо државе, тада не мислимо само на руководство те државе, већ и на све институције, органе, компаније и друге кориснике услуга служби безбедности. Истраживањем литературе која сагледава ову област у САД, установили смо да је терминологија коришћена у давању имена организацијама у Обавештајној заједници (енг. *Intelligence community*) САД веома разнолика, терминолошки неусаглашена на савезном нивоу (у самим нормативима, као и оно што се презентује у теорији, па и научним радовима), што доводи до тога да велики број лица, чак и на високим руководећим дужностима у министарствима САД, вероватно несвесно употребљава појмове тј. називе целина у Обавештајној заједници који нису компатибилни са оним што желе да кажу (често помињући агенције, чак и када се не ради о агенцијама, прим. аут.). Увидом у нормативе, јавно

доступне за истраживање, који регулишу ову област у САД, дошли смо до следећих показатеља.

Сходно Извршном наређењу (енг. *Executive Order*) 12333 и три допуне тј. амандмана које је претрпело ово наређење, 13284 (2003), 13355 (2004) и 13470 (2008), Обавештајну заједницу САД чине следећи *елементи* (укупно 17):
Централна обавештајна агенција – енг. *The Central Intelligence Agency;* Обавештајна агенција одбране – енг. *The Defense Intelligence Agency;* Агенција националне безбедности – енг. *The National Security Agency;* Национални извиђачки уред – енг. *The National Reconnaissance Office;* Национална геопросторна – обавештајна агенција – енг. *The National Geospatial – Intelligence Agency;* Обавештајни и контраобавештајни елементи војске, морнарице, ваздухопловства и маринаца – енг. *The Intelligence and Counterintelligence Elements of the Army, Navy, Air Force, and Marine Corps;* Обавештајни елементи Федералног истражног бироа – енг. *Intelligence Elements of the Federal Bureau of Investigation;* Обавештајни и контраобавештајни елементи обалске страже – енг. *The Intelligence and Counterintelligence Elements of the Coast Guard;* Биро за обавештајне послове и истраживање, Државног секретаријата – енг. *The Bureau of Intelligence and Research, Department of State;* Канцеларија за обавештајне послове и анализе, Одељење за трезор – енг. *The Office of Intelligence and Analysis, Department of the Treasury;* Канцеларија Националне безбедносне службе, Управа за борбу против дроге – енг. *The Office of National Security Intelligence, Drug Enforcement Administration;* Канцеларија за обавештајне послове и анализе, Одељење за унутрашњу безбедност – енг. *The Office of Intelligence and Analysis, Department of Homeland Security;* Канцеларија за обавештајне и контраобавештајне послове, Одељење за енергетику – енг. *The Office of Intelligence and Counterintelligence, Department of Energy;* Канцеларија директора Националне обавештајне заједнице – енг. *The Office of the Director of National Intelligence.* Овде можемо да закључимо да су ентитети који се појављују као субјекти у Обавештајној заједници САД Извршним наређењем одређени као *елементи* Обавештајне заједнице, а не као *агенције* (што већи део теоретичара и званичника од Владе САД, па широм планете наводи, што појмовно није тако дефинисано). Део елемената чине и агенције, али поред агенција ту су и канцеларије, одељења, уреди, управе, бирои, сервиси, службе и слични елементи заједнице.

Поред горе наведених елемената Обавештајне заједнице САД, према Извршном наређењу, она обухвата и следеће *департмане* у Обавештајној заједници САД:
Одељење за правосуђе, Управа за борбу против дрога Канцеларија обавештајне службе националне безбедности – енг. *Department of Justice, Drug Enforcement Administration Office of National Security Intelligence*; Одељење за енергетику, Канцеларија за обавештајне и контраобавештајне послове – енг. *Department of Energy, Office of Intelligence and Counterintelligence*; Одељење за унутрашњу безбедност, Канцеларија за обавештајне послове и анализу – енг. *Department of Homeland Security, Office of Intelligence & Analysis*; Стејт департмент, Биро за обавештајне послове и истраживање – енг. *Department of State, Bureau of Intelligence and Research*; Одељење за трезор, Служба за обавештајне послове и анализе – енг. *Department of the Treasury, Office of Intelligence and Analysis* (Executive Order 12333, 2008).

Наведени елементи Обавештајне заједнице у САД (енг *Intelligence community*) дају јединствени сет способности како би се носили са обавештајним претњама са којим се суочава Влада САД. Следеће су активности у којима се ангажују елементи Обавештајне

заједнице: *Независна компонента* – Централна обавештајна агенција (енг. *Central Intelligence Agency*) прикупља обавештајне податке, углавном радом са људима и обезбеђује анализу из свих извора у вези са питањима угрожавања националне безбедности за потребе руководства државе (политике), одбране, службеника за спровођење закона и војне службе. У иностранству, Централна обавештајна агенција спроводи и контраобавештајне активности и предузима посебне активности по налогу Председника државе (тајне акције и др. задатке). *Компоненте Министарства одбране* – Одбрамбена обавештајна агенција (енг. *Defense Intelligence Agency*) обезбеђује свеобухватне спољно – војне обавештајне податке за војне службе, руководство државе (политике) и одбране. Агенција за националну безбедност (енг. *National Security Agency*) прикупља и обрађује стране обавештајне информације, све у облику сигнала за чланове политичких и војних заједница и штити критичне америчке информационе системе од злоупотреба. Национална геопросторно – обавештајна агенција (енг. *National Geospatial – Intelligence Agency*) обезбеђује геопросторне обавештајне службе за подршку националне безбедности и Одељења одбрамбених мисија. Национална извиђачка канцеларија (енг. *National Reconnaissance Office*) пројектује, производи, управља и одржава националне извиђачке сателите. Обавештајне организације војске, морнарице, ваздухопловства и маринаца (енг. *Army, Navy, Air Force, and Marine Corps intelligence organizations*) прикупљају, обрађују и дистрибуирају обавештајне податке релевантне за њихове потребе, а сходно њиховој намени. *Неодбрамбене компоненте одељења* – Државно одељење/Биро за обавештајне и истраживачке послове (енг. *Department of State/Bureau of Intelligence and Research*) пружа анализу глобалног развоја државних структура (одељења, министарстава) и доноси своје јединствене процене за националну обавештајну заједницу. Министарство правде/Федерални истражни биро (енг. *Department of Justice/Federal Bureau of Investigation*) је надлежан за обавештајна питања везана за контрашпијунажу, тероризам и контраобавештајне активности у САД, претње домаћој безбедности, и подацима о међународним кривичним предметима. Одељење за унутрашњу безбедност/Канцеларија за обавештајне послове и анализе (енг. *The Office of Intelligence and Analysis, Department of Homeland Security*) надгледа, процењује и координира назнаке и упозорења о претњама држави, обједињава и интегрише информације везане за тероризам и процењује и реагује на регистровање рањивости критичне инфраструктуре државе, нације. Одељење за унутрашњу безбедност/Обавештајни подаци обалске страже (енг. *U.S. Coast Guard Intelligence*) процењује обавештајне податке и пружа информације надлежнима у вези са претњама економским и безбедносним интересима САД у било ком поморском региону, укључујући међународне воде и америчке обале, луке и унутрашње пловне путеве. Одељење за енергетику (енг. *Department of Energy*)/Канцеларија за обавештајне и контраобавештајне послове (енг. *The Office of Intelligence and Counterintelligence, Department of Energy*) обавља анализе страног нуклеарног оружја, нуклеарне непролиферације и обавештајних питања везаних за енергетску безбедност, као подршка политикама, програмима и циљевима националне безбедности САД. Одељење за трезор (енг. *Department of Treasury*)/Канцеларија за обавештајне послове и анализу (енг. *The Office of Intelligence and Analysis, Department of the Treasury*) прикупља и обрађује информације које се односе на америчку фискалну и монетарну политику и претње финансијским средствима и институцијама САД. Канцеларија Националне безбедносне службе, Управа за борбу против дроге (енг. *The Office of National Security Intelligence, Drug Enforcement Administration*) сагледава претње заједници које

испољава утицај дроге, прикупљајући (отворено или преко јавно доступних извора) и анализирајући како обавештајне, тако и контраобавештајне податке за подршку Обавештајној заједници. Комплетни послови тј. одговорности Централне обавештајне агенције, Одбрамбена обавештајна агенција, Агенција за националну безбедност, Национална извиђачка канцеларија и Национална геопросторно – обавештајна агенција, везане су за обавештајне активности, па се стога свака од ових организација у целини сматра чланицом Обавештајне заједнице. Остале организационе целине, попут одељења и горе наведених војних целина, баве се првенствено пословима и мисијама које нису обавештајне те су из наведеног разлога само делови њихових организационих целина ангажовани на пословима искључиво обавештајне природе, па се зато сматрају само делом обавештајне заједнице. На пример, у случају америчке морнарице, само се Канцеларија поморске обавештајне службе (енг. *Office of Naval Intelligence*) сматра за члана обавештајне заједнице. Поред горе наведених елемената Обавештајне заједнице, такође је успостављен и низ националних центара као што су Центар за борбу против тероризма (енг. *Counterterrorist Center*), Контролни обавештајни центар о оружју, непролиферацији и контроли оружја (енг. *Weapons Intelligence, Nonproliferation, and Arms Control Center*) и Центар за криминал и наркотике (енг. *Crime and Narcotics Center*). Национални центар основан статутом – Национални центар за борбу против тероризма (енг. *National Counterterrorism Center*) је основан Законом о реформи обавештајне службе и превенцији тероризма из 2004. године. У тим центрима ради особље из организација широм обавештајне заједнице и одговорни су за развијање адекватних приступа прикупљању и анализи обавештајних података о конкретним питањима (Weapons of Mass Destruction, 2005). Амандманом из 2008. године, који је резултат уочених пропуста од стране комисије у раду служби безбедности у САД, након терористичких напада реализованих 11. септембра 2001. године у САД, Извршно наређење 13470 (2008) је допуњено и циљ је била интеграција Обавештајне заједнице у САД под руководством директора Националне обавештајне заједнице. Наиме, овим би се решио проблем координације између служби безбедности, увођењем новог, независног елемента у Обавештајну заједницу, Канцеларије директора Националне обавештајне заједнице – енг. *The Office of the Director of National Intelligence*. Канцеларија је добила обавезе да надгледа активности служби безбедности, док директор руководи радом служби безбедности. Без обзира на место (институцију, цивилну, војну и сл.) где се налазе имплементирани делови елемената Обавештајне заједнице, поред обавеза према тој институцији, ти елементи Обавештајне заједнице имају обавезе према директору Националне обавештајне заједнице.

Вештачка интелигенција у одбрани проналази примену у бројним пројектима, (обавештајни, надзорни и извиђачки), као и у логистици, затим операцијама у сајбер простору, информационим операцијама, команди и контроли, полуаутономним и аутономним возилима и смртоносним аутономним системима наоружања. Према извештајима САД, РФ у свом развојном програму активно спроводи пројекте из војне примене вештачке интелигенције. Руска Федерација оснива низ организација посвећених развоју војне вештачке интелигенције. Умножавање истраживачких институција посвећених вештачкој интелигенцији може, међутим, довести до преклапања одговорности и бирократске инерције. Руска Федерација за потребе оружаних снага истражује велики број пројеката примене вештачке интелигенције, али тежишно се бави развојем полуаутономних и аутономних возила. Ову констатацију потврђује изјава коју је 1. новембра 2017. године дао

Виктор Бондарев, председник Комитета за одбрану и безбедност Савета РФ, који закључује да ће вештачка интелигенција моћи да замени војника на бојном пољу, пилота у авиону и да се ближи дан када ће аутомобили – возила добити вештачку интелигенцију. Успешно је тестирано возило Нерехта (*Nerehta*), без возача – човека (копнено возило), а које је наводно надмашило постојећа борбена возила са возачима – човеком. Ово возило би могло да буде коришћено за развој и употребу вештачке интелигенције у борби, прикупљању обавештајних података, логистичким улогама. У времену недостатака возача на читавој планети, ови пројекти би били прави успех по питањима логистике, а што се тиче прикупљања обавештајних података где су оваква возила увек на најистуренијим, најугроженијим местима у сукобима, вредност оваквих пројеката нема цену, с обзиром да би се кретало без човека и војника, оператер не би био угрожен (угроженост би била искључиво финасијски елемент сагледавања, евентуално доступности технологија, губитака и бројност таквих возила у сукобу будућности). Копнено возило способно за аутономну идентификацију циља и погађање мете је наводно један од пројеката РФ, по питањима вештачке интелигенције, мада постоје планови и за уградњу вештачке интелигенције у ваздушна, поморска и подводна возила без присуства човека у њима. Истраживање употребе вештачке интелигенције за даљинско детектовање и електронско ратовање је још једна област интересовања. Руска Федерација је доста користила технологије вештачке интелигенције за *пропаганду и надзор*, као и за *спровођење информационих операција* усмерених против САД и чланица Североатлантског савеза. Аналитичари примећују да су истраживачи из РФ направили мало истраживачких радова на тему вештачке интелигенције и да заостају за онима из САД и Народне Републике Кине, међутим, да ли је ова констатација (податак) меродаван за озбиљну процену, када имамо толико озбиљних реметилачких случајева у сајбер простору од РФ, како то наводе Западни медији. Врло често се у проценама помињу и добри односи Народне Републике Кине са РФ где се очекује да би већ освојене програме вештачке интелигенције Кина могла евентуално уступити РФ (Hoadley & Sayler, 2020).

4.2.1.4. Улога обавештајне активности

Обавештајна активност је долазак до података, са основном улогом сазнавања о свету око нас које ће помоћи државном и војном руководству да донесу квалитетније одлуке и да се припреме за супротстављање потенцијалним и новим претњама државним интересима. Обавештајна активност почиње као одговор на познате или уочене захтеве од високих креатора политике, службеника одбране и полиције и војних команданата. Мада неке од ових и сличних информација могу бити доступне јавности, велики део тога прикривају те владе или организације (нпр. као терористи) који желе да то остане тајна. Можемо закључити да те и сличне информације произилазе обично из људских или техничких извора чије прикупљање је тајне природе. Прикупљање таквих информација је кључна одговорност обавештајне заједнице. Начин како то раде организације у обавештајној заједници је помоћу различитих техника сакупљања података и то: човек као извор обавештајних података представља податке добијене од појединаца који поседују, знају или имају приступ осетљивим страним информацијама, а које имају утицај по безбедносне интересе државе, утицај по националну безбедност. У обавештајној заједници САД овом врстом прикупљања података радом са људима се тежишно баве Централна обавештајна агенција, у сегменту одбране прикупљања података од људи, елемент Одбрамбене обавештајне агенције (енг.

Defense Intelligence Agency), а од почетка XXI века, Федерални истражни биро (познат у јавности под акронимом ФБИ) је примарни сакупљач података радом са људима за обавештајну заједницу. Сигнали као извори обавештајних података представљају све врсте података добијених од пресретнутих комуникација и електронског преноса података. У САД се овом врстом прикупљања података за обавештајну заједницу бави примарно Агенција за националну безбедност. Слике такође могу да се појаве као извори обавештајних података, мада се ова врста прикупљања података назива и геопросторно сакупљање обавештајних података, што представља експлоатацију и анализу слика и других геопросторних информација за описивање, процену и визуелни приказ физичких карактеристика и географски евидентираних активности на земљи. Када говоримо о САД, мислимо на Националну геопросторну – обавештајну агенцију[24], агенцију која има примарну одговорност за координацију прикупљања и обраду, снимљених слика технологијом са земље, неба или из свемира, података за потребе обавештајне заједнице. Мерење као извор обавештајних података представља технику доласка до података описом категорије технички изведених података које пружају одређене карактеристике. Када посматрамо нпр. догађај, неку активност попут нуклеарне пробе, експлозије, тада се лоцира, идентификује и описује специфичност свих карактеристика мете (фиксних или динамичких извора) кроз средства као што су оптичка, акустична или сеизмичка врста сензора. У обавештајној заједници САД, обавештајне организације у оквиру Одељења за одбрану – посебно су Одбрамбена обавештајна агенција, Национална геопросторно – обавештајна агенција и војне службе примарни сакупљачи података путем мерења као извора обавештајних података. Отворени извори као носиоци обавештајних података представљају долазак до обавештајних података путем јавно доступних података који се појављују у штампаном или електронском облику. Прикупљање података битних за националну безбедност и интересе државе се врло често описује као сирова активност агенција све док то не буде могуће сортирати, интегрисати и проценити од стране аналитичара у агенцијама, који желе да извуку значење и разумевање доступних података у вези са њиховим утицајем на интересе САД када ти „сирови" подаци уз добијање елемената процена од аналитичара постају информације за државно и војно руководство или евентуално друге кориснике таквих информација. Није редак случај да део или већина прикупљених података буду контрадикторни, па чак и обмањујући, подметнути од стране страних сила које намеравају да прикрију своје праве намере. Искусни аналитичари морају да допуне прикупљене податке и да пре формирања информације сопственим вештинама, искуствима и својом стручношћу процене валидност, вероватно значење свих података који су им доступни. Тако урађене анализе се затим преносе државном и војном руководству, као и другим службеницима одбране, полиције или другим корисницима (Weapons of Mass Destruction, 2005).

[24] Национална геопросторно – обавештајна агенција (енг. *The National Geospatial – Intelligence Agency*) пружа геопросторне обавештајне податке светске класе која даје одлучујућу предност креаторима политике, ратницима, обавештајним професионалцима и онима који први реагују. Пружа геопросторне обавештајне податке за безбедност САД, а само једну од тема ове службе када наведемо, сортирање милион фотографија дневно, као и одбрана нације од сајбер претњи подржавајући друге обавештајне агенције дубинском анализом сајбер мрежа (The National Geospatial – Intelligence Agency, 2022). Овде препознајемо моћ ове службе у необавештајним активностима у реализацији одвраћања.

Службе безбедности РФ су показале склоност да преусмере свој рад на прикупљање података ка актуелним темама које се појављују на међународној сцени, као што су стране истраге о тајним активностима РФ и догађајима у вези са проширењем Североатлантског савеза, нпр. убиство Александра Литвињенка 2006. године у Уједињеном Краљевству, смрт Березовског у Уједињеном Краљевству 2013. године, обарање лета број 17 малезијског авиопревозника изнад Украјине 2014. године, агресивност када државе размишљају о чланству у Североатлантском савезу, упади у компјутере у Црној Гори; затим, ситуација када је Грчка протерала двојицу руских дипломата и блокирала визе још двојици у знак одмазде за мешање у питање именовања Северне Македоније, оптужбе за употребу хемијског оружја, где је непосредна реакција РФ да то негира, док службе безбедности истовремено циљају на настале међународне истраге, РФ је стала на страну Сирије негирајући наводе да је сиријска влада користила хемијско оружје против свог народа у сиријском грађанском рату 2017. и 2018. године, покушај хаковања Организације за забрану хемијског оружја у Хагу, даљински упад у компјутере усмерене на хемијску анализу у лабораторији у Швајцарској (Riehle, 2022); рачунари *Bellingcata* поново су били на мети 2019. године након што је организација пријавила идентитете руских официра умешаних у напад на Скрипала, Влада РФ оптужена је да спроводи усаглашени програм допинга који спонзорише влада за руске спортисте који се такмиче на међународним спортским догађајима и сличне друге теме (Riehle, 2022).

Вештачка интелигенција би могла бити посебно корисна у обавештајним активностима. Већ дужи низ година један од највећих проблема доласка до податка битног за службе безбедности представља управо велики број скупова података доступних за анализу. Пројекат *Мавен* (енг. *Project Maven*) имао је за циљ да обједини вештачку интелигенцију и компјутере у ћелије за прикупљање обавештајних података које би селектовале снимке из летелица (дронова) и аутоматски идентификовале непријатељске објекте, активности. Сједињене Америчке Државе су кроз пројекат *Мавен* користиле алгоритме вештачке интелигенције за идентификацију побуњеничких циљева у Ираку и Сирији. Ради се о аутоматизацији рада „људских аналитичара" преко вештачке интелигенције. Раније је велики број аналитичара морао проводити сате прегледавајући снимке дронова у потрази за подацима који би могли бити корисни. На овај начин се аналитичари ослобађају, тако да могу да доносе ефикасније и правовремене одлуке на основу података које добијају на овај начин. Треба напоменути и да службе безбедности имају у току низ јавно признатих истраживачких пројеката вештачке интелигенције (да не помињемо да су вероватно поред јавно признатих присутни и они који су тајне природе). Да поменемо само америчку Централну обавештајну агенцију која има око 140 пројеката у развоју који користе вештачку интелигенцију (за препознавање фотографија и предиктивну аналитику). Интересантно је поменути и пројекат о развоју алгоритама за вишејезично препознавање и превођење говора у бучним окружењима, геолоцирање слика без придружених метаподатака, спајање слика у две димензије и креирање модела у три димензије и друге алате на основу обрасца – анализе живота. Недостатак званичне дефиниције вештачке интелигенције у САД може додатно закомпликовати рад у овој области (свака од војних служби користи другачију дефиницију вештачке интелигенције), што доводи до недоследности у типовима пројеката о којима се разговара, извештава, који се надзиру, контролишу, употребљавају (Hoadley & Sayler, 2020).

4.2.2. Контраобавештајна активност

4.2.2.1. Појам контраобавештајне активности

Формирањем *Тајног комитета* и *Комитета за тајну преписку* (*кореспонденцију*), који су се углавном бавили обавештајним активностима, дана 5. јуна 1776. године Континентални конгрес је формирао један комитет који је добио надлежности које су спадале у прве контраобавештајне активности на тлу данашњих САД. Наиме, овај комитет је требало да се бави: „...особама које непријатељу преносе обавештајне податке или му обезбеђују намирнице и муницију" (Юрьевич, 2014, p. 28). Комитет је добио назив Комитет за шпијуне (енг. *Committee on Spies*). Један од огромних успеха новоствореног Комитета за шпијуне било је разоткривање шефа медицинске службе војске Конфедерације, др Бенџамина Черча, који је неколико година обавештајне податке преносио Британцима. Комитет за шпијуне се доста бавио правним активностима супротстављања шпијунима. Комитет је припремио предлоге за унапређење правних норми у циљу борбе против шпијунаже. На пример, на основу резултата истраге о случају Бенџамина Черча, Комитет је припремио предлоге за пооштравање кривичне одговорности за шпијунажу. Већ у августу 1776. године, донет је први, можемо да констатујемо „антишпијунски" акт у америчкој историји, који је прописао чак смртну казну за особе осуђене за прикупљање и преношење војном непријатељу података о утврђењима, саставу и распореду оружаних снага било које од држава. Случајеве шпијунаже судили су војни судови. Особе осумњичене за шпијунажу могле су бити осуђене само ако су прослеђивале обавештајне податке војном непријатељу снага Конфедерације, што значи да се наведено односило само на ратно стање и активности предузимане у току ратног стања. Допуна антишпијунског акта је уследила у фебруару 1778. године, када је додато да је кривично дело и преношење војном непријатељу Конфедерације података који су помагали непријатељу да „хвата или убија патриоте" (Юрьевич, 2014).

У САД појам контраобавештајне активности је одређен у *Закону о националној безбедности у САД* (енг. *Sec. 3, p. 5*) као енг. *counterintelligence* и означава прикупљање информација и спровођење активности у циљу заштите од шпијунаже, друге обавештајне активности, саботаже или атентата које су планирале стране владе или други елементи у њихово име страних организација или страних лица или међународних терористичких активности (National Security Act of 1947, 2021).

На сличан начин је контраобавештајна активност одређена и у Извршном наређењу 12333, Председника САД „тачка 3.5, параграф (а) који се опет позива на напред наведени Закон о националној безбедности, као прикупљање информација и активности спроведених у циљу идентификовања, обмањивања, експлоатације, ометања или заштите од шпијунаже, других обавештајних активности, саботаже или атентата за или у име страних сила, организација или особа, или њихових агената, или међународних терориста организације или активности" (Executive Order 12333, 2008, p. 15).

На основу Контраобавештајног речника[25] (енг. *Counterintelligence glossary*), можемо сагледати како велики број теоретичара на западу одређује термин контраобавештајног рада

[25] Контраобавештајни речник је 2014. године приредила канцеларија енг. *Defense Counterintelligence and Human Intelligence Center* (*DCHC*) која чини део Одбрамбене обавештајне агенције САД – енг. *United States Defense Intelligence Agency* (Counterintelligence Glossary, 2014).

тј. активности. Тако Годсон (*Roy Godson*) сматра да је рушење обавештајних напора противника централна функција контраобавештајне активности. Намара (*Francis McNamara*) каже да је контраобавештајна активност способност посебне врсте, плус још нешто и да се контраобавештајним радом прикупљају, чувају, анализирају и шире информације о одређеним страним претњама безбедности државе, а затим делује у циљу њиховог уништавања или неутралисања. Крајња сврха контраобавештајне активности нису пуко прикупљање и анализа информација, већ акција, и то успешна акција против оних који угрожавају безбедност државе. Контраобавештајна активност по Потету (*S. Eugene Poteat*) мора тежити да сазна све могуће о противниковим обавештајним способностима, укључујући његове изворе и методе прикупљања, његове необавештајне активности у утицају и управљању нашим акцијама и перцепцијама, па чак и његову културу и мисаоне процесе. Интересантна је и дефиниција Одома (*William E. Odom*) о контраобавештајној активности као информацији о противниковим обавештајним операцијама, способностима, агентима, технологији прикупљања итд. То није безбедност. Обавештајна активност је та на којој треба да се заснивају безбедносне политике. Ради се о прикупљању обавештајних података о противниковом креирању политике или војним операцијама или другим необавештајним способностима и активностима. Одом такође констатује да је контраобавештајна активност најтајанственија и организацијски фрагментиранија, најмање доктринарно разјашњена, а правно, тиме и политички, најосетљивија активност. Ловентал (*Mark M. Lowenthal*) говори да напори предузети ради заштите сопствених обавештајних операција од продора и ометања непријатељских држава или њихових служби безбедности чине контраобавештајну активност. То је и аналитичко и оперативно, није засебан корак у обавештајном процесу већ важна функција током читавог процеса. Контраобавештајну активност Милер (*Newton Miller*) одређује као национални напор да се спречи да стране службе безбедности продру у наше институције и успоставе потенцијал за бављење шпијунажом, субверзијом, тероризмом и саботажом. Хавер (*Richard L. Haver*) у контраобавештајну активност укључује употребу и офанзивних и одбрамбених мера за: заштиту осетљивих државних информација и операција од компромиса и продора страних служби безбедности и других непријатељских ентитета; обезбеђују безбедност и интегритет текућих државних дипломатских, војних и обавештајних операција; и продиру, компромитују и неутралишу непријатељске операције које су водиле стране службе безбедности, терористичке организације и нарко картели. Графенрајд (*Kenneth E, deGraffenreid*) сматра да контраобавештајна активност укључује све прикупљене информације и активности које спроводи влада у циљу откривања, анализирања и сузбијања претњи. Термин се односи на активне операције спроведене у циљу сузбијања – откривања, процене, неутрализације и манипулације – обавештајних операција страних држава и група. Укључује регрутовање страних обавештајних официра, прекид активности, гоњење кривично шпијунаже, манипулације и обмане. Укључује употребу надзора, двоструких агената и других тајних техника. Појам контраобавештајне активности Ричелсон (*Jeffery Richelson*) види као термин који се често повезује са хватањем шпијуна. То је такође прикупљање информација и активности спроведених у сврху ометања и неутралисања активности непријатељских служби безбедности. Кодевила (*Angelo Codevilla*) појам контраобавештајне активности дефинише као контролу квалитета обавештајних података и кључ борбе између држава и војски за повољан диспаритет знања. Тиче се свих осталих аспеката обавештајне активности и мора користити све елементе обавештајне службе као део себе, док

истовремено контраобавештајна активност у целини мора бити део анализе, прикупљања и прикривених акција коју спроводе службе безбедности. У својој перспективи која гледа према унутра, контраобавештајна активност је двострука провера сопствених обавештајних операција. У својој перспективи која гледа према ван, то је најоштрије оружје у обавештајном арсеналу. Започели смо са Годсоном (*Roy Godson*), па и да завршимо овај део истраживања са Годсоном, који контраобавештајну активност дефинише и као стратешки инструмент доступан државама да се заштите и унапреде своје интересе у борби за моћ, богатство и утицај. Крајњи производ, мисија контраобавештајне активности тј. службе, је акција – акција за заштиту од странаца и акција за манипулисање странцима у служби националних циљева (Counterintelligence Glossary, 2014). Циљ контраобавештајне активности је да заштити агенцију (или клијента) од инфилтрације противника, ради заштите од нехотичног цурења поверљивих информација и да осигура њихове инсталације и материјал против шпијунаже, субверзије, саботаже, тероризма и других облика политички мотивисаног насиља и преноса кључних технологија и/или опреме. То је активан модел који позива на дефанзивне, као и офанзивне методе безбедности и користи истраживање и анализу која су срж обавештајне функције. Иако постоји јасна разлика између обавештајне и контраобавештајне активности, ова линија разграничења може бити танка. Када се нација бави, на пример, недржавним актерима или транснационалном криминалном организацијом постоји мало разграничења између онога што би могло представљати питање националне безбедности и рецимо, проблем спровођења закона (Prunckun, 2019).

Контраобавештајна активност се састоји од дефанзивних и офанзивних мера заштите. Дефанзивних провером властитих државних службеника и намештеника, истрагама, праћењем познатих или сумњивих агената и надзорне активности ради откривања и неутралисања присуства страних обавештајних служби, а офанзивних кроз упоређивање информација о страним обавештајним службама и њиховом начину рада, кроз регрутовање агената и покретање операција за продор, ометање, обмањивање и манипулисање ове услуге и сродне организације у своју корист. Контраобавештајна активност је саставни део целокупног обавештајног процеса осмишљеног да се уверите да су прикупљене истините процене и информације. С обзиром да је шпијунажа злочин, неке контраобавештајне службе воде ка спровођењу закона операцијама. Међутим, хватање шпијуна и откривање страних техничких могућности су сложеније активности од хватања домаћих и страних криминалаца. Мотивације и ресурси који подржавају криминалце разликују се од оних које подржавају стране обавештајне службе (Geneva Centre For The Democratic Control Of Armed Forces, 2003).

Можда бисмо иностранa поимања контраобавештајних активности могли закључити констатацијом професора Џонсона (*Loch K. Johnson*) да „контраобавештајна активност значи прикупљање информација и спровођење активности на идентификацији, обмањивању, експлоатисању, ометању или заштити од шпијунаже, других обавештајних активности, саботажа или атентата спроведених за или у име стране силе, организације или лица или њихових заступника, или међународних терористичких организација или активности" (Johnson, 2017, p. 172). Једноставно речено, задатак контраобавештајних служби је да кроз примену контраобавештајних активности се осујете непријатељска дела почињена против једне нације активностима страних служби безбедности, терористичких фракција и унутрашњих субверзија (Johnson, 2017).

Поред теоретског закључка, можемо дати констатацију и државних органа САД о контраобавештајним активностима. Контраобавештајне активности обухватају „прикупљање података и спровођење активности ради идентификације, обмањивања, искоришћавања, онемогућавања или заштите од шпијунаже или друге обавештајне активности, саботаже, или атентата спроведеног за или у име стране силе, организације, или лица или њиховог агента, или међународне терористичке организације" (Strategic Plan 2018–2022, 2017, p. 2).

Контраобавештајна активност укључује све активности неопходне за разумевање и побеђивање претње од злонамерних учесника. Контраобавештајне активности су груписане у три основне области: „1) Анализа, сакупљање и контраобавештајне операције; 2) Ланац снабдевања, сајбер и техничка претња и процена рањивости и противмере; 3) Национална контраобавештајна политика и стратегија, мерење учинка, професионални развој контраобавештајне радне снаге и заступање ресурса" (Strategic Plan 2018–2022, 2017, p. 17).

У Републици Србији, контраобавештајну активност Мијалковски одређује као планирану, организовану и тајну активност служби безбедности Републике Србије, првенствено на њеној територији, ради откривања, праћења, пресецања и онемогућавања чињења недозвољених активности страних служби и необавештајних активности страних служби безбедности и других активности лица, група и организација на територији наше државе усмерених против интереса безбедности државе (Мијалковски, 2009). У животу, некада најобичнији, наизглед најбезазленији подаци о некој особи или некој ствари могу бити врло битни да остану тајна; некада датум рођења, венчања, подаци о деци и слично могу бити коришћени као приступне шифре за коришћење разних тајних података, употребе јединица оружаних састава државе, ракетних система, па до употребе нуклеарног наоружања. Приватне тајне могу довести до компромитације особе на послу, у друштву, породици, а службене тајне, у приватним фирмама или државним које се односе на националну безбедност неопходно је сачувати ради заштите живота људи, објеката, средстава, друштва, државе, па се тако развио сегмент рада служби безбедности познат као контраобавештајна активност. У основи свог рада, контраобавештајна активност представља превентивно деловање у сврху одвраћања: да се не почине недозвољене активности, а уколико исте буду учињене, онда се баве њиховим откривањем, у зависности од норматива у конкретној држави, врло често и документовањем такве активности ради процесуирања пред надлежним судовима. Неке контраобавештајне службе се поред контраобавештајне активности баве и другим безбедносним пословима (нпр. *безбедносне заштите* – наведено је изузетно комплексна и обимна област и могла би бити посебна теза за истраживање, па неће бити обрађивана у овом истраживању).

Мијалковић контраобавештајну активност дефинише као посебан облик мера, радњи и поступака које се предузимају најчешће од стране служби безбедности и усмерене су на спречавање и сузбијање: обавештајних и необавештајних (субверзивних) активности страних служби безбедности, тероризма, угрожавајућих делатности чији су носиоци екстремисти, угрожавања носилаца највиших државних и војних функција и објеката, као и најтежих облика привредног, финансијског и организованог имовинског криминалитета (Мијалковић, 2011). Конкретније, Бајагић под контраобавештајним активностима подразумева „активности на превенцији и пресецању обавештајних продора страних обавештајних служби и других ентитета, док класичне службе безбедности у делокругу свог рада имају заштиту уставног поретка, целовитости и независности земље, откривање и превенцију других претњи

безбедности, као што су екстремистичка понашања и деловања, разни облици кршења људских права и слобода, спречавање тероризма, организованог криминала, ширења оружја за масовно уништавање, итд.” (Бајагић, 2010, стр. 4). Сврха контраобавештајне активности је превентивно деловање и предлагање мера надлежним државним органима ради спречавања нежељених тајних делатности, а уколико исти не поступе сходно наведеним предлозима, треба да предузму део својих овлашћења ради спречавања угрожавања националних интереса.

4.2.2.2. Функције контраобавештајне активности у Сједињеним Америчким Државама и Руској Федерацији

Према Стратегијском Плану од 2018–2022, Националног контраобавештајног и безбедносног центра САД, селектовано је шеснаест сектора *критичне инфраструктуре* у САД које је неопходно штитити: „хемијски сектор, бране, финансијске услуге, информациона технологија, комерцијални објекти, одбрамбена индустријска база, храна и пољопривреда, нуклеарни реактори, материјали и отпад, комуникације, хитне службе, владини објекти (у јануару 2017, америчка изборна инфраструктура одређена је као подсектор постојећег сектора државних објеката), транспортни системи, критична индустрија (производња), енергија, здравство и јавно здравље, системи за воду и отпадне воде” (Strategic Plan 2018–2022, 2017, p. 6). Безбедносне активности укључују све активности неопходне за заштиту критичне инфраструктуре САД, поверљивост мрежа, информација и особља. „*Безбедносне активности* су груписане у три примарне области: 1) Процене безбедносних претњи; 2) Мере и активности на заштити извора и метода, безбедносни прегледи и инспекције; 3) Смернице за политику, Активности извршног агента за безбедност, Безбедносна дозвола за реформе, Стална евалуација, Програми инсајдерских претњи, Безбедносна радна снага, Програми стручног усавршавања и Заступање ресурса” (Strategic Plan 2018–2022, 2017, p. 17).

Контраобавештајна активност у САД представља прикупљање информација и примену разних врста мера, радњи и поступака које се спроводе у циљу идентификације, обмане, експлоатације, ометања или заштите од шпијунаже, других обавештајних активности, саботаже или убистава извршених за или у име страних сила, организација или лица, или њихових агената, или међународних терориста, организације или активности (Executive Order 12333, 2008). На основу наведеног, врло штурог одређења контраобавештајне активности (које не обухвата све послове, контраобавештајне активности, да ли намерно или не, није нам познато, прим. аут.), можемо закључити да у контраобавештајним активностима САД постоје следеће функције: а) прикупљање података (о деловању страних обавештајних служби, терориста, идентификацији обмане, примени субверзивних активности и др. недозвољених делатности), б) обрада и допуна података, в) процењивање, стварање информације, г) предлог превентивних мера и д) реализација одређених мера или контрола спроведених мера од стране надлежних лица, институција, организација.

Када је реч о РФ, ту имамо доста детаљније образложену контраобавештајну активност у Закону о Федералној служби безбедности РФ (за разлику од САД и термина активности, у РФ се користи термин делатност, контраобавештајна делатност). Контраобавештајна активност (делатност) обухвата радње које обављају савезни органи

службе безбедности и (или) њихове јединице (контраобавештајне службе), као и службена лица ових органа и одељења путем контраобавештајних мера у циљу откривања, спречавања, сузбијања обавештајне и друге активности специјалних служби и организација страних држава, као и појединаца, усмерене на наношење штете безбедности РФ (О федеральной службе безопасности, 2022). Функције контраобавештајних активности које произилазе из наведеног закона су следеће: „а) идентификација обавештајних и других активности специјалних служби и организација страних држава, као и појединаца, у циљу наношења штете безбедности РФ и предузимање мера према истим; б) установљавање догађаја или радњи које представљају претњу безбедности РФ и предузимање мера према истим; в) заштита тајних података (највишег степена); г) потреба за проучавањем лица која пружају или су пружала помоћ органима савезне службе безбедности на поверљивој основи; д) сопствена заштита; ђ) спровођење закона и за потребе других у складу са међународним уговорима РФ; е) борба против тероризма” (О федеральной службе безопасности, 2022, члан 9.).

Бајагић следеће функције наводи у контраобавештајним активностима: а) заштиту тајних података, б) прикупљање података о страним обавештајним службама и њиховим активностима и намерама; в) процењивање (анализа) безбедносно интересантних података и израду информација и г) мере у циљу предупређења чињења недозвољених делатности и операције у циљу уништавања и неутралисања потенцијала страних служби безбедности које предузимају друге разноврсне необавештајне активности против националних интереса и националне безбедности (Бајагић, 2009).

4.2.2.3. Процес контраобавештајне активности

Предузимање одређеног одговора састоји се од претњи или предузимања противмера. У наредном делу рада, уместо конкретног примера, сагледаћемо наведени процес кроз „виртуелни пример и замишљену матрицу”. Када говоримо о радњама предузетим као одговор на одређена кршења међународног права од стране друге државе, тада говоримо о једностраним реакцијама које су у суштини незаконите, када једна држава сматра да је друга починила међународну противправну радњу која би могла оправдати такву реакцију. Противмере се употребљавају када се жели подстаћи поштовање, као и спровођење међународних правних обавеза (неопходно је претходно међународно противправно дело; то дело да се може приписати држави; са циљем да се подстакне поштовање починиоца; мере су ограничене на ненасилне и само пропорционалне радње; потребан је претходни захтев починиоцу; и противмере нису дозвољене када је незаконито дело престало). У погледу реаговања на претходне сајбер инциденте који крше међународно право, противмере би се могле односити на активно хаковање када се зна која је локација, инфраструктура коришћена (мрежа, системи), тј. када је иста позната, нпр. ако је укључен штаб Главне управе (војне службе безбедности РФ, некада познатије као Главне обавештајне управе), да се заустави кршење, или да се покрене акција против државе која је требала да делује да заустави њихову инфраструктуру да чини такве прекршаје или нису уопште ни биле вољне да то учине (Ducheine & Pijpers, 2021).

Матрица (*Табела 6*) је састављена од разних инструмената снаге као што је претходно описано. Она показује како државе могу да прибегну посебним правним основама када се

разматра коришћење инструмената моћи. Нумерисане ознаке нуде реалистичне варијанте, комбинације инструмената/модалитета и правну основу.

Табела 6. Опција 1 – правних основа.

Инструмент правне основе	Пристанак	Реторзија (реципроцитет, узајамност)	Противмере	Изјава о неопходности	Самоодбрана
Дипломатија	1	2			
Информације и знање (укључујући службе безбедности)	3	4	5	6	7
Војска	8	9*	10*	11*	12
Привреда и финансије	13	14	15	16	
Култура	17	18			
Правни	19	20	21	22	

** означава само ненасилну акцију.*

Извор: Ducheine & Pijpers, 2021, p. 493.

Матрица приказује варијанту у којој је на основу одлуке Кабинета, министар спољних послова наредио преговарачком тиму билатералну трговинску сарадњу са неком државом, да паузира консултације. Одлука је донета након годишњег Извештаја једне од обавештајних служби када је откривено да је та држава ухваћена у покушају да ексфилтрира украдену интелектуалну својину. Министар је то најавио у Парламенту, који је формулисао питања да би се сазнало што више детаља. Користећи матрицу, овај пример се може приказати на следећи начин (*Табела 7*).

Табела 7. Опција 2 – Зауставити дипломатске консултације (реторзија).

Инструмент	Дипломатија
Акција	Зауставите консултације
Парадигма	Дипломатија
Ауторитет	Кабинет/Министарство спољних послова
Правна основа	Реторзија
Акција од	Министарство спољних послова
Надзор	Парламент

Извор: Ducheine & Pijpers, 2021, p. 494.

Следећа матрица (*Табела 8*) приказује опцију која укључује контраобавештајну операцију. На основу овлашћења министра унутрашњих послова, служба безбедности је преузела контролу над командом и контролним сервером који се налази у некој држави који је користио један од проксија те државе за управљање великим ботнетом који прети да преоптерети комуникације званичника. Министар је обавестио Парламентарни обавештајни одбор и Одбор за контролу служби безбедности како би проценили легитимност операције у наредној години.

Табела 8. Опција 3 – Контраобавештајна операција (предузимање противмера службе безбедности).

Инструмент	Информативни (службе безбедности)
Акција	Преузмите контролу над сервером
Парадигма	Контрамере
Ауторитет	Министар унутрашњих послова
Правни основ	Противмере
Акција	Служба безбедности (СБ)
Надзор	Парламент и Одбор за контролу СБ

Извор: Ducheine & Pijpers, 2021, p. 494.

Када говоримо о процесу контраобавештајних активности, Бајагић (позивајући се на литературу са запада) тада наводи да је у циљу откривања деловања страних обавештајних служби неопходно предузимати редовне (енг. *current*) и упозоравајуће (енг. *warning*) контраобавештајне активности. Наведено се предузима ради непредвидивости и изненадног штетног деловања офанзивних и умрежених страних обавештајних продора и других савремених претњи безбедности, а превенствено како би се спречиле нежељене делатности или ублажиле последице већ учињених обавештајних или необавештајних активности (Бајагић, 2009). Откривањем страних обавештајних активности, процес контраобавештајних активности обухвата преусмеравање сопствених капацитета и њихово дубоко стратешко, оперативно и тактичко имплементирање у структуре непријатеља на сопственој територији, територији државе која је носилац тих активности, или треће државе у којој се евентуално одвија страна обавештајна активност (Бајагић, 2009). Сагледан из овог угла, процес контраобавештајне активности укључује пасивне и активне мере у супротстављању непријатељским операцијама. У стратегијском смислу, према Бајагићу, процес контраобавештајних активности подразумева следеће: 1) развој контраобавештајних потенцијала; 2) руковођење контраобавештајним надзором; 3) развој контраобавештајних планова; 4) руковођење контраобавештајним операцијама, и 5) помоћ у имплементацији контраобавештајних мера (Бајагић, 2009). Фазе процеса контраобавештајних активности могу се сврстати у следеће: а) дефинисање планова и мера и заштита сопствених потенцијала и безбедносних интереса, б) реализација истраживања у циљу откривања и процене природе претњи, в) уочавање и разумевање претњи и процена рањивости, г) дефинисање и реализација акција на плану одвраћања претњи, д) анализа реализованих акција из угла процене коришћених људских и технолошких потенцијала, и е) дефинисање будућих (контра)обавештајних потреба и планова (Бајагић, 2009). Све наведене фазе процеса контраобавештајне активности су врло важне. Када говоримо о реализацији процеса контраобавештајне активности, морамо имати у виду и питања која се односе на избор метода, инфраструктуре и кадрова који учествују у тој реализацији. Ипак, посебно се истичу проблеми везани за људске изворе. Прво, људски извори могу обезбедити виталне информације, али је питање колико су они поуздани и да ли су подаци тачни или не (Бајагић, 2009).

У РФ се у процесу контраобавештајне активности (делатности) предузимају отворене и прикривене мере, чија је посебност одређена условима ове делатности. Поступак спровођења контраобавештајних мера се утврђује подзаконским актима савезног органа извршне власти у области безбедности. Спровођење контраобавештајних мера којима се ограничавају права грађана на тајност преписке, телефонских разговора, поштанских, телеграфских и других порука које се преносе преко електричне и поштанске мреже, дозвољено је само на основу одлуке суда и на начин прописан законом, путем законодавства РФ. Спровођење контраобавештајних мера „којима се ограничава право грађана на неповредивост њихових стамбених јединица, дозвољено је само у случајевима утврђеним савезним законом, или на основу одлуке судије" (О федеральной службе безопасности, 2022, члан 9.).

4.2.2.4. Контраобавештајно стратешко одвраћање

У јуну 1940. године, Конгрес је донео Закон о регистрацији (енг. *Smith Act*), који је такође прилично активно користила контраобавештајна служба у интересу спровођења националне безбедности САД од спољне претње. Ради се о Закону о регистрацији странаца, који је такође познат као Смитов закон. Закон се састоји од три наслова, од којих први криминализује позиве на рушење уставног поретка САД, затим подстицања и вршења пропаганде против Владе САД или против њених активности, и не садржи никакве услове за регистрацију. Углавном се састоји од измена и допуна Закона о имигрантима из 1917. године. Закон о регистрацији је предвидео утврђивање кривичне одговорности за евентуално избегавање регистрације. Закон о регистрацији странаца такође уводи обавезно узимање отисака прстију странаца који улазе у САД (изузетак су дипломатско и административно – техничко особље званичних мисија, службеници страних држава и неке друге категорије страних држављана). Супротстављање таквим претњама безбедности државе које долазе од спољних непријатељских снага. Закон о регистрацији није изгубио на актуелности и успешно решава задатке који су истим додељени (Alien Registration Act, 1940). Поред поменутих закона о регистрацији, усвојен је још један закон који директно утврђује обавезу регистрације оних лица која због својих професионалних *вештина* могу учествовати у обавештајним или субверзивним активностима против САД. Тако сва лица са вештинама или обуком у области шпијунаже, контрашпијунаже, саботаже или субверзивне делатности, или која су упозната са тактиком стране државе или стране у овим стварима, подлежу обавезној регистрацији код Министарства правде САД. Лица која служе у обавештајним или контраобавештајним јединицама стране државе такође морају бити регистрована (Registration of Certain Persons Trained in Foreign Espionage Systems, 1956). Услед евентуалног непријављивања, казне су ригорозне, до 5 година затвора или новчане.

Неопходно је поменути Закон о контраобавештајном и безбедносном унапређењу стања из 1994. године чиме је дата могућност САД да уступа финансијске подстицаје за лица која заинтересованим службама безбедности или другим овлашћеним државним агенцијама желе да уступе сазнања о поступцима шпијунаже и предузимања субверзивних активности усмерених против САД. Према Закону о унапређењу контраобавештајне службе и безбедности из 1994. године, свако лице које уступи САД, сазнања, која би довела до: хапшења или оптуживања особе која је извршила (било где) чин шпијунаже против САД, затим извршења хапшења или је подигнута оптужница против особе која је покушала или се удружила са другима да изврши дело шпијунаже против САД, као и ако је неко ко је учинио акт шпијунаже усмерен против САД спречен или осујећен да то учини, може рачунати не само на примање награде од САД, већ и на законску гаранцију поверљивости такве сарадње и заштите од стране САД (Counterintelligence and Security Enhancements Act of 1994, 1994).

Национални контраобавештајни извршилац – служба (енг. *National Counterintelligence Executive*) САД створен је 2001. године, а Канцеларија за Националну контраобавештајну службу (енг. *Office of the National Counterintelligence Executive*[26]) установљена је Законом о

[26] Хапшење Олдрича Ејмса (*Aldrich Hazen Ames*), бившег припадника Централне обавештајне агенције, дана 21.02.1994. године од стране Федералног истражног бироа, под оптужбом шпијунаже у корист Комитета државне безбедности је био повод формирања Националног контраобавештајног центра којег је Канцеларија за Националну контраобавештајну службу наследила 2001. године (Ames, 1994).

унапређењу контраобавештајне активности из 2002. године (*Counterintelligence Enhancement Act of 2002.*). У 2004. години, у складу са Актом о Реформи обавештајне службе и превенцији против тероризма (енг. *Intelligence Reform and Terrorism Prevention Act*), Канцеларија за Националну контраобавештајну службу је интегрисана у Канцеларију директора Националне обавештајне заједнице (енг. *Office of the Director of National Intelligence*). Центар за специјалну безбедност (енг. *Office of the Director of National Intelligence/Special Security Center*) и Центар за безбедносну процену (енг. *Office of the Director of National Intelligence/Center for Security Evaluation*) су накнадно интегрисани у састав Канцеларије за Националну контраобавештајну службу, 2010. године како би се ојачала координација и повећала енергија унутар ових целина, што се првенствено односи на контраобавештајне активности и безбедносне активности. Центар за специјалну безбедност је преименован у Управу за специјалну безбедност (енг. *special security directorate*), где наставља да се тежишно бави безбедношћу особља, обављајући функцију директора Националне обавештајне заједнице (енг. *director of National intelligence*). Извршни агент за безбедност (енг. *security executive agent*[27]) власти одобрава реформе и континуиране евалуације. Канцеларија за Националну контраобавештајну службу, у име директора Националне обавештајне заједнице, заједно са Федералним истражним бироом, у име америчког државног тужиоца, врши надзор и даје упутства Националној радној групи за инсајдерске претње (енг. *National Insider Threat Task Force*) која је основана Извршним наређењем 13587 (*Executive Order 13587*) 2011. године. Центар за безбедносну процену, у консултацији са Обавештајном заједницом (енг. *Intelligence community*), подржава владу у извршавању њених обавеза да обезбеди заштиту тајних информација о националној безбедности и да пружају друге функције везане за безбедност које утичу на интересе обавештајне заједнице у дипломатским и конзуларним објектима САД у иностранству. Директор Националне обавештајне заједнице је дана 1. децембра 2014. године означио Канцеларију за Националну контраобавештајну службу као Национални контраобавештајни и безбедносни центар (енг. *National Counterintelligence and Security Center*) да би ефикасно интегрисао и ускладио контраобавештајне активности Канцеларија за Националну контраобавештајну службу и области безбедносних активности под Управом за специјалну безбедност и Центром за безбедносну процену, омогућавајући директору Националне обавештајне заједнице да се бави контраобавештајним и безбедносним активностима у оквиру једне организације. Оснивање Националног контраобавештајног и безбедносног центра је у складу са овлашћењима директора Националне обавештајне заједнице за успостављање националних обавештајних центара за решавање обавештајних приоритета. Национални контраобавештајни извршилац – служба је такође била претпостављена директору Националног контраобавештајног и безбедносног центра и контраобавештајни ауторитет који је одређен у Закону о побољшању контраобавештајне активности из 2002. године, што је

[27] Директор Националне обавештајне службе, у складу са Извршним наређењем 13467, одговоран је, као Извршни агент за безбедност, за развој, имплементацију и надзор ефективних, ефикасних и јединствених политика и процедура које регулишу спровођење истрага и одлуке о подобности за приступ поверљивим информацијама и подобности за обављање осетљивих функција. Док је директор Националне обавештајне службе првенствено фокусиран на Обавештајну заједницу (енг. *Intelligence community*), као Извршни агент за безбедност, његове одговорности су додатно проширене да покрију процесе безбедности особља у свим агенцијама, широм владе (Security Executive Agent, 2022).

остало непромењено. Дана 1. децембра 2015. године, *нови печат* (*амблем*) је заменио стари печат Канцеларије за Националну контраобавештајну службу, тако да она има и контраобавештајну и безбедносну функцију, а тај нови печат је симбол формираног Националног контраобавештајног и безбедносног центра. Законом о овлашћењу обавештајних служби за фискалну 2017. годину, преименована је Канцеларија Националне контраобавештајне службе у Национални контраобавештајни и безбедносни центар, а Национална контраобавештајна извршна служба у Национални контраобавештајни и безбедносни центар (Strategic Plan 2018–2022, 2017).

Канцеларија за управљање особљем у САД (енг. *U. S. Office of Personnel Management – OPM*), односно Извршни агент за подобност (енг. *suitability executive agent*), пружа смернице и упутства у складу са Извршним наређењем 13467, да „процеси реформисања буду у вези са подобношћу за запошљавање у влади, подобности запослених у извођачима и квалификованошћу за приступ поверљивим националним безбедносним Информацијама". Оснивање Извршног агента за подобност као сопствене програмске канцеларије у оквиру Канцеларије за управљање персоналом САД, резултат је амандмана на Извршно наређење 13467 (Suitability Executive Agent, 2022).

Вршење безбедносне провере представља испитивање лојалности, карактера, поверења и поузданости појединца за приступ тајним подацима везаним за националну безбедност. Даље у Извршном наређењу 13467 је прописано да ће директор Националне обавештајне заједнице служити као извршни агент за безбедност и да ће управљати надзором истрага и утврђивања подобности за приступ тајним подацима или подобности за обављање осетљивог положаја било које агенције у САД. Дужан је да обезбеди делотворну, ефикасну и благовремену истрагу и одлуку у вези са утврђивањем подобности за приступ тајним подацима или подобности за обављање одређених дужности. Вршење провере о подобности је испитивање карактерних особина и понашања особе које се могу утврдити толико да то буде довољно да се одлучи да ли би пријем таквог лица у систем, његово (њено) запослење или друга варијанта (за лица која су већ запослена, постављења на више или одговорније дужности или са вишим степеном приступа тајности и сл.), наставак рада провераваног лица, заштитио интегритет или унапредио ефикасност службе њиховим пријемом или наставком рада. Директор Канцеларије за управљање особљем у САД, односно Извршни агент за подобност ће спроводити потребне процедуре. Директор Канцеларије за управљање особљем у САД ће бити одговоран за развој и примену једнообразних политика и процедура како би се обезбедио ефективан, ефикасан и правовремен рад на проверама и доношењу одлука у вези са утврђивањем подобности лица за приступ тајним подацима и/или раду на одређеним дужностима у служби (Executive Order 13467, 2008).

Продирање у службе безбедности (обавештајну или контраобавештајну) РФ даје низ предности, и то следећих: омогућава РФ да идентификује агенте, шпијуне у својој средини, пружа поглед, правац, усмерење у приоритете националне безбедности друге земље и отвара приступ поверљивим информацијама које се деле са службама безбедности из читавог циљаног иностранства владе и њених савезника. Већина јавно познатих случајева наступа припадника служби безбедности РФ од 2000. године односи се на Естонију, што одражава и

агресивне контраобавештајне напоре Естоније против РФ и њену спремност да отворено разговара[28] о продорима своје контраобавештајне службе (Riehle, 2022).

Да се држава мора поштовати, говори и велики број *средстава* (обавезујућих нормативних аката) у РФ који на стратешком нивоу регулишу одвраћање које се примењује првенствено у контраобавештајне сврхе. Наиме, низ нормативних аката Федералне службе безбедности може се користити у сузбијању интерног неслагања међу грађанима у РФ, а ради се првенствено о следећим нормативима: порески закони, закони против екстремизма, тероризма и организованог криминала, као и против прања новца и трговине наркотицима, као и законима који забрањују изазивање мржње или јавно вређање овлашћеног представника у вези са испуњавањем његових обавеза према држави. Неопходно је напоменути да је 2012. године Државна дума РФ усвојила амандмане којима се судијама дозвољава да се у поступку према лицима које надлежни органи реда у држави приведу правди, протест једног лица третира као недозвољено окупљање, под условом да се документује „заједничка намера и организација" (Riehle, 2022, p. 103). Мера коју је РФ предузела после 2016. године је формирање Националне Гарде која је одговорна за спровођење закона против окупљања и спречавање протеста ради угрожавања владајућег режима. Није наодмет констатовати да формирање Националне Гарде подсећа на формирање Окхране од стране цара Александра III, па се може поставити питање шта је поред свих постојећих служби безбедности у РФ навело руководство ове државе на овакав потез.

4.2.2.5. Контраобавештајне активности у корпоративној безбедности

Можда први или један од првих норматива на Западу који одређује, даје обавезе службама безбедности према корпорацијама јесте Обавештајна директива Савета за националну безбедност број 7 из 1948. године о одговорности америчке Централне обавештајне агенције за развој обавештајних извора у америчким корпорацијама и невладиним организацијама. Директива такође наводи обавезе за америчку Централну обавештајну агенцију према страним службама безбедности и обавезе службе безбедности у САД. Једна од тих обавеза је да се прибаве информације о страним обавештајним подацима које су одсеци и агенције добили као нуспроизвод нормалног односа у пословању корпорација и других невладиних организација и појединаца у САД у вези са необавештајним активностима (National Security Council Intelligence Directive No. 7, 1948). Давање обавезе кључној служби безбедности у САД да прибави информације о пословању корпорација и других невладиних организација, за озбиљну службу као што је Централна обавештајна агенција (која се иначе тежишно бави обавештајним, али како овде констатујемо и задацима контраобавештајне природе у које се укључују приватне фирме, корпорације, невладине организације) значило је стратегијски правац ангажовања службе. Наглашавамо да се ради о 1948. години, а када само помислимо на сва дешавања на територији читаве Европе, па и бивших република Социјалистичке Федеративне Републике Југославије и другим државама где је видно било присуство САД у „регулисању безбедносних проблема",

[28] Монографија у којој је анализирано кривично гоњење коришћењем естонског закона о издаји, добила је податке од Канцеларије главног тужиоца Естоније 2019. године и том приликом је идентификовано 20 лица процесуираних по наведеном закону од 2008. до 2018. године. Карактеристично је да је свих 20 лица било повезано са Руском Федерацијом (Riehle, 2022).

можемо да констатујемо да је три деценије уназад наведена активност доживела експанзију резултата овог и сличних деловања услед инфилтрације у наведене ентитете или чак и формирање истих од стране служби безбедности без званичног признања.

Поново морамо нагласити да, према Џонсону (*Loch K. Johnson*), контраобавештајно (обавештајно) особље мора бити квалитетно обучено. Постоји тенденција да се било који контраобавештајац (обавештајац) може преместити из службе безбедности без додатне обуке и обављати контраобавештајне (обавештајне) послове како у својој агенцији, тако и у приватним фирмама (Johnson, 2007b).

Служба безбедности у РФ која се бави првенствено контраобавештајним активностима, Федерална служба безбедности, одговорна је за „борбу против тероризма, екстремизма и етнички заснованих организованих криминалних активности. Међутим, важно је нагласити да она спроводи и контраобавештајне активности у министарствима здравља, културе и просвете, у верској сфери и у некомерцијалним организацијама" (Riehle, 2022, p. 70). Неопходно је донети један од битних закључака, да и службе безбедности великих сила Запада и Истока наглашавају присуство контраобавештајне службе и обављање контраобавештајне активности не само у државним фирмама, организацијама, већ и у цивилним, односно некомерцијалним организацијама и разним компанијама.

Занат контраобавештајне активности знатно је еволуирао до данас и можемо слободно рећи до тачке у којој чак и мало озбиљније корпорације не могу без примене овог заната (ове активности више нису само привилегија државних структура). Чланови корпоративног одбора се ослањају на обавештајне и контраобавештајне целине у корпорацијама, како би им боље помогли у предвиђању спољашњег окружења. Савршена организација корпоративне безбедности не постоји, али усклађивање потреба корпорације са контраобавештајним захтевима пружа проактивну безбедност корпорације која доноси одређене погодности као што су побољшана средства управљања знањем, обавештајни резултати, рано упозорење на претње конкуренције, ефикасан рад са људским изворима, способности захваљујући проактивном безбедносном образовању, поуздани интерни извор вести и трендова у вези са спољним окружењем, побољшана оперативна комуникација у вези са безбедношћу унутар организације, побољшана корпоративна безбедносна култура између запослених (Ivanov, 2017).

У деценијама иза нас, можемо констатовати да обавештајна и контраобавештајна активност све више нису привилегија само државних структура, већ најчешће у облику корпоративне безбедности, односно пословне обавештајно – контраобавештајне активности (енг. *competitive intelligence*) налазе велику примену и у приватном сектору где представљају долазак до података и сазнања у вези пословног окружења где орбитира фирма са својим пословањем, као и оним што може да угрози њено пословање, запослене, активности фирме, а уколико се предузму мере од пословног руководства фирме у складу са информацијама које су настале услед доступних података битних за корпоративну безбедност једне фирме, може се очекивати остварење предности у пословању фирме или олакшати доношење одређене одлуке, као и превентивно деловати услед регистрованих претњи.

Пандемија је поред економских последица довела до глобалне трговине, али једног новог облика, непоштене трке и борбе, служењем свим средствима, почев од *кофера пуних новца* код *агената* служби безбедности који по читавом свету купују медицинску опрему за заштиту од вируса, па до понашања држава *свако за себе*, нема *заједничког размишљања и*

деловања (Марјановић и Мићовић, 2022). Економија се пре или касније опорави, али неће се вратити изгубљени животи, нарушено здравље грађана, где ретко ко уопште сагледава посредне ефекте које изазива епидемија, односно пандемија (немогућност одласка на редовне терапије пацијената, запостављање редовне бриге о угроженом здрављу радника у корпорацијама које нису директно проузроковане епидемијом већ немогућношћу коришћења потребних терапија или услуга за лечење и слично). Све ово је током кризе и фокуса на пандемији стављено у други ред, а управо су ти секундарни ефекти стварали много веће последице (Марјановић и Мићовић, 2022). Кризе које се не могу спречити морамо научити да препознамо на време (уз научна истраживања и утемељеност), као што морамо бити оспособљени за хитно и правилно реаговање (када се догоде), а дугорочно стварати отпорна друштва (док их нема). Стварањем могућих процена и сценарија, кризе могу бити препознате правовремено са предвиђеним средствима за супротстављање у првој фази и другим мерама предвиђеним за умањење деловања нежељених дејстава потенцијалних кризних ситуација (Марјановић и Мићовић, 2022).

4.2.3. Необавештајна активност

Временом су многе државе, борећи се против конкуренције, имале оружане сукобе, али и све више коришћен утицај (присиле) на друге државе ради остварења сопствених националних, државних интереса. Еволуција овог утицаја је највише дошла до изражаја у политичком и научном свету приликом хладног рата, када су две велике силе, САД (представник Запада) и Совјетски Савез (представник Истока), поларизовале свет. Резултат те еволуције је појава различите терминологије која описује сличне или идентичне типове, врсте стратешког утицаја (присиле) једне државе на другу, преко служби безбедности, где је један од назива тих активности, *тајне акције*, највише коришћен у Западној терминологији (САД), а термин *активне мере* употребљаван на Истоку (РФ), док је у Републици Србији термин који углавном обухвата све наведено – *необавештајне активности* служби безбедности.

У англосаксонској обавештајној теорији поред термина *тајне акције*, у употреби су и називи *тајне операције* (енг. *covert operations*) и *специјалне активности* (енг. *special activities*), али се најчешће користи термин *тајне акције* (Harder, 2017). У Великој Британији за *тајне акције* се користио назив *тајне политичке акције* (енг. *secret political actions*) као врста активности коју примењују службе безбедности, а која има за циљ да испољи утицај на политичке, војне или економске услове у некој држави или више држава када дипломатија и друге мере политике не успевају. У државама са више служби безбедности обично спољне обавештајне службе учествују у оваквим активностима (Harder, 2017).

Термин који се користи у САД – тајна акција, а британски термин је посебна политичка акција, представља покушај владе државе или неке групе да утиче на догађаје у другој држави или територији без откривања сопствене умешаности (Godson, 1995). Тајна акција или прикривена акција је амерички термин који је у употреби у периоду после Другог светског рата (Godson, 1995).

На савезном нивоу у САД, тајна акција је одређена као „активност или активности Владе САД у циљу испољавања утицаја на политичке, економске или војне услове у иностранству, али са намером да улога Владе САД неће бити очигледна или јавно призната. Тајне акције не укључују активности чија је примарна сврха стицање обавештајних података,

традиционалне контраобавештајне активности, традиционалне активности за побољшање или одржавање програма оперативне безбедности Владе САД или административне активности" (50 U.S.C. 3001, 2022, p. 90). Без обзира на горе наведено, званичном одређењу тајне акције у највишем нормативу САД (што је низ других подзаконских аката углавном преписивао, прим. аут.), пракса је ипак показала да је овај елемент јавног признања постао дискутабилан у појмовном одређењу, јер више се не чека по 50 година да би се одређени класификовани – поверљиви подаци уступали јавности, већ су ради безбедносних процена (првенствено испољавања још једног новог притиска, остваривања још једног циља поред већ реализоване тајне акције, на одређену државу, организацију, групу, ентитет, појединца) у актуелним догађајима званичници САД чак и јавно признавали одређена учешћа у тајним акцијама, чак и она са смртним исходима највиших државника других земаља.

Законодавним одређењем појма *тајна акција – операција* у САД, намерно је избегнуто прописивање истражних радњи које треба размотрити у *тајним операцијама*. Дефинисање овог појма негацијом, односно набрајајући само оне радње и поступке служби безбедности које не обухватају, односно које нису *тајне операције*, даје велики спектар могућности и „маште" планера акција и операција у погледу тога шта је то што је национални, државни интерес и што могу да предузимају као одређену радњу. У својој држави, на овакав начин је легализован сваки поступак сходно овој директиви. Оваквим уређењем је на дужи временски период регулисана оваква активност. Знајући да службе безбедности делују тајним методама рада и да имају изузетно широк спектар задатака са којима се суочавају, а који су им додељени од стране државе, овако „флексибилан" приступ одређењу појма *тајних акција – операција*, омогућава државницима САД да доделе истраживање или извршење било каквих радњи за које је држава заинтересована (Юрьевич, 2014).

Необавештајна (субверзивна) активност обухвата радње и поступке служби безбедности (и других ангажованих чинилаца у држави и иностранству) којима се дестабилизује страна држава и може довести до промене уређења државе, утицаја на друштвено – политички поредак, или испољити други утицај – присила на владу, фирму, организацију, лице. Службе безбедности се током реализације необавештајних активности често ослањају на одане појединце, групе унутар државе која се напада, помоћу којих се други доводе у заблуду и представљају се у наступу као унутрашње, а не спољашње активности (Мијалковић, 2011). Необавештајне активности су веома разнолике, врло често садрже деструктивне психолошко – пропагандне облике деловања, атентате, отмице, диверзије, саботаже, терористичке акте, субверзивне шпијунаже, изазивање и управљање кризама, подршку политичким истомишљеницима у другим државама, свргавање *непослушних* режима или политичких струја које нису истомишљеници, односно разним насилним активностима и акцијама које дају повод за војну интервенцију и довођење до економске зависности читаве нације. Као и у свим активностима службе безбедности, тако и у необавештајним активностима, исте ће бити стално прилагођаване захтевима и задацима политичког руководства једне државе, мењане и прилагођаване новонасталим потребама решавања задатака добијених од државног руководства (Мијалковић, 2011).

4.2.3.1. Генеза необавештајне активности у САД

Кључни документи у вези са тајним акцијама и обавештајним активностима. На основу докумената са којих је скинута тајност, могу се сагледати промене и развојне процедуре током периода док су председници САД били: Труман, Ајзенхауер, Кенеди, Џонсон, Никсон и Форд. У децембру 1947. године, Савет за националну безбедност је издао низ поверљивих директива које су детаљније одредиле и проширile тајну мисију америчке Централне обавештајне агенције. Забринутост Труманове администрације због совјетских „психолошких ратова" подстакла је нови Савет за националну безбедност да овласти, директивом (енг. *National Security Council 4–A*) из децембра 1947. године, покретање мирнодопске тајне акције тј. операције. Овим документом (енг. *National Security Council 4–A*) је поставио директора Централне обавештајне службе одговорним за психолошки рат, успостављајући истовремено и принцип да је тајна акција била искључиво функција извршне власти. С обзиром на то да је Централна обавештајна агенција располагала са средствима која није морала правдати у Вашингтону, ово је био логичан избор службе која ће бити задужена за то (National Security Council 4–A, 1947).

Каснија директива (енг. *National Security Council 10/2*), донешена је дана 18. јуна 1948. године и она је заменила претходну (енг. *National Security Council 4–A*). У овом документу (енг. *National Security Council 10/2*) је прописано да ангажовање Централне обавештајне агенције мора да буде *тајно*, али не само по питањима *психолошких* операција, него их сада дефинишући као све активности које ова влада спроводи или спонзорише против непријатељских страних држава или група или у подршци пријатељским страним државама или групама, али који су тако планирани и извршени да свака одговорност Владе САД за њих није евидентна неовлашћеним лицима и да, ако се открије, Влада САД може уверљиво да се одрекне било какве одговорности за њих (National Security Council 10/2, 1948). Врсте тајних активности набројаних[29] у новој директиви су укључивале: *пропаганду; економски рат; превентивно директно деловање, укључујући мере саботаже, рушења и евакуације; субверзија против непријатељских држава, укључујући помоћ подземном отпору, покретима, герилским и избегличким ослободилачким групама и подршку аутохтоних антикомунистичких елемената у угроженим земљама слободног света*. Такве операције не би требало да укључују оружани сукоб од стране признатих војних снага, шпијунаже, контрашпијунаже и прикривања и обмане за војне операције (National Security Council 10/2, 1948). Начин оваквог (широким спектром одобрених активности за службе безбедности) прописивања необавештајних активности у САД је држави омогућио да у будућности реагује на озбиљну, непредвиђену претњу националној безбедности држави, тајним средствима. Тајна акција мора бити у складу са националном политиком и мора бити подржана, на одговарајући начин стављена у оквир политике националне безбедности. Веома је битно

[29] У 5. тачки директиве (енг. *National Security Council 10/2*) из 1948. године, за необавештајне активности је употребљен термин *тајне операције* које подразумевају све активности које спроводи или спонзорише ова Влада против непријатељских страних држава или група или у подршци пријатељским страним државама или групама, али које су тако планиране и извршене да било каква одговорност Владе САД за њих није очигледна неовлашћеним лицима и ако се открије, Влада САД може веродостојно да се одрекне било какве одговорности за њих. У овој директиви и наведеној тачки 5 је, можемо слободно рећи, први пут на највишем државном нивоу у САД јавно извршена класификација тајних акција, односно тајних операција, односно необавештајних активности (National Security Council 10/2, 1948).

схватити суштину тајне акције и то да она никада не сме да се користи као замена за политику. Врло често се мешају тајне мисије и тајне акције. Наиме, тајност код мисија се односи на чување података о планираној и спроведеној операцији, тактичку тајност саме операције, док се тајност у реализацији тајне акције односи на прикривање, држање у тајности стварних спонзора планиране, реализоване тајне акције. Ове и сличне тајне акције могу укључивати широк спектар активности и то почев од пропаганде и дезинформација до операција политичког утицаја, затим економске дестабилизације, као и паравојних операција (Reagan, 2014). Историјски посматрано, Централна обавештајна агенција је била носилац тајних акција за САД (Reagan, 2014).

У октобру 1951. године издата је директива (енг. *National Security Council 10/5*), поново је потврђен мандат тајне акције дат у директиви (енг. *National Security Council 10/2*) и проширен за делокруг ангажовања Централне обавештајне агенције над герилским ратовањем (*паравојно ангажовање – активности*). Проширење надлежности тајној акцији (операцији) у директиви (енг. *National Security Council 10/5*) помогло је да се обезбеди даља употреба тајне акције која би била ексклузивитет и једна од главних функција Централне обавештајне агенције (National Security Council 10/5, 1951). Неопходно је нагласити да поред Централне обавештајне агенције, реализација тајне акције може бити додељена и другој служби безбедности, али само ако то налажу специфичне околности њене реализације.

Ајзенхауерова администрација је почела да смањује надлежности Централне обавештајне агенције 1954. године, у складу са низом директива Савета за националну безбедност, где је прецизирана одговорност директора Централне обавештајне агенције за даље извођење тајних операција. Тако је председник Ајзенхауер одобрио директиву (енг. *National Security Council 5412*) 15. марта 1954. године, поново потврдивши одговорност Централне обавештајне агенције за спровођење тајних акција у иностранству. Државни секретар, секретар за одбрану и председник морају бити унапред обавештени о великим програмима тајних акција које је покренула Централна обавештајна агенција. Било је неопходно дати одобрење политике за такве програме и квалитетну координацију подршке међу одељењима укљученим у активности, сегментима одбране и Централне обавештајне агенције (National Security Council 5412, 1954).

Годину дана касније, 12. марта 1955. године, издата је директива (енг. *National Security Council 5412/1*), идентична као (енг. *National Security Council 5412*) осим што је одређена Група за координацију планирања као органа задуженог за координацију тајних операција (National Security Council 5412/1, 1955). Овде региструјемо предузимање мера на регулисању адекватне координације у планирању тајних операција служби безбедности. Морамо нагласити да је ово изузетно битан документ, јер један од најпроблематичнијих сегмената у реализацији било које врсте операције представља сегмент координације који, уколико није предвиђен и спроведен у дело како треба, може угрозити операцију и лица која је релаизују.

Директивом (енг. *National Security Council 5412/2*) од 28. децембра 1955. године формирана је група која је постала позната као *National Security Council 5412 – Специјална група* или једноставно *Специјална група*. Ова група је прегледала и одобравала покренуте програме тајних акција од стране Централне обавештајне агенције. Састав Специјалне групе коју су чинили извршни органи власти, варирао је у зависности од ситуације са којом се суочава. Састанци су били ретки до 1959. године, када су почели да се одржавају на

недељном нивоу. Никада нису постојали неки прописани критеријуми за изношење пројеката пред групу, већ је ту иницијативу давала Централна обавештајна агенција (National Security Council 5412/2, 1955).

Специјална група 5412 је 2. јуна 1964. године променила назив у Комитет 303. Ова промена ни на који начин није мењала састав, функцију или одговорност Специјалне групе 5412 како је овлашћена са директивом (енг. *National Security Council 5412/2*), од 28. децембра 1955. године (National Security Action Memorandum No. 303, 1964). У финалном извештају[30] Чурчовог комитета у САД, констатовано је између осталог, да специјална група и Комитет 303 су одобрили 163 тајне акције за време Кенедијеве администрације и 142 за време Џонсонове администрације до фебруара 1967. године, као и 104 за време Ајзенхауерове администрације. Све тајне акције које су одобраване од стране Комитета 303, чиниле су укупно нешто више од једне деветине свих акција које су реализоване, док су наводно оне које Комитет 303 није прегледао биле нискоризичне и јефтине операције (Foreign and Military Intelligence, 1976).

Од новембра 1961. до октобра 1962. године карактеристична је и операција *Мунгос* (енг. *Operation Mongoose*), велика тајна акција, програм који је имао за циљ збацивање Кастровог режима на Куби, а који је укључивао паравојне активности, саботажу и политичку пропаганду (енг. *National Security Action Memorandum* No. 124), превенцију и отпор, субверзивну побуну и друге облике индиректне агресије у пријатељским државама. Дана 17. фебруара 1970. године председник Никсон је потписао Одлуку о националној безбедности Меморандум 40 (енг. *National Security Decision Memorandum 40*), који је заменио директиву (енг. *National Security Council 5412/2*) и променио назив групе за одобравање тајних акција у Комитет 40. Неопходно је да Централна обавештајна агенција прибави одобрење Комитета 40 за све велике и *политички осетљиве* тајне операције (National Security Decision Memorandum 40, 1970). Према Завршном извештају рада *Црквеног комитета*[31] (енг. *Church committee*) из 1976. године, Комитет 40 је разматрао само око једне четвртине појединачних тајних акција Централне обавештајне агенције и то тежишно великих пројеката који су обезбедили широке смернице политике за све тајне акције. Нису чак ни све веће операције изведене пред Комитет 40: председник Никсон 1970. године је упутио директору Централне обавештајне агенције задатак да промовише државни удар против чилеанског председника Салвадора Аљендеа без координације или одобрења Комитета (Foreign and Military Intelligence, 1976).

Историјски гледано, необавештајне активности, од инвазије у Заливу свиња (енг. *Bay of pigs*), Куба, до употребе беспилотних летелица у глобалном рату против тероризма су за Централну обавештајну агенцију створиле више проблема него прикупљање обавештајних

---

[30] С обзиром да се ради о тајним активностима државе и служби безбедности, неопходно је нагласити да је у Бостонској библиотеци овај извештај јавно објављен тек 1. јануара 2014. године (38 година касније од званичне објаве конгресу САД).

[31] *Church committee*, енг. назив је добио према сенатору из Ајдаха Френк Чурчу (*Frank Church*) који је председавао комитетом, где је комитет, одбор формиран ради сазнања да је америчка Централна обавештајна агенција вршила прислушкивање својих грађана ради прикупљања података о политичким активностима америчких грађана и ради припрема и вршења атентата. Тако је председник САД донео Извршну наредбу (енг. *Executive order 11905*) 18. фебруара 1976. године и овом извршном наредбом је забрањено бављење оваквим и сличним активностима свим запосленима у влади САД (Foreign and Military Intelligence, 1976).

података. Након скандала Вотергејт[32] и низа новинских чланака о активностима Централне обавештајне агенције, како америчког Сената, тако и америчког Представничког дома, формирани су комитети за истрагу активности Централне обавештајне агенције. Најистакнутији од одбора био је сенатски одбор којим је председавао сенатор Франк Чурч (*Frank Church*) из Ајдаха. Овај одбор је истраживао такве наводе као што је умешаност Централне обавештајне агенције у покушај атентата на стране лидере, укључујући Фидела Кастра, председника. Под притиском Конгреса да постави смернице за активности овог типа, председник Гералд Форд (*Gerald Ford*) одлучио је да изда Извршно наређење 11905, које је потом замењено Извршним наређењем 12333 које је издао председник Роналд Реган 1981. године, где је једно од најбитнијих ограничења необавештајних активности у Извршном наређењу 12333 било регулисано у енг. „*PART 2 Conduct of Intelligence Activities, 2.11.*" на следећи начин: „Забрана атентата. Ниједно лице запослено у Влади САД или делује у њено име неће се укључити у заверу или извршити заверу за извршење атентата" (Goldman, 2016, p. 228, 229). Међутим, сведоци смо тога да ескалација примене необавештајних активности достиже врхунац у XXI веку, јер и поред овог наређења, у јануару 2020. године је дроном убијен Касим Сулејмани где је председник САД, Доналд Трамп, врло брзо у медијима, више пута, званично признао убиство овог иранског генерала, сматраног за најбитнијег појединачног оперативца на Блиском истоку, уз образложење да је убијен да би био спречен рат, а не да би га започели.

У Извршном наређењу 12333 у тачки 1.7 (енг. *Intelligence community elements*), параграф (*a – The Central intelligence agency*), подпараграф (4), наведено је да осим Централне обавештајне агенције, ниједна друга агенција (или Оружаних снага САД у време рата који је прогласио Конгрес или током било ког периода обухваћеног извештајем председника Конгресу у складу са ратним овлашћењима Резолуција, јавни закон 93–148) не може спроводити било коју тајну акцију осим ако председник не утврди да је већа вероватноћа да ће друга агенција постићи одређени циљ. Даље у Извршном наређењу 12333, тачка 2.13 (енг. *Limitation on covert action*) је дефинисано да је тајна акција ограничена, односно „не може се спроводити ниједна тајна акција која има за циљ да утиче на политичке процесе у САД, јавно мњење, политику или медије" (Executive Order 12333, p. 14). У Извршном наређењу 12333, прописано је у тачки 3.5, параграф (б) да тајна акција представља операцију контраобавештајне службе која обухвата активност или активности државе у циљу утицаја на политичке, економске или војне услове у иностранству, где је намера да улога државе неће бити очигледна или јавно призната. *Тајне акције* не укључују активности „чија је примарна сврха стицање обавештајних података, традиционалне контраобавештајне активности, традиционалне активности за побољшање или одржавање оперативне безбедности државе, традиционалне дипломатске или војне активности, традиционално

[32] Афера Вотергејт (неодобрено прислушкивање политичара по налогу председника САД, Ричарда Никсона као и друге нелегалне активности застрашивања, политичке шпијунаже, субверзивних активности и сл. што је довело до оставке председника) је пре била једна од операција служби безбедности САД, што потврђује око 30 година касније обелодањивање ко је био наводно извор података новинарима (мада пре можемо закључити да се ради о коришћењу извора података што су највероватније били новинари, а не да је припадник службе безбедности био извор у овој афери – што је у медијима пласирано као званична верзија, највероватније ради „мира у кући"), а радило се наводно о другом човеку у хијерархији у служби безбедности САД– ФБИ, што не значи да је ова служба реализовала операцију или је овај припадник искоришћен од стране друге службе за реализацију операције.

спровођење закона и активности за спровођење рутинске подршке отвореним активностима" (Executive Order 12333, 2008, p. 15).

Обавештајна директива Савета за националну безбедност број 7 о одговорности америчке Централне обавештајне агенције за развој обавештајних извора у америчким корпорацијама и невладиним организацијама. Директива такође наводи обавезе за Централну обавештајну агенцију према страним службама безбедности и обавезе служби безбедности у САД. Једна од тих обавеза је да се прибаве информације о страним обавештајним подацима које одсеци и агенције су добили као резултат нормалног односа са пословањем корпорација и других невладиних организација и појединаца у САД у вези са необавештајним активностима (National Security Council Intelligence Directive No. 7, 1948).

Хјуз – Рајанов закон, 1974 (енг. *Hughes – Ryan Act 1974*) усвојен је у децембру 1974. године због критике у вези са необавештајним активностима америчке Централне обавештајне агенције у Чилеу. Био је то покушај успостављања неких ограничења у пракси Централне обавештајне агенције, као и побољшања одговорности, посебно уз поштовање председника. Назван је по сенатору Харолду Е. Хјузу из Ајове и представнику Леу Ј. Рајану из Калифорније, који су тражили да председник пријави *необавештајну активност* – необавештајне операције релевантним конгресним одборима, којих је било првобитно три (касније четири) и у Представничком дому и у Сенату (Uram, 2005).

Генерал потпуковник Вилијам Одом (*William E. Odom*), директор службе безбедности у САД – Агенција националне безбедности, када дефинише контраобавештајну активност, између осталог наглашава следеће: „не ради се о подацима о противниковом креирању политике или војним операцијама или другим *необавештајним способностима и активностима*" (Counterintelligence Glossary, 2014, p. 348). Овде директор једне од најбитнијих служби безбедности у САД прави разлику између контраобавештајних, политичких, војних и *необавештајних активности*.

Годсон (*Roy Godson*) такође прави разлику између *тајне акције* и контраобавештајне активности, где је овај последњи термин усмерен на противничке обавештајне оперативце и њихове политичке господаре у поређењу са првим који циља „*необавештајне активности*, играче" (O'Brien, 2007, p. 25). Можемо закључити да је Годсон овде предвидео да се необавештајним активностима, поред обавештајне и контраобавештајне активности, супротставља необавештајним активностима матичне државе.

Необавештајна активност дефинисана је у енг. *Title 50 U.S. Code, § 3093*. као активност или активности Владе САД да утиче на политичке, економске или војне услове у иностранству, са намером да улога САД неће бити очигледна или јавно призната (Title 50 U.S. Code, § 3093, 2014). Необавештајна активност не укључује: активности са примарном сврхом прибављања обавештајних података, традиционалне контраобавештајне активности, традиционалне активности за побољшање или одржавање оперативне безбедности владиних програма САД или административне активности; затим традиционалне дипломатске или војне активности или рутинску подршку таквим активностима; традиционалне активности спровођења закона које реализују агенције за спровођење закона Владе САД или рутинска подршка таквим активностима; активности за пружање рутинске подршке било којим другим отвореним активностима других државних агенција САД у иностранству (Title 50 U.S. Code, § 3093, 2014). Историјски примери необавештајне активности укључују организацију пуча 1953. године у Ирану од стране Централне обавештајне агенције; затим Залив свиња –

инвазија на Кубу 1961. године (као резултат неуспеха, директор, заменик директора и помоћник директора операција ове агенције су приморани да поднесу оставке); тајни рат из Вијетнама у Лаосу; и подршка пољском синдикату солидарности током 1970–их и 1980–их и муџахединима у Авганистану током 1980–их и др. (Krishnan, 2018).

Јасна је потреба за проналажењем *необавештајне активности* у оквиру студије о међународним односима уопште и посебно у оквиру служби безбедности. Од 11. септембра политички контекст, како национални тако и међународни, промењен је. Усред распрострањених позива на реформу служби безбедности у САД постоје они који се залажу за радикалну нову концептуализацију улоге података добијених од служби безбедности у политици националне безбедности. Бивши виши официри америчке Централне обавештајне агенције, између осталог, заговарају промену оријентације америчке обавештајне службе од прикупљања информација до лова на противнике САД (Scott & Jackson, 2004). Позивајући се на Извршно наређење 12333 Председника САД, одређено је значење термина *тајна акција* што означава активност или активности Владе САД да утиче на политичке, економске или војне услове у иностранству, где се намерава да улога Владе САД неће бити очигледна или јавно призната, али те активности не укључују (1) активности чија је основна сврха стицање обавештајних података, традиционалних контраобавештајних активности, традиционалних активности за побољшање или одржавање оперативне безбедности програма Владе САД или административних активности, (2) традиционалне дипломатске или војне активности или рутинску подршку таквим активностима, (3) традиционалне активности спровођења закона које спроводе агенције за спровођење закона Владе САД или рутинска подршка таквим активностима или (4) активности које пружају рутинску подршку отвореним активностима других владиних агенција САД у иностранству (Mccurdy, 1991). Сличан термин *тајне акције* дефинисан као активност Владе САД да утичу на политичке, економске или војне услове у иностранству, са намером да улога САД неће бити очигледна или јавно призната егзистира и данас (Cumming, 2006). У америчкој литератури назив *тајне акције* настао је непосредно после Другог светског рата и везује се за тзв. *Бизелову доктрину* (Ричард Бизел, руководилац у Централној обавештајној агенцији) према којој *тајне акције* представљају покушаје мешања у унутрашње ствари других држава средствима закулисних игара (Marchetti & Marks, 1983). Тајне операције треба, у неке сврхе, поделити у две класификације: обавештајна и контраобавештајна колекција, најпре шпијунажа или прибављање података обавештајних и контраобавештајних, прикривеним средствима и необавештајне активности, покушавајући да утичу на унутрашње афере других нација – које се понекад називају *интервенцијом* прикривеним средствима. Иако се ове две категорије активности могу раздвојити у теорији, пракса је показала да је то катастрофално решење, интеракција прикупљања обавештајних података и необавештајне активности. Један од таквих покушаја био је „оснивање Канцеларије за координацију политике – ОПЦ (енг. *Office of policy coordination*) у раним данима Централне обавештајне агенције (1948) као засебног органа за реализацију необавештајних активности. Иако је Централна обавештајна агенција подржала и дала покриће, ова организација је била независна, али врло брзо је стопљена са тајном обавештајном организацијом у начин на који је у оквиру тамошњих комбинованих тајних служби била потпуна интеграција прикупљања обавештајних података и функције тајне акције у свакој подели подручја" (Marchetti & Marks, 1983, p. 329). Главни проблем је то што необавештајне активности често стварају више проблема него што их решавају. Дакле,

трошкови обелодањивања и срамота се морају пажљиво проценити и тамо где су политички трошкови значајни, необавештајне активности би највише требало да покрећу само демократије са убедљивим разлозима, тј. када је безбедност државе директно угрожена, када се може показати да државни систем не ради и када потенцијални штетни ефекти акција не надмашују могуће користи (Geneva Centre For The Democratic Control Of Armed Forces, 2003). Хрватски аутор Биланџић (*Mirko Bilandžić*) под појмом *тајне акције* подразумева покушаје владе да утиче на догађаје у другим државама или територијима без откривања своје умешаности (Bilandžić, 2005). Биланџић такође износи да се анализом инструмената спољне политике долази до закључка да су необавештајне активности, активност између дипломатских и војних средстава и да се предузимају када дипломатска акција више није делотворна. Једна од битних одлика необавештајне активности је да њен иницијатор може „уверљиво негирати" своју укљученост, а у случају евентуалне компромитације (Bilandžić, 2005).

Министарство одбране САД је прописало Доктрину подршке обавештајне заједнице Министарству одбране у операцијама 2–01 (енг. *Joint Publication 2–01*) 2017. године у којој су дефинисани основни појмови, обавезе и задаци учесника у подршци Министарству одбране у реализацији одређених операција и обратно. Тако *операције* служби безбедности обухватају разноликост обавештајних и/или контраобавештајних активности које спроводе различите службе безбедности у оквиру обавештајног – контраобавештајног процеса. Обавештајни – контраобавештајни *процес* представља „процес којим се подаци претварају у информацију (крајњи обавештајни – контраобавештајни податак) и ставља на располагање корисницима, а који се састоји од шест међусобно повезаних активности и то: планирање и усмеравање; прикупљање, обрада и експлоатација; анализа и производња; ширење и интеграција; и евалуација и повратне информације. Обавештајни – контраобавештајни *систем* представља било који формални или неформални систем за управљање прикупљањем података, добијањем и обрадом података, интерпретирањем података и образлагањем закључака доносиоцима одлука као основе за одређено поступање" (Joint Publication 2–01, 2017, p. 214, 215).

Да је могуће супротставити се *сивој зони* и делом конвенционалних снага констатовано је у следећем. Истраживање је сагледало ове могућности кроз пешадијску бригаду[33] оружаних снага САД. Пример конвенционалних сила које омогућавају супротстављање непријатељским мерама РФ сагледане су кроз могућности пешадијске бригаде, њене капацитете као и додатне могућности које се могу користити из виших нивоа хијерархије (означено са * где постоје и снаге, капацитети, могућности које се могу очекивати у подршци и користити из вишег ранга, хијерархијског од нивоа бригаде у оружаним снагама САД). „Тимови за прикупљање људских обавештајних података као и (*) Тимови за прикупљање људских обавештајних података. Тимови за прикупљање контраобавештајних података као и (*) Тимови за прикупљање контраобавештајних података. Мали беспилотни ваздушни системи кратког домета[34] и ограничену обраду,

[33] *U.S. Army infantry brigade combat team,* енг. – оружане копнене снаге САД пешадијска бригада, борбени тим. Сваки војни борбени тим, ове врсте састоји се од три маневарска батаљона, ватрене подршке – батаљона, извиђачког одреда, батаљона за подршку бригаде и батаљона специјалних снага бригаде.
[34] *Unmanned aerial system,* енг. – беспилотни ваздушни систем.

експлоатацију и ширење обавештајне информације. Већа средства, беспилотни ваздушни системи већег домета и напредна обрада, експлоатација и ширење обавештајне информације. Даљински сензори тла и тимови за надгледање (*) Тимови даљинских сензора тла. Прикупљање обавештајних података о сигналима кратког домета. Напредно прикупљање обавештајних података дужег домета. Вод за анализу обавештајних података Бригаде за позадину за обавештајну анализу. Вод војне полиције, Батаљони војне полиције, Радари за земаљско осматрање (*) Радарски тимови за земаљски надзор. Класификоване и некласификоване радио и мреже података Напредне командне и контролне могућности. Информационе операције војне подршке[35] тимови Стратешке комуникационе способности. Одељење за односе са јавношћу са могућношћу повратног контакта, потпуно интегрисани медијски тимови. Стручњаци за безбедност информација, Тимови за сајбер – електромагнетне активности. Јединице хемијске, биолошке и радиолошке одбране (*) Хемијска, биолошка, радиолошка одбрана. Пешадијске борбене и ватрене јединице, оклоп, авијација, ватре на великом домету и здружени утицаји" (Connable et al., 2020, p. 66).

4.2.3.2. Одређење необавештајне активности у Руској Федерацији

Појам „необавештајне активности" (*активне мере*) наведен у Речнику контраобавештајне службе који је издао Комитет државне безбедности је следећи: дела контраобавештајне службе која омогућавају продирање у намере непријатеља, дозвољавајући предвиђање његових нежељених корака, да води непријатеља грешком, да од њега преузме иницијативу, да осујети његове диверзантске акције. *Активне мере* су омогућавале откривање и спречавање непријатељских активности у раним фазама, приморавајући противника да се изложи, намећући му вољу да делује, присиљавајући га да делује неповољним условима и на начине које желе контраобавештајне службе. У пракси, *активне мере* укључују пројекте који имају за циљ изградњу положаја шпијуна у табору непријатеља и околине, дириговање оперативне игре са непријатељем, дезинформације упућене на њега, компромис и деморализацију, прелазак на територију Савеза Совјетских Социјалистичких Република лица од посебне оперативне вредности, прибављање обавештајних података, итд. Под *активним мерама* служби безбедности у бившем Совјетском Савезу су се подразумевале активности којима се настојао извршити утицај на збивања, политичке ставове и јавно мњење у некомунистичким и другим државама, применом обмањивачких и прикривених метода. Све необавештајне активности имале су заједнички циљ да, нарушавајући углед противника, појачају утицај Совјетског Савеза на међународном плану (Darczewska & Zochowski, 2017). *Активне мере* обухватале су различите акције, од манипулације медијима до специјалних операција. Под *активним мерама* се у совјетској литератури подразумевала примена различитих политичких и паравојних техника ради остваривања утицаја на појединце или акције страних влада (Darczewska & Zochowski, 2017).

Када говоримо о активностима обухваћеним термином *активне мере*, а које се подразумевају у Западном говорном подручју, тада се мисли првенствено на операције утицаја, прикривене субверзије, манипулације информацијама и ангажовање плаћених агената од утицаја. Важно је нагласити да вековима имају главну компоненту у државном

[35] *Military information support operations*, енг. – информационе операције војне подршке.

управљању. Како би се остварио значајнији ефекат, често се врши обједињавање, односно групно деловање са продором агената, провокатора у непријатељске групе и ангажовање да повремено чине акте насиља. С обзиром на то да помињемо термин „вековима", то поткрепљујемо чињеницом да је још од времена *Царске тајне полиције* (*Окхрана*) примењиван читав низ активних мера да би се маргинализовале или победиле домаће дисидентске групе као што је нихилистичка Народна воља, са жељом да руска монархија буде збачена са власти, док је у иностранству Окхрана вршила надзор и продоре у емигрантске дисидентске организације у Француској. Успевало им је понекад да намаме вође дисидената назад у Русију, где би најчешће били убијени. Оперативци Окхране су такође ангажовали култивисане агенте од утицаја у европској штампи како би помогли у управљању перцепцијом царске Русије. Окхрана је успешно саботирала сваки антицарски политички покрет у Европи осим једног, покрета бољшевика. Вођа прве совјетске тајне полицијске организације, Феликс Џержински, применио је сва ова искуства према противницима комунизма (Schoen & Lamb, 2012).

Када се методе које су раније употребљаване од стране служби безбедности (*активне мере*) упореде са садашњим операцијама, онда мора бити закључено да у ствари постоји ефикасан хијерархијски систем менаџмента који координира фабриковање и дистрибуцију лажних вести и омогућава да се исте шире. Када не би било оваквог начина управљања система, било би немогуће постићи висок ниво кохезије између активних мера, односно креирања политике, употребе војске и примена дипломатије. Наведено обухвата координацију и замагљивање догађаја, као што је било све везано за Крим, и активности РФ у источној Украјини. Уколико је настављен совјетски модел командовања – руковођења и исти опстао као шаблон, онда су службу безбедности, Комитет државне безбедности, замениле следеће службе безбедности: Федерална служба безбедности, Спољна обавештајна служба и Главна обавештајна управа (Главна управа), које су поделиле своје активности према њима прописаним надлежностима (Fedchenko, 2016).

Активне мере су активности које се разликују од обавештајних и контраобавештајних активности. Такве активности укључују напоре да се врши контрола над и манипулише страним медијима, *дезинформацијама и обманама*, као и активности политичког утицаја. Када се говори о обавештајним подацима у модерној ери, мисли се углавном на прикупљање и анализу података – шпијунажу, сајбер истрагу, сателите и аналитичку подршку креаторима политике, док службе безбедности настоје да стекну увид и украду тајне, далеко већи нагласак стављајући на субверзију и политичку акцију (Sipher, 2018).

Још од бољшевичке револуције 1917. године, први задатак служби безбедности био је да руководство чврсто држи на власти. Саботаже, поремећаји, активне мере и атентати су кључне централне поставке функционисања државе. Такве мере су дизајниране да убеде потенцијалне унутрашње непријатеље да су политичке промене немогуће. У опису Института *Хенри Џексон* стоји да „Кремљ користи руске информативне операције и као увод у рат, а и као алтернативу рату и као слушкињу у рату" (Sipher, 2018, p. 2).

Примена необавештајних активности од стране служби безбедности у Савезу Совјетских Социјалистичких Република названа је *активним мерама*, али не искључујемо могућност да је овај термин који је коришћен у доба хладног рата „у постхладноратовском периоду променио назив у *мероприятия содействия* (рус.), *measures of support* (енг.), на српском језику *мере подршке*" (Riehle, 2022, p. 86). Када кажемо да не искључујемо

могућност, морамо да нагласимо у овом делу истраживања да се ради о материји (методологији рада служби безбедности) која је у свим државама на планети одређена као област у којој су скоро сви подаци у вези рада служби безбедности одређени као тајни подаци са високим степеном тајности, најчешће строго поверљиво или државна тајна, па наглашавамо да је ово истраживање базирано искључиво и само на сазнањима из јавно доступних извора.

4.3. СПРЕГА ДИПЛОМАТИЈЕ И СЛУЖБИ БЕЗБЕДНОСТИ

4.3.1. Теоријско одређење дипломатије

Дипломатија као делатност, стара је колико и држава, мада је и пре настанка државе у комуникацији између племена било преговарања, развијања односа и посматрања и обавештавања. Према томе, дипломатија је стара колико и политика, а за обе је карактеристично мноштво дефиниција, различитих појмовних одређења и схватања (Марјановић, 2015). Наравно, као делатност и инструмент креирања и спровођења државне политике у свеукупним односима са другим државама и субјектима, укључујући и војне односе, дипломатија је ужи појам од политике (Марјановић, 2015).

Први трагови дипломатских знања и умећа налазе се у цивилизацијама старог Истока, концентрисани у рукама тадашњих владара. Они су се договарали да заједнички ратују против трећег, а после о подели плена (Марјановић, 2015). Већ тада су склапани споразуми о ненападању и узајамној помоћи. Дипломатија је и тада била вештина којом се постиже циљ и решава проблем, а сила је била у другом плану. Тако су развијани и први облици дипломатског апарата (Марјановић, 2015).

Наводећи низ дефиниција појма дипломатија од познатих аутора, Миодраг Митић за дипломатију каже да је она: „уметност преговарања и остваривања међународних односа; вештина која се стиче обуком и радом; професија са специфичним карактером посла, начином рада и сопственим правилима и научна дисциплина, односно наука” (Митић, 1999, стр. 8).

Дакле, дипломатија представља комплексан састав сачињен од великог броја вештина, институционалних и ванинституционалних међународних односа, који се, за разлику од традиционалне дипломатије, не ограничавају на формалне контакте између представника влада различитих држава (Зечевић, 1990). Дипломатија са својом основном функцијом – представљањем своје државе у иностранству и промовисањем њених интереса и циљева, једна је од најбитнијих активности државе изван њених граница. Она је задужена да као „инструмент спроводи спољну политику коју утврђују тела државне власти (председник, влада, парламент или друга уставом одређена тела), а путем њих група која држи власт у својим рукама” (Зечевић, 1990, стр. 11).

4.3.2. Активности служби безбедности и дипломатије, сличности и разлике

Основна функција дипломатије је представљање своје државе у иностранству и промовисање њених интереса и циљева. Она је задужена да као инструмент спроводи спољну политику коју утврђују тела државне власти (Марјановић, 2015). Спровођење спољне политике и одржавање међународних односа с другим субјектима (државама, међународним организацијама и сл.) подразумева и развој специфичних метода (између

осталог ту спада и дипломатски протокол) те апарата који ће обављати ту функцију (тзв. служба спољних послова). Једноставно дефинисано, задаци дипломатије су: представљати и заступати, преговарати, штитити и обавештавати своју земљу. Ако се гледа кроз историју, може се рећи да су развој међународних односа, промовисање положаја властите државе и спречавање рата најважније активности дипломатије. Осим традиционалних политичких, у дипломатске активности спадају и економски, културни, научни, војни и други односи. Савремена дипломатија, осим традиционалних задатака, бави се и проблемима људских права, незаконитих миграција, заштите околине, организованог криминала, те учествује у борби против тероризма (Марјановић, 2015). Када политика, односно дипломатија, није у могућности да реализује стратегију одвраћања самим постојањем одређеног оружја или оруђа, тада се између избора за ратни сукоб и немоћи дипломатије укључују службе безбедности које путем политичких, пропагандних, економских, паравојних или других активности врше реализацију националних, државних интереса.

Вилиам Одом (*William E. Odom*), директор Агенције за националну безбедност (енг. *Director National Security Agen*cy), истичући битност служби безбедности у функционисању и раду државе и државних апарата констатује да се учинак служби безбедности једноставно не може одвојити од спољнополитичког и учинка војне операције (Johnson, 2007a). Овом фантастичном одређењу које је дао Одом бисмо само могли придодати поред учинка и присуство службе безбедности. Када кажемо присуство службе безбедности, то подразумева непосредно присуство овлашћеног службеног лица – оперативца службе безбедности или присуство извора података службе безбедности.

Суштина дипломатског инструмента је начин комуницирања са државним или недржавним актерима од стране државе. У последње време, актуелно је да се као актери у преговорима у дипломатији између сукобљених страна све чешће појављују не више велике силе директно, већ државе које би биле тзв. неутрални преговарачи између сукобљених страна (један од таквих примера је и ангажовање дипломатије Републике Србије у преговорима, покушајима помирења талибана и власти у Авганистану, односно једне врсте одвраћања страна у сукобу, које се догодило два пута на територији Републике Србије, према изјавама Ивице Дачића, на телевизијском каналу *PTC1*, у другој недељи августа 2021. године, а да се наведено догодило док је Дачић био на дужности шефа дипломатије, првог дипломате Републике Србије, односно министра спољних послова). На овај начин се сукобљеним странама омогућава да мирно функционишу, а да стратегија одвраћања буде спроведена. Врло битан сегмент је економска акција што је довело до велике међузависности држава. Тако да попут ефекта „црног лептира" може одјекнути неки наизглед најобичнији поремећај у економији једне државе, са једног краја планете, на државе у другом крају.

Информације као инструмент моћи, гледајући са аспекта доласка до њих преко служби безбедности, могу се схватити на више начина. Наведено укључује вредност извора информација, било физичких, когнитивних или виртуелних. Ове изворе можемо посматрати као људе и/или машине. Контрола над овим структурама се може користити за поседовање моћи. Институције које надгледају, осмишљавају, доприносе току информација где у својој понуди имају базе података такође представљају моћне инструменте (Ducheine & Pijpers, 2021).

Свакако свима добро познат начин испољавања спољнополитичког утицаја (делом и јавног карактера) представља ангажовање амбасада у другим земљама. Знајући наведено,

поготово да се у њеним саставима налазе оперативци служби безбедности стране државе, све озбиљне службе безбедности, контраобавештајног карактера, па тако и Федерална служба безбедности, користе следећу меру како би успориле или спречиле рад амбасада. Ради се о методу служби безбедности узнемиравања дипломата, првенствено дипломата САД као и других земаља у РФ, за који постоје сазнања да се драматично повећало од 2014. године. Када се каже узнемиравање, тада се мисли на активности служби безбедности које обухватају координисане активности са другим државним и недржавним субјектима ради ометања рада дипломата, али да се води рачуна да се ипак ради о лицима која најчешће штити дипломатски имунитет и да се избегну колико је то могуће, инциденти међудржавног нивоа. Ради се о следећим активностима: „произвољна" полицијска заустављања дипломата, физички напади, провале у куће и станове где живе дипломате, као и емитовање детаља из њиховог личног, приватног живота на државним телевизијским каналима изазивајући (посредно) друга лица да им науде. Све набројане активности служби безбедности (у овом конкретном случају говоримо о Федералној служби безбедности) руководиоци служби предузимају најчешће из следећих неколико разлога: као један од облика супротстављања или средства за спровођење освете за спроведене контраобавештајне или операције САД усмерене на дипломате РФ, како би извршила идентификацију дипломатски покривених обавештајних службеника, да доведе до реакције која би изазвала одговор који се може користити против САД у пропагандним порукама, мада довољно је и једноставно да створи стрес код дипломатског особља, чиме се већ утиче на њихов рад, односно ограничава се њихова ефикасност. Везано за узнемиравање дипломата у РФ, можемо да закључимо да узнемиравање страних дипломата од стране служби безбедности, односно Федералне службе безбедности, представља контраобавештајни метод рада и необавештајну активност службе безбедности коју планира, организује и у сарадњи са другим органима, институцијама, организацијама или недржавним актерима (ради спровођења необавештајних активности) спроводи служба безбедности под покровитељством Владе РФ са циљем смањивања укупне способности, ефикасности страних операција служби безбедности у РФ (Riehle, 2022).

4.3.3. Значај дипломатије за активности служби безбедности

Тренд међународних односа који данас доминирају у глобалном информационом простору је оштра конфронтација због жеље неких држава (великих сила) да другима наметну своје интересе у решавањима међудржавних проблема. Наведено се чини ради потреба да се оправдају претензије у лидерству. Дужи временски период се против РФ води отворена информациона операција, рат, од стране центара светског информационог утицаја (Тимофеев, 2017, p. 8).

Информативна агенција САД (енг. *United States Information Agency – USIA*), која је радила од 1953. до 1999. године, била је агенција САД посвећена *јавној дипломатији*. Пре реорганизације служби безбедности у САД (1999. године) председник САД јој је доделио културну и обавештајну функцију. Бивши директор телевизијске и филмске службе *УСИА*, Алвин Снајдер, присећа се у својим мемоарима из 1995. године да је Влада САД водила организацију за односе с јавношћу која пружа све услуге, највеће на свету, отприлике величине двадесет највећих америчких комерцијалних компанија за односе са јавношћу, заједно. Ради се о више од 10.000 запослених, распоређених у око 150 земаља широм света, са задатком да улепшавају имиџ САД и уништавају имиџ Савеза Совјетских

Социјалистичких Република (после РФ). Трошкови оваквих активности су прелазили две милијарде долара годишње. Највећи део ове машинерије је чинила пропагандна машина *УСИА* (United States Information Agency, 2022).

Комплетан обавештајни систем Савеза Совјетских Социјалистичких Република, према Александру Орлову, бившем припаднику службе безбедности, био је организован у око осам *оперативних линија* (Riehle, 2022), што је он описао у Приручнику за обавештајно и герилско ратовање из 1963. године (енг. *Alexander Orlov, The Handbook of Intelligence and Guerrilla Warfare, Ann Arbor, University of Michigan Press, 1963*).

Орловљева *прва линија* деловања била је *дипломатска обавештајна служба*, што бисмо данас могли назвати политичком службом безбедности, као и органи који проводе дипломатију, односно Министарство спољних послова. Комитет државне безбедности током Хладног рата и Спољна обавештајна служба данас, политичка служба безбедности је увек била велики напор, а највећи део резидентуре Спољне обавештајне службе чини политичка категорија људских извора.

Инфилтрација служби безбедности страних земаља је *друга линија* деловања. Када говоримо о овој линији тада мислимо на контраобавештајне и обавештајне активности. Док инфилтрација у страну службу безбедности пружа очигледну прилику да се идентификују регрутовани агенти унутар сопствене владе, стране службе безбедности, установе, шифрована средства комуникације, које се могу искористити за даље прикупљање обавештајних података. Улогу инфилтрирања у стране службе безбедности (обавештајног и контраобавештајног карактера) унутар РФ данас обавља Федерална служба безбедности, док је за исту функцију ван РФ надлежна Спољна обавештајна служба.

Индустријску активност службби безбедности, односно економске активности, чине с*ледеће две линије* деловања и оно што је Орлов назвао економски обавештајни подаци – то су подаци који су РФ потребни да би разумели економске полуге које друге земље користе против РФ. Ове линије обухватају напоре за идентификацију стране завере да се нанесе штета економији РФ (има економску контраобавештајну мисију). Данас, ова активност је у надлежности службби безбедности, Спољне обавештајне службе и Федералне службе безбедности. Када данас кажемо Орловљева *индустријска активност*, тада мислимо на научну и технолошку (енг. *Science and Technology*) активност службби безбедности којим настоје да прикупе најновија научна достигнућа страних земаља која РФ може да користи или за подстицање сопственог развоја технологије или за састављање противмера у овој области. Страна војна технологија за подршку војном планирању РФ су одговорност војне службе безбедности, некада Главне обавештајне управе (сада Главне управе), који се посебно фокусира на војну технологију, али и Спољне обавештајне службе.

Када говоримо о Орловљевој *петој линији* деловања, тада мислимо на службу безбедности која се својим оперативним ангажовањем бави доласком до података о претњама са којима ће РФ морати да се бори. Овде спада све од тактичких података о војним јединицама и опреми па до података о стратешким циљевима које би РФ морала да неутралише у неком наредном сукобу или рату, како би изашла из тог сукоба као победник. Приоритет у реализацији ових задатака има војна служба безбедности, некада Главна обавештајна управа (сада Главна управа), али и Спољна обавештајна служба и Федерална служба безбедности такође учествују у прикупљању ових података.

За свако руководство државе, најбитније линије деловања представљају управо Орловљеве последње *три линије* деловања и то дезинформације, утицај на одлуке страних влада, па саботажа и герилски рат. Према Орлову, уместо задатака прикупљања података из надлежности служби безбедности, у овом случају говоримо о задацима политичке природе који су додељени директно од руководства државе служби безбедности РФ на реализацију.

Дезинформације су најзаступљеније, најпознатије од тих задатака захваљујући широко објављеним напорима РФ, од мешања у стране изборе до манипулисања страним истрагама агресивних акција РФ у иностранству. Примена необавештајних активности од стране служби безбедности у Савезу Совјетских Социјалистичких Република названа је *активним мерама*, али према доступним сазнањима овај термин је коришћен у доба хладног рата, па је у постхладноратовском периоду највероватније променио назив у, рус. *мероприятия содействия* (срп. *мере подршке*; енг. *measures of support*).

Утицај на одлуке страних влада може имати форму регрутовања одређене имовине са приступом лицима који се питају у држави за одређене битне одлуке и доносе политичке одлуке како би на одређен, суптилан начин, користећи своју близину, испољили утицај на одлуке у корист РФ.

Још од периода бољшевичке револуције, саботажа и герилски рат су били укључени у активности служби безбедности. На руском језику *разведка* значи „прикупљање података и коришћење тајних операција против непријатељских снага и укључује активности од подршке страним револуцијама до циљања критичне и војне инфраструктуре непријатеља током рата" (Riehle, 2022, p. 86). Можемо да закључимо да су наведене, последње три оперативне линије у директној вези са претходним линијама и њихов рад и ангажовање се базирају на подацима до којих се дошло ангажовањем служби безбедности (прикупиле су у другим линијама) и представљају прикривене и тајне алате које држава може да користи за унапређење својих политичких, војних и економских циљева. Такође, важно је нагласити да у последње три оперативне, Орловљеве линије деловања, препознајемо необавештајне активности служби безбедности.

5. ОДВРАЋАЊЕ НЕОБАВЕШТАЈНИМ АКТИВНОСТИМА СЛУЖБИ БЕЗБЕДНОСТИ

5.1. НЕОБАВЕШТАЈНА АКТИВНОСТ СЛУЖБИ БЕЗБЕДНОСТИ

Први јавни наступ (мада су и до тада службе безбедности, али тајно, већ примењивале необавештајне активности, тајне акције) из којег се могло закључити да ће САД да доживи одређене озбиљне промене у начину тј. методама коришћења спољне политике, односно одвраћања, првенствено у употреби служби безбедности, била је Хуверова комисија 1954. године, где је констатовано да уколико САД жели да преживи, концепт *фер игре* се мора преиспитати; морамо научити да *подмећемо, саботирамо и уништимо* наше непријатеље *паметнијим, софистицираним и ефикаснијим* методама од оних које се користе против нас (Krishnan, 2018).

Китзен и Куијк (*Martijn Kitzen and Christina van Kuijck*) разматрају сегмент одвраћања везан за побуњенике и локализовано одвраћање. Тада не говоримо о стратешким претњама, већ о тактичком и оперативном нивоу, пошто би војници употребили поређење за нивое одвраћања побуњеника и обезбеђивања подршке од локалног становништва. Као што део

теоретичара предлаже кумулативност када је реч о одвраћању терориста, тако се и овде предлаже континуран утицај у комбинацији са типологијом и карактеристичним описом циљне групе, уз примену различитих метода, а посебно некинетичке природе. Низ инструмената одвраћања укључује меке алате (информације), економске подстицаје и награђивање сарадње (или њеног повлачења). Међутим, мора укључивати и више него што се генерално евидентира у западним доктринама. Када говоримо о томе да мора укључивати више него што је написано, тада се мисли на принудна средства, оснаживање ривала локалних моћника и употреба силе против оних које можемо назвати непомирљиви (Kitzen & Kuijck, 2021).

Обавештајна активност страних субјеката „који делују ка политичким, економским и безбедносним чиниоцима у матичној држави, поред осталог и кроз субверзивно – пропагандне активности усмерене на дестабилизацију институција и изазивања тензија у друштву, представља претњу по безбедност матичне државе" (Стратегија националне безбедности Републике Србије, 2019, стр. 27). У овом одређењу обавештајне активности видимо да је у најзначајнијем државном документу за безбедност државе, стратегији националне безбедности државе, сегмент политичких, економских, безбедносних чиниоца обухваћен и као посебан сегмент необавештајне (субверзивне) активности, што представља деструктивни, офанзивни део активности служби безбедности једне државе.

5.1.1. Теорија необавештајне активности у Републици Србији

У Републици Србији теоретичари су о необавештајној активности служби безбедности изнели следеће: Бајагић износи да службе безбедности као специјализоване агенције извршне власти реализују поред обавештајних, контраобавештајних и необавештајне активности. Под *необавештајним дејствима*, Бајагић наводи да је то субверзивна активност односно доводи у паралелу са тајним акцијама служби безбедности (Бајагић, 2015а). Стога, у овом истраживању *необавештајна активност*, термин употребљаван у Републици Србији, најприближнији је терминима *тајне акције* и *активне мере* тако да ће као такав бити употребљаван у истраживању.

Милован Трбојевић наводи да у обавештајној теорији не постоји јединствена дефиниција за појам *необавештајна активност*, међутим, међу теоретичарима обавештајног рада постоји општа сагласност да је активност из ове области деловања обавештајних служби у функцији реализације циљева из домена спољне политике (Трбојевић, 2017). Најчешће употребљавани синоними за необавештајне активности у стручној литератури која се бави обавештајном делатношћу су: *прикривене операције, тајне операције, тајне акције, специјалне активности, неконвенционална дејства* (Трбојевић, 2017).

Мијалковић Саша износи да обавештајни феномен обједињава обавештајну, безбедносну и необавештајну – субверзивну активност, којима се у основи остварује национална безбедност, и организацију – установу која је компетентни организатор и извршилац те активности, служба безбедности (Мијалковић, 2011).

Тако Смиља Аврамов сматра да *тајне акције*, како су дефинисане у америчкој литератури, представљају процес навођења једне владе на одређени курс путем тајних операција на војном, политичком, економском и научно – уметничком подручју. Она износи да такве акције представљају тотално игнорисање правних и етичких стандарда (Миљковић, 2016). У нашој литератури ове акције су називане и *субверзивне акције* или *необавештајна*

дејства. Саша Мијалковић износи да тајне субверзивне акције изводе стране службе безбедности или снаге за извођење специјалних дејстава, уз ослањање на тзв. унутрашњег непријатеља, политичке покрете, партије, организације, екстремистичке етничке и верске групе, опозицију и политичке непријатеље владе (групе и фракције). Мијалковић даље сматра да од субверзивне активности треба разликовати тзв. стратегију доминације, која је знатно ширег обима и садржаја (Мијалковић, 2015). Реч је о „способности државе или групе држава да доминирају и контролишу друге државе, посебно мање и слабије или регионе, као и међународне процесе, а не само да утичу на њих" (Мијалковић, 2015, стр. 200).

У питању су активности у којима учествују или које спроводе службе безбедности, а где је веома тешко установити идентитет лица (група, организација, компанија, ентитета) који их спроводе; сами извршиоци су врло често (не увек) физички удаљени од ефеката оваквих операција (напада), врло често у другим државама и интензивно се користе као замена за савремени агентурни рад, док је сврха необавештајних активности спровођење једне врсте присиле најчешће великих сила у одређеним активностима (политичким, пропагандним, економским, паравојним и др.), са посебним освртом на информационе операције ради остварења најчешће спољнополитичких циљева, мада не треба искључити и друге циљеве (Марјановић, 2022).

5.1.2. Облици необавештајних активности

У директиви (енг. *National Security Council 10/2*) су већ први пут побројани облици необавештајних активности. Тајне операције обухватају све тајне активности које се односе на: пропаганду, економски рат, превентивно директно деловање укључујући саботаже, мере против саботажа, рушења и евакуације, субверзија против непријатељских држава, укључујући помоћ подземним покретима отпора, герилцима и групама за ослобођење избеглица и подршку аутохтоним антикомунистичким елементима у угроженим земљама слободног света (National Security Council 10/2, 1948). Важно је нагласити да је овом директивом регулисано да тајне операције не обухватају оружани сукоб признатих војних снага, шпијунажу, контрашпијунажу и прикривање и обману војних операција (National Security Council 10/2, 1948).

Ако се користи на опрезан и ограничен начин, „тајна акција може послужити као суптилнији и хируршки прецизан алат, него облици признатог коришћења моћи и утицаја САД" (Weapons of Mass Destruction, 2005, p. 33). Амерички закон захтева да председник одобри све тајне радње пре њиховог извршења у писаном „налазу" и да се обавештавају два обавештајна одбора у Конгресу. „Тајне акције могу укључивати политичке, економске, пропагандне или паравојне активности. Тајне акције спроводи америчка Централна обавештајна агенција уз помоћ других (уколико је иста неопходна) елемената обавештајне заједнице, а према упутствима председника" (Weapons of Mass Destruction, 2005, p. 585).

Ради одвраћања других држава, необавештајне активности су покривале деловања служби безбедности у политичким, економским, пропагандним, као и у паравојним активностима. САД су биле у великој мери изненађене кад су њихове службе безбедности открile да је РФ покренула неколико необавештајних активности, почев од сајбер напада у Естонији 2007. године, затим у руско – грузијском оружаном сукобу 2008. године и приликом анексије Крима 2014. године, све до широко распрострањене операције утицаја усредсређене на америчке председничке изборе 2016. године, сајбер напада у Украјини 2017.

године, сајбер напада у Пољској 2021. године усмерених на политичаре и других сличних активности у 2022. години. Овакве операције присутне су скоро свакодневно широм планете, међутим, поменуте операције су најбитније и највеће акције овог типа.

Приликом отварања Вагнер центра 2022. године (*Слика 4*), један од гостију на отварању Центра био је Руслан Осташко, ултрапатриотски телевизијски водитељ и пропагандиста, али и члан одбора Фонда за развој интернет иницијатива. Фонд је у суштини фирма ризичног капитала коју финансира наводно РФ и један је од Путинових пројеката. Фонд води Кирил Варламов, бивши инжењер из Јекатеринбурга, члан Сверуског народног фронта, беспоговорно лојалан Путину, и без репутације или пословног искуства ван пројеката које финансира влада. Током 2021. године, влада је обезбедила 15 милијарди рубаља (250 милиона долара) за развој 200 *патриотских* пројеката, укључујући телевизијске серије, компјутерске игрице и софтвере (Бороган & Солдатов, 2022).

Слика 4. „Центр ЧВК Вагнер в Санкт – Петербурге”, рус. (Вагнер центар – приватна војна компанија). Извор: Бороган & Солдатов, 2022.

Постоји велики избор алата, или, ако говоримо о сукобу, тада није ретко употребљаван и термин оружје у овим и сличним операцијама (рату или како Израел дефинише у својим стратешким документима *Кампање између ратова*, прим. аут.) у свету информационо – комуникационих технологија. Ради се првенствено о „комбиновању старих класичних облика информационог сукоба (пропаганда, манипулација јавним мњењем, дезинформације) са новим методама њиховог спровођења (астротурфинг[36], креирање лажних онлајн налога, електронски фишинг[37] и др.). Информациони рат подразумевао је лично

[36] Појам *астротурфинг* је у суштини врста манипулације јавном свешћу (на Западу познато под називом *креирање* става, или мишљења јавности) којом се публика уверава да постоји одређени природни општи став јавности, а у ствари се ради о вештачки изазваном, развијеном, унапред одређеном и наметнутом ставу мале групе људи. Основ ове појаве изложен је у радовима Гистава Лебона (Француска) и Ванса Пакарда (САД). Нешто пре нациста, медијску манипулацију свешћу су ради политичких циљева пре свих покушали да развију пропагандисти Лењиновог доба Савеза Совјетских Социјалистичких Република, користећи достигнућа руске модерне, али је тај покушај брзо пропао. Дакле, ради се о опсежној операцији манипулације свешћу (Ковачев, 2018).

[37] *Фишинг* (енг. *phishing*) напади представљају једну врсту социјалног инжењеринга где жртва најчешће добија мејл са линком који на први поглед има адресу познатог сајта, међутим адреса линка је необична или се незнатно разликује. Најчешће се у мејлу тражи да се улогујете уписујући своје корисничко име и лозинку и то хитно, под неким од образложења где бисте наводно били оштећени услед непоступања по том захтеву. Назив

извиђање, диверзантске акције за подривање позадине непријатеља" (Мельникова, 2020, p. 68).

Табела 9. Организација необавештајних активности у РФ.

Врста необавештајне активности	Државне целине	Приписано и неприписано приватним војним компанијама	Страни партнери РФ	Главни изазови за постизање циља
Војне (паравојне) активности	Главна управа /Спетсназ[38]; Ваздушно десантне снаге[39]	Приватне војне компаније (*група Вагнер*)	Сепаратисти	• Релативно високо способне лаке јединице, снаге • Тешко је разликовати од наоружаних цивила у почетку; одговор органа за спровођење закона може бити недовољан, док војни одговор сноси политичке последице и може да допринесе пропаганди РФ
Политичке активности	Могућа реализација од стране служби безбедности (Главна управа[40], Федерална служба безбедности [41], Спољна обавештајна служба [42])	Патриотске групе повезане са државом (нпр. бајкери Ноћни вукови и сл.)	Атака[43] у Бугарској, Фронт Национални у Француској, Алтернатива за Немачку у Немачкој	• Политички утицај у циљним земљама • Приписивање Влади РФ • Заснован на већ постојећим политичким поделама
Економске активности	У државном власништву предузећа (нпр. Газпром, Росњефт)	Приватно, повезано са државом, компаније (нпр. Лукоил)	Трговински партнери са РФ	• Обимне европске трговинске везе са РФ • Потешкоће у разликовању легитимних активности
Информационе активности	*Русија Данас*, Россииа Сегодниа, Спутњик, службе безбедности	Агенција за истраживање интернета (и друге фарме тролова)	Корисници који појачавају медије РФ или несвесно учествују – *корисни идиоти*	• Обмањујући или лажним садржајима • Тешко се регулише • Приписивање • Глобални досег
Сајбер активности	Главна управа, Федерална служба безбедности, Спољна обавештајна служба	Кооптирани независни хакери: АПТ[44]28, АПТ29	Патриотске хакерске групе: *CyberBerkut*	• Високо способан • Приписивање • Глобални досег

Извор: Radin, Demus & Marcinek, 2020, p. 9.

фишинг је варијација речи фишинг односно пецање, јер се фишинг мејлови обично шаљу на велики број адреса као мамац, тако да слично као приликом риболова – пецања, *неке рибе се упецају док неке не* (Мельникова, 2020).

[38] Спетсназ, специјалне снаге војне службе безбедности Главне управе.

[39] Ваздушно десантне снаге оружаних снага Руске Федерације.

[40] Главна управа, служба безбедности војног карактера, Главна управа Генералштаба оружаних снага РФ, а ранији назив службе безбедности је био Главна обавештајна управа, међутим у великој употреби је и даље овај стари назив међу теоретичарима.

[41] Федерална служба безбедности, служба безбедности првенствено контраобавештајног карактера у РФ.

[42] Спољна обавештајна служба, служба безбедности првенствено обавештајног карактера у РФ.

[43] Атака, ултранационалистичка странка у Бугарској, скраћено од енг. *Attack Party*.

[44] АПТ, акроним на енг. *APT – advanced persistent threat* (напредна упорна претња – у овом случају наводно хакери).

У наредних неколико пасуса објашњавамо наведену табелу (*Табела 9*) о организацији необавештајних активности у РФ. Прва колона у табели указује на различите категорије актера који су укључени у субверзивне активности, од оних који су део Владе РФ, или оних који то нису (чине то свесно или несвесно), а деле заједнички интерес са РФ у сарадњи по одређеним питањима (Radin, Demus & Marcinek, 2020).

Мијалковски и Конатар, као карактеристичне врсте необавештајних активности које обавештајне службе једне државе примењују против друге државе, првенствено на њеној територији, описују следеће (Мијалковски и Конатар, 2010): „тајна (покривена) пропаганда; обавештајно – индоктринарне операције; субвенционисање појединца; организовање и извођење саботажних акција; подстицање, организовање и учествовање у спровођењу организованог криминала ради подривања економске и политичке основице друштва; обука појединца и колективитета за конкретну врсту необавештајне активности; изазивање и подстицање међуетичких, међуверских и сличних напетости; корумпирање и уцена особа у владином и невладином сектору и њиховог ангажовања за саботирање у доношењу одлука којима се успешно штити национална безбедност државе жртве и опструисање донетих одлука у ту сврху; формирање група у појединим областима друштвеног живота за јавни притисак на органе власти; подстицање и руковођење терористичким, пучистичким, превратничким и побуњенистичким активностима; тајно стварање милитантних састава и њихово наоружавање и оспособљавање за примену оружаног насиља; планирање и извођење атентата на државне званичнике и истакнуте јавне личности; изазивање и управљање кризом у држави жртви и др.” (Мијалковски и Конатар, 2010, стр. 115, 116).

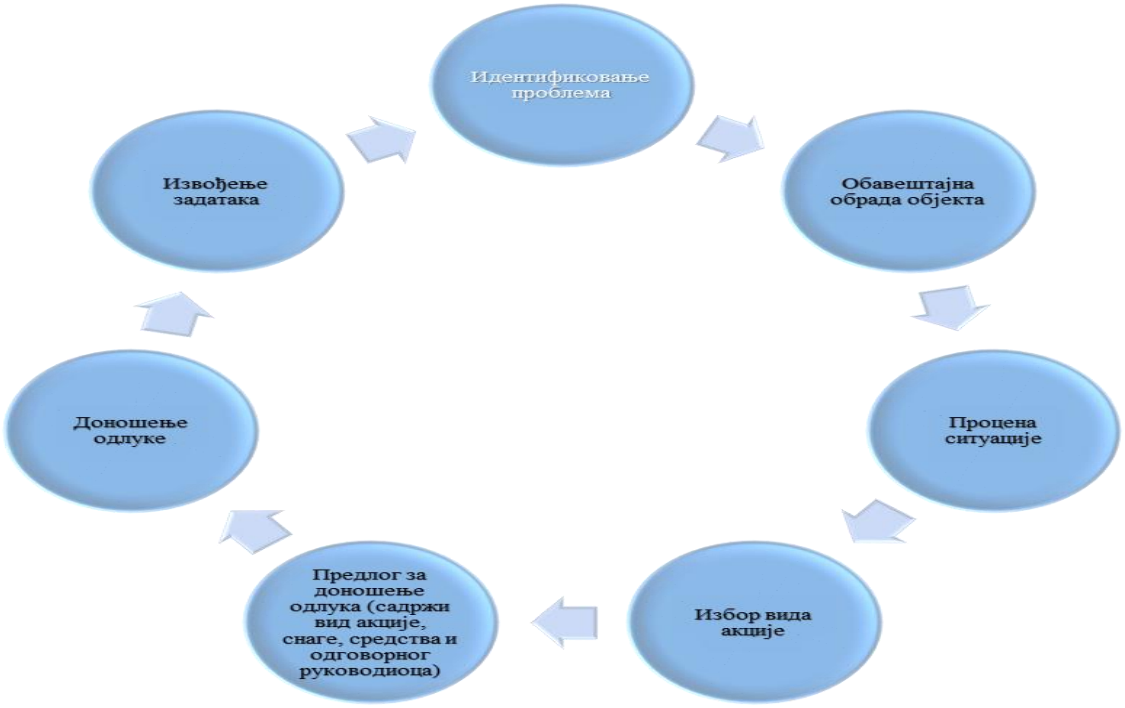
5.1.3. Процес необавештајних активности

Марк Ловентал (*Mark Lowenthal*) сагледава процес необавештајних активности (у САД: *тајних акција*) кроз следеће фазе: Планирање мора почети са креаторима политике који дефинишу националне државне интересе и решење препознају у необавештајним активностима као изводљивом средству за постизање задатих циљева. Како би оваква активност била успешна, неопходно је обезбеђивање финансија за њену припрему и извршење. Следећа фаза је неопходна базна припремљеност за реализацију активности (брзо обезбеђење опреме, превозних средстава, лажних докумената и друго, као и обучено особље, укључујући страну имовину) мора бити обезбеђена у сваком тренутку. Логистичка подршка за одржавање састанака, поседовање агената за надзор, за писма, за техничку подршку и друге специјалности. Потребно је време за припрему и реализацију ове врсте активности. Следећа фаза је достављање државним руководиоцима званичних процена од служби безбедности о томе колики је ризик за предузимање одређене активности. Тај ризик се појављује као ризик од излагања – упознавања са активношћу (операција може бити изложена ризику док траје активност или убрзо након њеног завршетка или оне које су откривене годинама касније). Следеће што можемо да наведемо је ризик који треба предвидети услед неуспеха активности и предвиђање поступака у свим варијантама (Lowenthal, 2009).

Под процесом планирања и извођења специјалних акција и операција, пензионисани пуковник Мирковић је обухватио следеће (*Шема 2*) начелне сегменте поменутог процеса: идентификовање проблема, обавештајну обраду објекта, процену ситуације, избор вида

акције, предлог за доношење одлука (садржи вид акције, снаге, средства и одговорног руководиоца), доношење одлуке и извођење задатака (Мирковић, 1999).

Шема 2. Процес необавештајних активности.



Извор: Аутор, према регистрованим фазама (У: Мирковић, 1999).

Када о процесу необавештајних активности говоре други теоретичари, Мијалковски и Конатар (*Шема 3*) у Републици Србији, тада имамо следеће фазе које у својим корелацијама обухватају један процес необавештајне активности службе безбедности: политичко – налогодавна фаза, стручно – налогодавна фаза, фаза планирања, организациона фаза, извршна фаза и аналитичко – извештајна фаза (Мијалковски и Конатар, 2010).

Шема 3. Процес необавештајне активности службе безбедности.

Извор: Мијалковски и Конатар, 2010, стр. 106.

Процес необавештајне активности је сложена активност коју чини више међусобно повезаних фаза у којима се као учесници, извршиоци или носиоци (или помоћни носиоци) активности појављују службе безбедности, као и велики број уско специјализованих предузећа, фирми, компанија, организација, институција, група, до појединаца из великог броја различитих сфера државе и друштва, где се, у виду једног или више циклуса, реализује циљ постављен од државног руководства, најчешће спољнополитичког карактера. Како бисмо успели да на што квалитетнији начин објаснимо шта је све неопходно урадити како бисмо дошли до крајњег производа необавештајних активности служби безбедности, а ради комплексности ове материје коју истражујемо, неопходно је повезати све фазе у један круг (*један циклус*), уз регистровање великог броја корака (у свим фазама) који заједно чине процес необавештајне активности. Када се све ове фазе (могли бисмо констатовати да су то три фазе) које засебно чине један од сегмената необавештајне активности обједине, оне чине један процес необавештајних активности уз специфичности сваке активности за себе. У суштини, скоро све ове фазе можемо груписати у фазе које обухватају све што се чини од стране наредбодаваца за предузимање одређених спољнополитичких циљева и служби безбедности и других учесника у необавештајним активностима у *припреми* активности, затим током *извршења* – реализације операције (активности или најчешће више активности) као и оно што највећи број аутора, како домаћих тако и страних, заборавља, а то је *експлоатација* – стабилизација, поступање након завршетка необавештајне (операције) активности (припадника службе безбедности и/или других лица, организација, компанија, ентитета).

Шема 4. Процес необавештајних активности (фазе операција – активности).

Извор: Аутор.

На основу истраживања већег броја теоретичара (Мирковић, 1999; Савић, 2006; Мијалковски и Конатар, 2010; као и на основу личних запажања аутора), можемо закључити следеће. Процес необавештајних активности можемо поделити у три фазе (*Шема 4*):
I Припремна фаза активности, *II Фаза извршења* активности и *III Фаза експлоатације – стабилизације* активности.

I Припремна фаза обухвата низ поступака који претходе извршењу неке необавештајне активности (операције).

Одређивање контраобавештајних, обавештајних потреба најчешће диктирају спољнополитички одлучиоци (могу то да чине самостално или да се консултују са шефовима служби безбедности).

После ових одређења, следи преношење тих потреба од наредбодавца (политичког руководиоца стратегијског нивоа) до установа, службе безбедности која треба да реализује или учествује у реализацији постављеног задатка, где у овој другој варијанти мора да пренесе задатке до извршиоца, учесника у необавештајним активностима (који зависно од врсте необавештајне активности варирају од структура државног апарата војних и цивилних, фирми, организација, компанија, институција, група, појединаца).

Следи анализа расположивих контраобавештајних, обавештајних сазнања, података, информација неопходних за реализацију необавештајне активности.

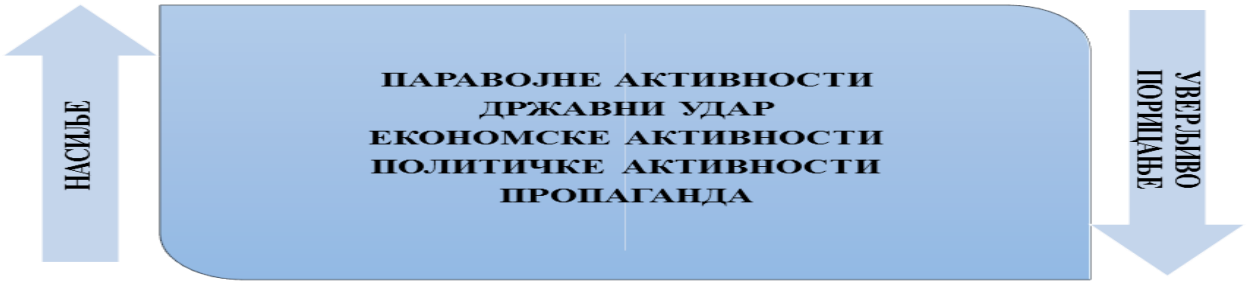
Затим следи фаза планирања у којој службе безбедности морају до детаља да предвиде све потребне обавештајне и контраобавештајне активности које је неопходно предузети за потребе необавештајне операције, активности, затим неопходне снаге, средства, потребна финансијска средства (начин обезбеђења) и посебно начин (одређење шта је тајно у поступању, а шта су јавно дозвољени подаци за употребу) на који ће нешто бити реализовано.

Пред свако извршење активности следи припрема, ангажовање стручних лица, специјалиста из својих области рада, и по потреби едукација тј. обука потребних лица (за део лица ово је стални задатак) и припрема логистичке природе за реализацију необавештајне активности, поготово у успону сајбер технологија и информационих операција.

II Фаза извршења није случајно на слици приказана црвеном бојом, будући да представља најкритичнију и најризичнију фазу у процесу необавештајних активности. У фази извршења, у зависности од врсте необавештајне активности која се примењује, време трајања може бити релативно кратко (уколико се ради о економским, политичким, саботажним активностима, атентату и сл.), а може трајати и дужи временски период (пропагандне, паравојне, смена власти – државни удар и сл.), када су неопходна стална прилагођавања већ урађених планова извршења операције, активности. Ризичност ове фазе карактеришу сазнања, подаци и информације који су добијени од стране службе безбедности у фази припреме активности, али с обзиром на то да велики број фактора утиче на реализацију необавештајне активности која се најчешће изводи изван матичне државе, долази до још већег броја непознаница. Те непознанице су присутне зато што службе безбедности не могу никада све да сазнају (велики број података њима је познат, док део остане непознаница), а посебну тежину даје и то што ће лица, групе, организације и институције који су укључене у реализацију необавештајних активности највероватније да се суоче са непознатим утицајем много фактора које није могуће сазнати, предвидети, нити на њих утицати, већ тек када отпочне извршење активности, операције. Навешћемо део метода које службе безбедности примењују у необавештајним активностима ради реализовања ове фазе необавештајне активности: употреба агената од утицаја, фракција и група, постављање одређених информација и дезинформација, фалсификати, претње насиљем и примена насиља, атентати, уцене са компромитованим материјалима или опет насиљем, низ активности у сајбер домену и друго.

Када говоримо о насиљу, Марк Ловентал (*Mark Lowenthal*) је дао приказ раста – односно опадања примене насиља (од пропагандних активности као најнижег степена

регистрованог насиља, па до паравојних активности које се одликују највишим степеном насиља) и уверљивог порицања у одређеним тајним акцијама (необавештајним активностима које је најнижег нивоа током паравојних активности, а расте све до употребе пропагандних активности када достиже врхунац уверљивог порицања) и то је приказано (види *Слику 5*) на следећи начин (Lowenthal, 2009).



Слика 5. Приказ раста нивоа насиља и уверљивог порицања услед примене одређене врсте необавештајне активности односно њиховог опадања.
Извор: Lowenthal, 2009, p. 182.

Основна карактеристика ових необавештајних активности је да се ради о недозвољеним активностима у страној држави, а за матичну државу најчешће одобреној активности од државног руководства, што не значи да се и тад ради о легалној активности.

III Фаза експлоатације – стабилизације представља фазу када је реализована необавештајна активност, спроведена једна врста присиле над неким (или нечим) и обухвата низ радњи које предузимају првенствено службе безбедности како би се анализирала извршена активност, сагледале позитивне и негативне стране предузиманих радњи, извештавање о предузетим активностима. У овој фази се врши процена да ли је извршењем активности дошло до постизања постављеног циља у задатом плану у припреми операције тј. активности или је неопходно наставити процес необавештајних активности чиме се понавља циклус са ановљеним задацима, снагама, средствима, како новим сазнањима и подацима уступљеним од стране служби безбедности, тако и са логистичком подршком, односно по потреби увођењем нових структура и нових сазнања који ће бити укључени у реализацију необавештајне активности. Након свих ових закључака, политичком руководству се у овој фази након анализе презентује шта је то урађено и какви су ефекти, са предлогом даљих радњи које је неопходно предузети. У овој фази се примењују мере *маскирања*, како за податке о извршеној активности, тако и за део или све учеснике, наоружање, средстава, фирме, компаније, рачуне и слично, уколико је то неопходно за конкретну необавештајну активност.

На наведеној шеми (*Шема 4*) смо све време посматрали круг, односно процес који, уколико није довршен постављени циљ, може (уз захтев тј. одобрење наредбодавца) да се понавља (идентичан или са променама дела или већине или свих делова плана активности) док се не реализује постављени циљ најчешће спољне политике државе и не постигне жељени циљ руководства државе применом необавештајних активности. У свим овим ситуацијама, фазама, како на почетку, тако током активности, па до завршетка експлоатације

необавештајне активности појављују службе безбедности као непосредни или посредни учесници који директно учествују као реализатори необавештајне активности или као помоћни носиоци те активности у улогама оперативаца или аналитике обављајући контраобавештајне и/или обавештајне активности стварајући услове за спровођење оваквих и њима сличних активности.

Разумевање повратних података је врло битно за квалитетну примену необавештајних активности. На тај начин се долази до података шта је довело до тога да нека активност не буде реализована или не буде реализована онако како је то испланирано. Да ли су лоши обавештајни (контраобавештајни, безбедносни) подаци, информације, процена лица или неке активности или употреба неких погрешних средстава логистичке природе, што би могло у некој новој активности или новом процесу, циклусу отклонити и смањити евентуалне губитке, резултате, време или неки други услов. Ради се о једном изузетно моћном средству спољне и не само спољне политике, да би се реализацијом – извршењем активности завршавао процес необавештајне активности. Управо и то је један од разлога зашто је аутор увео трећу фазу необавештајне активности као обавезан део процеса. Напредне технологије су довеле до брзих промена и у врстама необавештајних активности служби безбедности, јер су претње еволуирале са напретком технологија и преселиле се у другу – сајбер димензију. Зато је веома битно да и када се говори о врстама необавештајних активности, па и начину спровођења истих, констатујемо да је наведена област условљена великим бројем фактора који нас окружују, који су опет променљивог карактера и директно испољавају утицај на избор врсте необавештајне активности (или евентуално стварања нове) која би била адекватно применљива у конкретном случају.

5.1.4. Специфичности необавештајних активности

Након 11/09 се наглашава важност придржавања заштите приватности и грађанских слобода. Страх је оправдан, јер доступност података на више адреса доводи до могућности већих злоупотреба. Важно је и нагласити да треба узети у обзир променљивост природе претње, зато што се фокус подршке служби безбедности у ангажовању на заштити националне безбедности државе доста изменио, тј. еволуирао је, и то од класично државног према недржавним актерима. Појединци све чешће делују сами или као део групе која није повезана ни са једном државом (видљиво није повезана, што највише говори о необавештајним активностима). Прикупљање података против ових претњи захтева поштовање правила и прописа о надзору служби безбедности, као и додатну годишњу обуку радне снаге ангажоване на овим пословима (DeVine, 2019a).

Када говоримо о реализацији необавештајних активности служби безбедности САД, најпознатија у протеклом периоду била је компанија из САД, енг. *Blackwater USA* (сада већ под другим називима), која је учествовала у пословима највишег безбедносног нивоа у земљи и иностранству. Врло често су се у медијима помињале оптужбе на рачун ове компаније и то за више злочина над цивилним становништвом у Ираку. Све ово је правдано под покровитељством заштите наводно дипломата САД у Ираку. Ангажмани ове компаније обухватају милионске износе изражене у доларима, а сличним активностима се баве и многе друге компаније о којима ће детаљно бити речи у поглављу паравојне активности овог истраживања (Мијалковић, 2010).

Када говоримо о реализацији активних мера (необавештајних активности) служби безбедности РФ, првенствено о службама и снагама које поседују за спровођење истих, тада говоримо следеће. Федерална служба безбедности, морамо је поменути као наследника два саставна елемента за реализацију активних мера од Комитета државне безбедности, а ради се о јединицама под називом *Алфа* и *Вимпел* (које су биле део Првог главног директората Комитета државне безбедности током постојања Савеза Совјетских Социјалистичких Република и имале су улогу планирања, организовања и спровођења прикривених страних акција). У периоду од 1991. године, ове две јединице су промениле надлежност, тако да су постале задужене за предузимање активних мера унутар РФ (Алфа и Вимпел су одговорни за праћење и неутралисање терориста или других претећих субјеката унутар РФ). Ова година је била разлог промена надлежности, јер је формирана служба безбедности Спољна обавештајна служба која има спољни елемент и јединицу *Заслон* за овакве потребе (Riehle, 2022). Међутим, важно је нагласити да се ове целине, Алфа и Вимпел, баве искључиво унутрашњом безбедношћу, али да реализације својих операција могу изводити и у иностранству. Њихово ангажовање у чеченским ратовима и током талачких ситуација на Северном Кавказу, као што су операције у школи у Беслану и болнице у Буденовску. Истрага *Bellingcat*[45] из 2020. године показала је „да је убица умешан у убиство грузијског емигранта и чеченског милитанта Зелимкана Кангошвилија у Немачкој у августу 2019. године био повезан са јединицом Вимпел. Није искључено и да су Алфа и Вимпел можда стајали и иза убистава других чеченских вођа милитаната ван Русије" (Riehle, 2022, p. 72). Чувена војна служба безбедности РФ, Главна обавештајна управа, а од 2010. године са новим именом Главна управа Генералштаба, надлежна је за прикупљање обавештајних података у циљу подршке доношењу војних одлука и за тајне операције за подршку спољнополитичким циљевима (Riehle, 2022). Спољна обавештајна служба у свом саставу поседује организациону целину познату као Заслон, која је наводно директно потчињена директору службе безбедности. Ради се о целини наводно задуженој за заштиту одређених лица из амбасаде РФ, као и других званичника Владе РФ када путују на ризична одредишта у иностранство. Забележен је случај овакве врсте, када су припадници Заслона, официри, обезбеђивали тадашњег потпредседника Владе РФ, Дмитрија Рогозина који је 2014. године путовао у Сирију. Овај састав, такође спроводи активне мере, тајне акције. Мало се у јавности зна о овој целини, саставу, али је наводно основана 1998. године да замени јединице специјалних снага које су биле подређене Првој главној управи Комитета државне безбедности током постојања Савеза Совјетских Социјалистичких Република (Riehle, 2022).

У периоду до 2010. године, било је активно неколико међународно фокусираних, оперативних руских приватних безбедносних компанија, које су првенствено водили бивши војни службеници и припадници служби безбедности. У почетку су ове компаније нудиле традиционалну обуку и услуге заштите за приватне фирме, укључујући услуге борбе против пиратерије. Често су ове групе радиле или су имале везе са руским државним нафтним и гасним компанијама. Временом су се формирале нове компаније које су имале акценат на

[45] *Bellingcat*, енг. је група истраживачког новинарства са седиштем у Холандији која је специјализована за проверу чињеница и обавештајних података отвореног кода – употреба података отвореног извора. *Звоњење мачке* (енг. *Bellingcat*) које потиче из средњовековне бајке о мишевима који расправљају о томе како учинити мачку безопасном, са закључком мишева да ставе звоно на мачку. Сви мишеви подржавају идеју, али нико није вољан да то уради.

борбеним активностима и укључивале су не само обуку и координацију локалних снага, већ и учешће у директној борби. Више приватних предузетника регистровано је у РФ и у иностранству (укључујући Кипар и Хонг Конг). Ради прикривања стварног власника компаније, овакве компаније се врло често расформирају, трансформишу и поново формирају са новим именом, лицима која воде компанију и локацијом. У медијима се као једно од најзвучнијих имена оваквих компанија из РФ појављује приватна војна компанија *група Вагнер* (*Wagner*) и с њом повезана лица, наводно финансирана и руковођена од стране Јевгенија Пригожина (богатог бизнисмена, тј. преко његове компаније – *Concord Management and Consulting*). Ангажовањем на заштити националних интереса САД, службе безбедности САД су преко надлежних државних органа обезбедиле да Влада САД уведе санкције Пригожину (познатијем и као „Путинов кувар" – западна конструкција надимка) и *Вагнер групи* и са њим(а) повезаним појединцима и ентитетима под образложењем реализованих акција повезаних са РФ и Украјином, као и мешањем у изборе у САД и подршком бившој Влади Судана. Врло често је у медијским извештајима навођено да су *Вагнер група* и њени повезани ентитети у изузетно блиским везама са војном службом безбедности у РФ, Главном управом[46] и да су им кампови за обуку *Вагнер групе* у близини база где су стациониране специјалне снаге оружаних снага РФ. Без обзира што се на папиру као власник *Вагнер групе* налази приватно физичко лице, Министарство финансија САД идентификује *Вагнер групу* као проглашене снаге Министарства одбране Русије. У почетку сукоба РФ и Украјине, РФ је интензивно користила приватне војне компаније као и у току сукоба у Сирији, затим у Либији, Централној Афричкој Републици, Судану. Повећавањем улоге приватних војних компанија, повећавала се и политичка и економска моћ њихових власника (Bowen, 2020). Дана 16. септембра 2022. године, на великом броју телевизијских и других медија широм света, појавио се снимак на којем се једно лице које тврди да је припадник *Вагнер групе* (у медијима су помињали да се ради лично о Јевгенију Пригожину, који је наводно био затвореник у једном периоду живота) налази у неком затвору, највероватније негде у РФ и нуди великом броју присутних затвореника под конкретним условима (јасно прецизирајући шта морају да раде уколико дођу у *Вагнер групу*, а шта ни случајно не смеју да раде као припадници групе) да буду ангажовани 6 месеци на украјинском ратишту и после тога би били ослобођени казне. Дана 5. новембра 2022. године велики број прозападних и происточних медија је објавио вест о отварању центра приватне војне компаније *Вагнера* у Санкт Петебургу, РФ и да је Јевгениј Пригожин почео да шири спектар активности од чисто паравојног деловања према окупљању проналазача у центру, затим програмера, уопште стручњака за информационе технологије, разне врсте експерименталних произвођача и слично (где можемо да препознамо будућа интересовања ове групе, компаније, приватних компанија и државних служби о чему следи наредни део истраживања).

[46] У периоду од 2010. године, званичан назив војне службе безбедности оружаних снага РФ је Главна управа (рус. *Главноие управление*) Генералштаба оружаних снага РФ, али се ради о служби безбедности која је много познатија по некадашњем називу Главна обавештајна управа (рус. *Главноие разведивательное управление*) и није ништа чудно што се и данас читају и пишу текстови под називом Главна обавештајна управа (Bowen, 2021).

5.1.5. Учешће у информационим операцијама

Офанзивне сајбер операције – дефинисане као операције „којима је намењена пројекција моћи применом силе у и преко сајбер простора" – такође се могу назвати *тајном акцијом*, ако се изводе према овлашћењима из норматива у САД, енг. *Title 50 U.S. Code, § 3093*. који предвиђа законске одредбе које нека активност треба да испуни да би била *тајна акција*.

Осетљиве војне сајбер операције су подкатегорија осетљивих војних операција. Конгрес дефинише осетљиве војне сајбер операције под називом енг. *Title 10 U.S. Code* као операције које спроводе оружане снаге САД којима је циљ да изазову сајбер ефекте изван географског места на коме су оружане снаге САД умешане у непријатељства или где су непријатељства прогласиле САД. Осетљиве војне сајбер операције имају две подкатегорије. Прве, офанзивне операције сајбер простора нису дефинисане статутом, већ је то учинило Министарство одбране, као „мисије намењене пројектовању моћи у и кроз сајбер простор". Друга, одбрамбена операција у сајбер простору, дефинисана је статутом као операција „изван информативних мрежа Министарства одбране чији је циљ победа текуће или непосредне претње." Осетљиве војне сајбер операције не укључују вежбе обуке које имају ефекте на стране државе, све док се ове државе слажу нити се сматрају необавештајним активностима (DeVine, 2019b, p. 9). Део теоретичара на западу је дефинисало сајбер напад као „акције предузете преко рачунарских мрежа дизајнираних за порицање, деградирање, поремећај или уништење информационог система, информације о мрежи или информације које се налазе на њима" (Iasiello, 2015, p. 24).

Страна служба безбедности предводила је сајбер напад 2008. године на компјутерске системе оружаних снага САД. Заменик министра одбране САД Вилијам Лин рекао је да се напад догодио након што је заражени флеш диск убачен у лаптоп америчке војске у бази на Блиском истоку, отпремајући злонамерни компјутерски код на мрежу Централне команде. Овај раније поверљиви инцидент био је најзначајнији пробој америчких војних компјутера икада. Више од 100 страних обавештајних организација покушава да упадне у америчке мреже. Сајбер напади нуде средство за потенцијалне противнике да превазиђу огромне предности САД у конвенционалној војној моћи и то на начине којима је тренутно и изузетно тешкоући у траг. Лажни код, укључујући такозване „логичке бомбе" које изазивају кварове, такође се може убацити у софтвер док се развија (Stewart, 2020).

У периоду након 2010. године у званичној терминологији САД одлучено је да се термин *психолошке операције* замени термином *информационе операције војне подршке* (енг. *Military Information Support Operations*). Наведено је образложено чињеницом да нова терминологија више одражава активности Министарства одбране у области информисања и утицаја на непријатеља, неутрално и пријатељско јавно мњење усмерено на постизање стратешких циљева америчке војне команде. Промена терминологије није имала утицаја на текуће операције. Заједнички начелник штабова Оружаних снага САД је у доктрини војних информационих операција подршке навео да су такве операције најважнији елемент америчке иностране политике. Примењују се за успостављање и јачање спољашњих перцепција Оружане снаге САД, политички и економски потенцијал, док у оружаним сукобима такве операције повећавају ефикасност борбене моћи (представљају множилац снага). Информационе операције војне подршке се састоје од следећих фаза: планирање, идентификација и анализа циљне публике, развој сета мера, развој неопходних ресурса,

одобрење менаџмента, производња и дистрибуција, оцена обављеног посла. Посебна пажња је посвећена идеолошким аспектима одржавања информационе операције војне подршке, посебно у обезбеђивању безбедности стране државе (енг. *Foreign internal defense*), приликом спровођења таквих операција против тероризма, операције стабилизације сукоба, операције за борбу са покретима устаника и током специјалних војних операција – неконвенционално ратовање (Шариков, 2020).

Појам информације према теоретичарима из РФ представља „скуп чињеница, норми и других података, неопходних за доношење конкретних одлука и извршавање одређених задатака и преноси се на одређени начин између субјеката, лица и техничког средства, као и између самих техничких уређаја" (Мельникова, 2020, p. 48). У РФ, теоретичари појмове везане за информационе операције одређују на следећи начин: „*Информација* је степен промене знања о неком предмету. *Информациона операција* представља дистрибуцију и наметање скупа међусобно повезаних порука, уједињених заједничком темом, с тенденцијом сталног раста и усмерених на промену стања јавне свести. *Информационо оружје* представља техничка средства и технологије наменски коришћене за активирање, уништавање, блокирање или креирање процеса у информационом систему за које је заинтересован субјект који користи оружје." (Расторгуев & Литвиненко, 2014, p. 126). Некада се одређене појаве могу гледати и ништа не видети, затим могу се и слушати и опет ништа не чути, као и не разумети. Да бисте разумели одређен изазов, ризик или претњу, морате разумети како се оне стварају. У том циљу неопходно је констатовати главна информациона оружја, и то „службе безбедности, информационе операције и наравно управљање и планирање информационих операција" (Расторгуев & Литвиненко, 2014, p. 120, 121).

Све је већа адаптација служби безбедности, односно рада њихових припадника услед све већег развоја информационо – комуникационих технологија где су потребна многа прилагођавања. Доста је примера ангажовања служби безбедности према лицима из сектора информационих технологија. Тако су службеници Федералне службе безбедности приморавали држављанина РФ (запосленог у фирми енг. *TLSContact* на одржавању рачунарске мреже у конзулату Уједињеног Краљевства у РФ) да им преноси информације о британском систему захтева за визу, што је радио до 2016. године када је пребегао. Захтев Федералне службе безбедности је поред информација био и да се тајно обезбеде визе за два држављана РФ. Наведене активности су доведене у везу са одласком два официра Главне управе, одговорним за покушај убиства Сергеја Скрипала 2018. године. Поред оперативног деловања према Уједињеном Краљевству, Федерална служба безбедности је офанзивно деловала и вероватно и даље делује према САД. Наводно је регрутовао жену, држављанку РФ која је била веза између канцеларије тајне службе САД у Москви и служби безбедности РФ као и агенција за спровођење закона. Она је имала одобрење и приступ систему електронске поште амбасаде САД све док није отпуштена са посла 2017. године. Јерменска амбасада у Москви је наводно доживела сајбер нападе који су установљени 2020. године, где је као реализатор тих активности означена јединица за компјутерске операције Федералне службе безбедности. Активности служби безбедности које су реализоване на сличан начин су пријављене и у делегацији Европске Уније у Москви 2017. године. Карактеристично је и наводно „пецање" путем мејлова 2018. године преко једне европске амбасаде у Москви која је укључивала мејлове маскиране као наводно поруке од *Јанес*, британске новинарске

компаније за одбрану, са одређењем, метом на Министарство спољних послова у Северној Америци и Европи (Riehle, 2022). Није искључено да су овакви и њима слични догађаји јако честа појава и да су службе безбедности упознате са оваквим инцидентима, али да се много тога не пријављује или остаје неоткривено. Свакако, не треба искључити ни могућност да је један од разлога непријављивања инцидената и избегавања јавног говора о својим рањивостима, управо заштита система.

У периоду од 20. октобра 2010. године, па до децембра 2022. године, од званичника РФ су само по питањима информационе безбедности донете 44 изјаве, констатације, најаве и промене везане за информациону безбедност у РФ (Information Security, 2022).

Посебан осврт у овом истраживању биће на *информационим операцијама* које су по својој суштини и пореклу војне природе. Дефиниције информационих операција пре свега су присутне у војним и безбедносним доктринарним документима западних држава, док теоретичари РФ дефинишу и користе појам информациона дејства или информациона борба. За ово истраживање прихваћен је термин информационе операције (Миљковић, 2016).

Информациони простор је одавно постао саставни елемент спољне стратегије САД. Велики број начина је данас доступан руководству државе да би се осигурала национална безбедност државе (углавном називани *мека* или *паметна* моћ, много ефикаснији начин), а да то није коришћење *тврде моћи*. Председник САД Барак Обама је у својим говорима[47] више пута најавио стратегију „паметног" лидерства, вођства у спољнополитичкој стратегији САД. У војној терминологији је избегаван термин рата као традиционалног појма, већ се све више користи термин *информационе операције* која подразумева да информативне медије користе оружане снаге заједно са конвенционалним оружјем или другим средствима војне силе. Оружане снаге САД тренутно спроводе активности везане за информационе операције у 14 области: „1) стратешка комуникација, 2) заједничка међуагенцијска координациона група, 3) јавни послови, 4) цивилно – војне операције, 5) операције у сајбер простору, 6) обезбеђивање безбедности информационе инфраструктуре, 7) свемирске операције, 8) операције подршке војним информацијама, 9) обавештајне (интеграција информационих операција у обавештајној активности), 10) војна обмана, 11) оперативна безбедност, 12) специјалне техничке операције, 13) комбиноване операције у електромагнетном опсегу, 14) ангажовање кључних лидера" (Шариков, 2020, p. 2). Утицај не би требало да се деси само преко америчких јавних информативних медија, већ и преко приватних. Блиска сарадња са приватним медијским организацијама је високи приоритет за међународну информациону политику. У савременој војној стратегији САД, односи с јавношћу (*Public Affairs*) су једна од

[47] Председник САД Барак Обама је ово изјавио парафразирајући познатог професора Џозефа Ная (*Džozef S. Naj,* харвардски професор, саветник неколико америчких администрација и творац чувеног концепта *паметне моћи*). Још у својој књизи из 2004. године, *Мека моћ: путеви успеха у светској политици*, Ај је увео појам *паметна моћ* који се односи на комбиновање тврде и меке моћи у једну успешну стратегију. Представља комбинацију тврде моћи присиле и исплате са једне стране и меке моћи убеђивања и привлачења, с друге. Да би се створила *паметна стратегија* она, по мишљењу Ная, мора одговорити на 5 главних питања: „Који су жељени исходи и циљеви?"; „Који су ресурси на располагању и у којим контекстима?"; „Које су позиције и преференције одабраних мета на које се покушава утицати?"; „Који облици понашања моћи имају највише изгледа за успех?"; „Колика је вероватноћа успеха?". Стратегија мора повезивати средства са крајњом сврхом што захтева јасноћу циљева (жељених исхода), ресурсе, као и тактику за њихову употребу". Ај не даје решење, већ свака држава треба да по угледу на ту „паметну стратегију" осмисли своју сопствену „стратегију паметне моћи" (Арежина, 2011, p. 294).

активности у контексту информационе операције. Извођење цивилно – војних операција се може састојати од одређивања циљне публике, синхронизације медија и других средстава за преношење информација, као и ширења вести и информација између локалног становништва. Цивилно – војне операције су „делатност МО САД, коју врше одговарајуће цивилне или војне снаге, усмерене на успостављање, одржавање, утицај или коришћење односа између оружаних снага и цивилних институција и становништва стране државе" (Шариков, 2020, p. 5). Информационе операције су саставни део активности Владе САД у вршењу утицаја, уништавању, подмићивању или потпуном контролисању процеса доношења одлука стварних или потенцијалних противника, уз обезбеђивање сигурности од спољног мешања у процес доношења одлука америчке војне и политичке команде. У реализацији војно – цивилне операције су могући следећи правци спровођења информационе операције и то укључивањем кључних лидера, затим информисањем становништва о извођењу војно – цивилних операција и подршке, исправљањем дезинформација и непријатељске пропаганде коју шири непријатељ у циљу дискредитовања грађанских власти једне стране државе, па обезбеђивањем легитимитета цивилне власти међу локалним становништвом и прикупљање информација о расположењу локалног цивилног становништва, кроз анкете јавног мњења (Шариков, 2020).

Председник Руске академије војних наука генерал Макхмут Гарејев, упозорио је 2011. године да постоје субверзивне информационе технологије Запада као основни узрок нереда у северној Африци и на Блиском истоку, што је такође познато као арапско пролеће. Даље, Гарејев наводи да је Запад такође користио ове субверзивне технологије у Грузији и другим бившим совјетским републикама. Када се све ово догађало, РФ је мислила да је то опасно по њих и да би се арапско пролеће могло проширити и на њихов регион, као што је нпр. Кавказ. РФ је такође била дубоко импресионирана развојем информационих операција на Западу (Bouwmeester, 2020). Инспирисан првим размишљањима о информационим операцијама и развоју арапског пролећа, лица стручна за ову област у оружаним снагама РФ су осврtом на информациони рат урадили следећи концепт: *Концептуални поглед на активности оружаних снага РФ у информационом простору.* Овај концепт, када говори о информационом рату, наглашава да овај вид сукоба нема за циљ само да оштети информационе системе и критичну инфраструктуру, већ да су ту и други циљеви, попут поткопавања политичких, економских и друштвених система. Када се предузимају ови видови активности, тада се помиње подстицање масовне психолошке активности међу становништвом конкретно изабране зоне дејства, са задатком дестабилизације свог друштва, испољавања присиле над конкретним метама ради прављења одлуке против њихових интереса. У овом концепту, препознаје се много већа улога власти РФ у вођењу информационог рата и овај вид сукоба се поставља у централно место сукоба у будућности. Према овом концепту, информациони рат би могао и требало да буде ефикаснији чак и од директне употребе силе у постизању традиционалних стратешких циљева (Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space, 2011).

Сагледавајући доктринарне документе оружаних снага РФ (Савеза Совјетских Социјалистичких Република), прикривање и обмана играју важну улогу у вођењу сукоба.

Начелник[48] Генералштаба оружаних снага РФ истакао је важност разматрања модерног начина ратовања кроз војна и невојна средстава ратовања, уз постизање изненађења. Наглашава важност превентивних мера, идентификовања рањивости, стварања одвраћања и одржавања способности за преузимање стратешке иницијативе. Заменик[49] председника Владе РФ је 2013. године изјавио да непријатељ може да парализе критичну инфраструктуру циљне државе сајбер нападима. Према процени лица стручних у области информационих технологија у РФ, сајбер напад на циљеве у РФ могао би да нанесе огромну штету економији РФ. И сам председник РФ је изјавио да је РФ као опкољена тврђава и да је треба заштитити. Ова опсада се проширила на сајбер простор. Према Игору Ашманову, руском стручњаку за информационо – комуникационе технологије, сајбер рат против РФ води се сваки дан и за њега не важе никаква правила рата. Главни задаци РФ у погледу одвраћања и спречавања војних сукоба су стварање услова за смањење ризика од коришћења информационо – комуникационих технологија у војно – политичке сврхе. РФ заостаје за водећим државама у развоју конкурентне информационе технологије, а овај јаз јача перцепцију о њеној стратешкој рањивости у сајбер простору. Сајбер одвраћање РФ састоји се од побољшане заштите њене критичне информационе инфраструктуре, припрема за изолацију руског сегмента интернета од глобалног интернета, појачаног надзора, забране анонимности корисника на РуНету и тежње да се увезена информационо и комуникациона технологија замени оном која је произведена у РФ. Елементи РФ делују у сајбер окружењу. Турунен и Кари наводе да поред сајбер шпијунаже усмерене на Демократску партију САД 2016. године, РФ је заслужна за упад у мејлове представника норвешког и финског парламента 2020. године, што је РФ активно негирала. РФ се доводи у везу са насилним епизодама попут оне око Бронзаног војника у Естонији 2004. године, Грузијског рата 2008. године и освајања Крима 2014. године. Свим наведеним сукобима претходио је сајбер напад на неки сегмент друштвено важног дела система у циљној држави. На основу ових неколико наведених примера може се проценити да РФ и њене власти имају добре могућности да контролишу сајбер активности у њеној сфери утицаја (Turunen & Kari, 2022).

Поред копненог, морског, ваздушног и свемирског простора, информациони простор је заузео битно место у широком спектру војних задатака у оружаним снагама великих сила. Оружане снаге РФ тренутно су развиле солидан систем дизајниран за ефикасно одвраћање, спречавање и решавање оружаних сукоба у информационом простору. Доктрина информационе безбедности РФ коју је одобрио председник РФ 9. септембра 2000. године, дала је основне приоритете за супротстављање овој претњи (Ministry of Defence Russian Federation, 2022).

Када правимо поређење између великих сила, САД и РФ, по питању погледа на информациони рат тада можемо констатовати да је поглед РФ доста обимнији од погледа САД и других држава Запада. Сајбер је термин коришћен на Западу, а РФ званично под информационим ратом обухвата „свеобухватни концепт који укључује сајбер шпијунажу, сајбер нападе и заштиту од сајбер напада и стратешке комуникације" (Bouwmeester, 2020, p.

[48] Валериј Васиљевич Герасимов, генерал армије, Начелник Генералштаба оружаних снага РФ, за *Краснаја звезда* новине Министарства одбране РФ, дана 4. марта 2019. године дао изјаву.

[49] Дмитриј Олегович Рогозин, политичар у РФ, дипломата, доктор наука, бивши генерални директор Роскосмоса, од 2011. до 2018. године био задужен за одбрамбену индустрију и свемир.

289). Током оружаног сукоба РФ и Грузије, информационе операције су биле спроведене од стране РФ. Развој информационих операција се убрзава, па су револуције, повезане са арапским пролећем, такође вратиле сећања на обојене револуције многима. У РФ као важни аутори по питањима информационог ратовања и размишљања о истом се наводе Панарин Игор, Дугин Александар, Лисичкин Владимир, Шелепин Александер, Чекинов Сергеј и Богданов Сергеј (Bouwmeester, 2020).

Теоретичари у Републици Србији сајбер напад дефинишу на следећи начин: сајбер напад начелно представља акте агресије унутар сајбер простора или кроз сајбер простор на информациони систем другог ентитета. Он је облик војног дејства еквивалентан примени оружане силе, па се може предузимати и у офанзивном и у дефанзивном смислу. Сајбер напади су везани за сајбер простор. Кључни садржај сајбер простора су подаци и информације у електронском облику, а фактор који га омогућава јесу информационо – комуникационе технологије. У сваком случају, сајбер напад је напад и стога је потребно анализирати шта оба појма значе у контексту примене информационих и комуникационих технологија у сајбер простору, у смислу информационе и сајбер безбедности, и у смислу војно – политичке и међународноправне примене. Војне дефиниције напада су усмерене на дејства војних система (рачунарских мрежа, рачунара и информација у њима) и начин и врсту дејства које напади остварују на те системе. У војном смислу, напади у сајбер простору се изводе применом средстава информационо – комуникационих технологија, применом рачунара и рачунарских мрежа, са циљем измене или уништавања информација у информационим системима или самих система. Оне у први план не истичу технику којом је изведен напад, већ његову војну намеру, којом се остварује војни допринос напада. Политичко – безбедносно дефинисање сајбер напада се односи више на процес сукоба (оружаног и неоружаног), а не на процес ратовања, који карактерише оружана примена силе. По њима, циљ напада је угрожавање безбедности у циљу остваривања ефеката на циљ напада. Њихова заједничка карактеристика је да се изводе у сајбер простору применом специфичних средстава. У техничком погледу, сајбер напад представља намерно угрожавање информационе безбедности неког система или информација садржаним у њему, предузето од стране неког ентитета, заобилажењем безбедносних механизама система, злоупотребом недостатака у систему техничке или нетехничке природе (Младеновић, 2016).

Када говоримо о сајбер нападима, тада мислимо на једну, у последњем периоду изузетно много присутну, субверзивну активност, која својим дејством нуди флексибилан алат за прикривено постизање низа циљева. У оружаним снагама САД, кибернетичка средства се често схватају као посебно поље деловања, док се у РФ тежи да ова област буде један елемент у низу других елемената у информационом ратовању. Није ретка појава да се сајбер напади користе за класичне шпијунске операције. Међутим, сајбер напади се могу користити и за долазак до (уз различите напоре) обликовања страних наратива. Као пример утицаја на стране наративе, износимо сајбер напад из 2016. године на Демократски национални комитет (енг. *Democratic National Committee*), чиме је омогућено прикупљање података који доприносе широј информативној кампањи. Интересантан је пример наводног лажног приписивања руског хаковања рачунара и телефона жена (супруга) војног особља САД према Исламској Држави „Сајбер Калифату", чиме се највероватније желела скренути пажња са РФ према Исламској Држави. Први познати масовни сајбер напад који се приписује РФ је био сајбер напад који је реализован ускраћивањем услуга за више ентитета у Естонији

у априлу и мају 2007. године. Наведени поступци су довели до гашења веб – сајтова који припадају парламенту и другим државним органима, политичким странкама, банкама, информационо – телекомуникационим компанијама и др. У периоду од 2015. године, велики број напада који се приписују актерима из РФ су идентификовани кроз две групе и то: АПТ[50]28 (познат и као *Fancy Bear, Sofacy Group* и *Pawn Storm*, између осталих) и АПТ29 (*Cozy Bear, Dukes*). Према извештају спољне обавештајне службе Естоније из 2018. године, група АПТ28 је била повезана са војном службом безбедности РФ, Главном управом (некада Главном обавештајном управом), док је друга група, АПТ29 повезана са службама безбедности РФ, Федералном службом безбедности и Спољна обавештајна служба. Обе групе (АПТ28, АПТ29) су означене као починиоци напада на Демократски национални комитет 2016. године као и на друге владине институције и у САД и Европској унији. Сајбер напад регистрован 2015. године, крајем године, на електричну мрежу у Украјини је приписан групама из РФ. *NotPetya* у јуну 2017. године, сајбер напад који је циљао на широко коришћени порески софтвер у Украјини и значајно пореметио финансије украјинске инфраструктуре, ставља се на терет војној служби безбедности РФ, Главној управи. Важно је нагласити да се понекад фирме за сајбер безбедност не слажу око приписивања извршиоца напада, што је онда у свету *дезинформација* и разумљиво поступање, те је неопходан опрез током оваквих истраживања, коришћења, односно злоупотребе оваквих догађаја. Можемо као пример да наведемо и постојање спекулација о томе да ли је проруска хактивистичка група *CyberBerkut* повремено у координацији са АПТ28 или је заиста испостава АПТ28 (Radin, Demus & Marcinek, 2020). Ове врсте активности предузимају и државни и недржавни актери. Када говоримо о другој категорији, категорији недржавних актера, врло често су они свесно или несвесно ангажовани од стране државних актера, најчешће припадника служби безбедности. Службе безбедности располажу техничким могућностима да чине овакве активности, али довођење у везу служби безбедности РФ (или било које службе безбедности у некој држави) са недозвољеним активностима оставља негативне последице на стратегијском нивоу, што би највишем државном руководству правило огромне проблеме. Како би избегла ову врсту проблема, за такве активности се врло често користе други актери, ентитети, који свесно или несвесно реализују ове активности. Важно је нагласити да када се ради о несвеном делу предузимања одређених сајбер активности, опет и у тој варијанти активности мора бити један број свесних лица (или најмање једна особа) која руководе свим активностима.

Вештачка интелигенција ће вероватно бити најбитнија технологија у унапређењу војних сајбер операција. Мајкл Роџерс (командант америчке сајбер команде – адмирал) изјавио је 2016. године да је ослањање само на људску интелигенцију у сајбер простору *стратегија губитка*. На такмичењу 2016. године (енг. *Defense Advanced Research Projects Agency 2016 Cyber Grand Challenge*), приказана је моћ сајбер алата са вештачком интелигенцијом. Учесници је требало да развију алгоритме вештачке интелигенције који би могли аутономно да открију, процене и закрпе софтверске рањивости, што је учињено у року од неколико секунди, уместо уобичајених месеци ангажовања. Овом приликом је регистрована брзина рада сајбер алата са вештачком интелигенцијом и способности

[50] АПТ (напредна претња – наводно хакери) акроним од следећих речи на енглеском језику: *APT – Advanced Persistent Threat.*

алгоритма да истовремено предузима радње напада и одбране. Овакве и њима сличне карактеристике пружају велике могућности и стварају огромну предност у евентуалном вођењу сајбер операција (Hoadley & Sayler, 2020).

Служби безбедности у Украјини је Стратегијом информационе безбедности у Украјини из 2021. године (можда и касно усвојена, прим. аут.) додељен велики број задатака, јер је РФ одређена као претња Украјини са својим информационим операцијама. Као одговор на претње РФ, овај документ је предвидео рестриктивне мере, санкције. Служба безбедности Украјине у оквиру својих надлежности врши праћење посебним методама и средствима домаћих и страних масовних медија и интернета. Овде се наглашавају и активности Службе безбедности Украјине, како у Украјини тако и у иностранству. У спровођењу ових мера је дозвољено ангажовање научно – истраживачких институција које пружају научно – аналитичку и стручну подршку (СТРАТЕГІЯ інформаційної безпеки, 2021). На основу наведеног, део послова додељених служби безбедности у поступцима информационе безбедности можемо сагледати кроз њихово ангажовање, првенствено на необавештајним активностима, како у земљи, тако и у иностранству, а ради смањења или неутралисања претњи по националну безбедност матичне државе. У Стратегији националне безбедности Републике Србије је одређено да „динамика глобалног развоја информационих технологија условиће даље интензивирање активности у сајбер простору чију безбедност ће, превасходно, угрожавати сајбер шпијунажа, напади на критичну инфраструктуру, неовлашћени продори у базе тајних података, као и ширење лажних вести и дезинформација путем друштвених мрежа.” (Стратегија националне безбедности Републике Србије, 2019, стр. 16). У Стратегији одбране Републике Србије одређено је да „Сајбер напади на објекте критичне инфраструктуре, високотехнолошки криминал, угрожавање информационо – комуникационих система, као и ширење лажних вести и дезинформација у оквиру концепта хибридног и информационог ратовања може се негативно одразити на функционисање елемената система одбране. Због тога је неопходно континуирано развијати технолошку и информациону заштиту елемената система одбране на свим нивоима организовања” (Стратегија одбране Републике Србије, 2019, стр. 22). Препознавањем информационог ратовања концептом ширења лажних вести и дезинформација, држава је дала правац снагама за супротстављање овој врсти претњи, па између осталих и службама безбедности. Овај проблем је велики за мале државе као што је Република Србија, али без обзира на огромна уложена средства у ове и сличне операције, против наведених претњи могуће је супротстављати се и то искључиво чињеницама (добијеним на време и у потпуности провереним – тачним) које ће обезбедити за то обучене структуре у држави, првенствено службе безбедности.

5.2. ПОЛИТИЧКЕ АКТИВНОСТИ И ОДВРАЋАЊЕ

Када говоримо о службама безбедности РФ, наглашавамо да оне врло блиско мешају концепте прикупљања обавештајних података, контраобавештајних података и тајне акције. Прве две наведене активности (обавештајне и контраобавештајне) првенствено су намењене прикупљању података битних за националну безбедност државе и наведене податке службе безбедности *претварају* у информације које служе за подршку доносиоцима одлука, а тајна акција представља углавном офанзивни део активности служби безбедности, односно извршење планова и политике доносилаца одлука. Службе безбедности РФ највише спроводе

тајне активности у три главне категорије и то *политичке активности* (операције), непријављене војне операције (*паравојне активности*) и операције атентата. Аналитичари из РФ тврде да САД већ воде политички рат против РФ. Званичници РФ сматрају да су *револуције у боји* које су се у почетку десиле у Киргистану, Грузији и Украјини, а касније у другим земљама, Сирији и Либији, манифестације ничег другог него западних тајних политичких операција. Лидери РФ на сличан начин анализирају и демонстрације које се спроводе против Путина, које су се десиле 2011–2012. године, као политички рат служби безбедности са Запада. Став руководства РФ је да се мора бранити од дезинформација које се пројектују на Западу, нпр. јавне тврдње да РФ шпијунира широм света, затим војних и паравојних активности, као што је наводна подршка РФ терористима у Чеченији, Сирији и Либији, као и операције атентата (Riehle, 2022).

Свака велика сила, па и РФ, настојала је да развија везе са странкама и лидерима, како у Европи, тако и у остатку света. Политичке везе са иностранством се ослањају првенствено на широку мрежу људи и организација, где првенствено спадају: одређени олигарси, као што је Константин Малофејев који је наводно подржавао сепаратистичке покрете у Украјини, па одређене групе, организације, удружења као што су *Ноћни вукови*, бајкерска група састављена од лица која су сумњиве криминалне прошлости и у блиским везама са председником РФ, Путином, затим Руска православна црква и сл. Заступљено је приближавање државама у којима је Православна црква доминантна, као и руским партијама које чине мањину у другим државама, али и придобијање политичких партија које не говоре руски. Странке које не заговарају позитивну политику према Северноатлантском савезу, а ни Европској унији, представљају интересантан део могућег деловања. У западној Европи, РФ је наводно подржала странке које подржавају неке спољнополитичке позиције РФ, попут Француске – Ле Пенов национални фронт и Немачке – Алтернатива за Немачку (Radin, Demus & Marcinek, 2020).

5.2.1. Појмовно одређење

Током совјетске ере, Комитет државне безбедности је спроводио тајне политичке операције означене као *активне мере*, хладноратовски концепт тајне политичке манипулације, а данас службе безбедности РФ више не користе синтагму *активне мере* већ уместо тог назива служба безбедности Спољна обавештајна служба има дирекцију са ознаком *МС* (рус. *мероприатиа содејстиа* – *МС* или срп. *мере подршке*) која у постхладноратовском периоду спроводи активности служби безбедности еквивалентне оном што је раније називано *активне мере*. У говору[51] одржаном 1992. године, дато је званично одређење *мера подршке* када је Примаков, директор руске службе безбедности изнео да: „мере подршке су оне мере које се спроводе како би се политика РФ, наше државе одвијала боље и ефикасније" (Riehle, 2022, p. 191). Затим је наводећи пример[52] кроз исти, директор

[51] Јевгениј Примаков, директор службе безбедности РФ, Спољне обавештајне службе поновио је велики део Митрохинове дефиниције о *активним мерама* (Riehle, 2022).

[52] Изјава Примакова, 1992. године, пример *мера подршке* службе безбедности: „Уколико нека држава заоштрава своју позицију и жели да спречи Г7 да пружи велику економску подршку реформама које се спроводе у РФ, онда се методе рада служби безбедности РФ могу и требају користити за довођење јавног мњења и лидера земаља Г7 до жеље једне од држава чланица да пребаци економски терет на рамена других и искористи ситуацију како би генерисала подршку за свој став по територијалном питању" (Riehle, 2022, p. 203, 204).

појаснио на шта је мислио. Дезинформација је намерна манипулација информацијама, представља тајну акцију и самим тим је у директној вези са службама безбедности. Политичар Томас Рид, изнео је веома интересантну констатацију. Наиме, према Риду, разумевање *сајбер операција* у XXI веку немогуће је уколико се прво не схвате операције служби безбедности у XX веку. Током хиљада и хиљада спроведених активних мера од стране Савеза Совјетских Социјалистичких Република према САД и европским савезницима, начин како се вршило супротстављање овим мерама, неопходно је разумети да би уопште могло да се супротстави операцијама дезинформација данас. Следећи ову Ридову констатацију навешћемо неколико примера кампања активних мера из доба XX века (*Табела 10*).

Табела 10. Неколико кампања *активних мера* из периода XX века.

Време	Кампање необавештајних активности руских служби безбедности
1977.	Фалсификовани документи америчког Стејт департмента који критикују египатско вођство
1977.	Књижица *200 година Америке*
1977 – 78.	Кампања против појачаног радијационог оружја
1979 – 80.	Кампања нуклеарних снага против учесника
1983 – 87.	Операција ИНФЕКЦИЈА – дезинформација вируса АИДС
1984.	*Реган значи рат!*
1985.	Подршка САД режиму апартхејда у Јужној Африци
1985.	Контра наратив у вези са САД испорукама житарица Савезу Совјетских Социјалистичких Република, унији
1985.	Америчка милитаризација свемира
1987.	Приче о *деловима за бебу* – дезинформације о киднаповању ради узимања органа

Извор: Riehle, 2022, p. 207, 208.

Рид за методе рада служби безбедности Савеза Совјетских Социјалистичких Република (РФ) у необавештајним активностима наводи да постоји континуитет руских намера током последњих 100 година. Крајем 2000. године, операције дезинформација су поново почеле да повећавају интензитет. Можемо да кажемо да се модерне кампање дезинформисања РФ фокусирају на одређен сталан број тема. Руководство РФ понавља ове теме током реализације информационих операција: није битно да ли се ради о отвореним или прикривеним операцијама. Ради се о следећим темама: Савез Совјетских Социјалистичких Република (наследник РФ) је играо водећу улогу у Другом светском рату, РФ је жртва, САД је извор нестабилности, Североатлантски савез је претња међународној безбедности, Европска унија је на ивици колапса (пандемија *COVID–19* омогућила је РФ да шири дезинформације у Европи). Према Џону Емерсону, информационе операције, како историјске тако и актуелне, показују образац активности служби безбедности који се може описати са четири слова енг. *D* и то: изобличити – *distort,* ометати – *disturb*, одбацити, одбити – *discard* и гађење/огадити – *disgust* (Riehle, 2022). Руска Федерација користи различите канале за ширење очигледно лажних или варљиво полуистинитих информација. Медијски канали РФ се често користе за дистрибуцију дезинформација, затим недозвољени интернет канали. Приликом реализације информационих операција користе се и отворени медијски канали који нису из РФ, као што су новине, платформе друштвених медија и новинарски форуми, како би се пласирали политички штетни подаци или припремиле информације које изазивају поделе и које изазивају конфузију.

Активне мере укључују пропаганду, медијску манипулацију, дезинформације, обману, коришћење фалсификата, атентате, финансирање екстремистичких и опозиционих група, ширење теорија завере и гласина, и сајбер нападе. Најважнији део сваке кампање активних мера је *политички утицај*. Политички утицај укључује коришћење агената и кооперативних контаката за директно промовисање руских интереса унутар политичких, обавештајних, дипломатских и војних структура земаља непријатеља. Ове особе (високо позициониране у друштву), које тајно раде у име РФ, називају се *агентима од утицаја*. *Активне мере* су облик асиметричног ратовања, где попут тероризма, такве методе представљају средство за наношење штете непријатељу без директне, званично признате употребе оружаних снага РФ (Sipher, 2018). Мада, сведоци смо да се током оружаних сукоба РФ и Украјине појављивао велики број припадника оружаних снага разних држава Североатлантског савеза који су наводно, пар дана раније напустили оружане снаге своје земље и отишли да учествују у оружаним сукобима на страни Украјине. Службе безбедности РФ професионализовале су алате за дезинформисање. Кампање дезинформација РФ су скоро превише бројне да би се документовале, као и од држава представника Запада.

Критична компонента активних мера је да имате агенте од утицаја који могу да пруже и увид, предузму радње на највишем нивоу за потребе службе безбедности, обезбеде приступ обавештајним подацима, а још боље, да имате контакте који могу да предузму активности у ваше име. Упркос фокусу на субверзији у активним мерама, совјетска и руска масивна улагања у обавештајне службе осигурала су готово сталну сигурну активност служби безбедности где је, пре кубанске ракетне кризе, прикупљање совјетских обавештајних података било далеко боље од оних што су спроводиле службе безбедности САД. Током XX века, совјетске и руске обавештајне службе су имале агенте у скоро свим кључним службама безбедности. Поред водећих служби безбедности, током Другог светског рата и Хладног рата, Русија је имала агенте у САД у Конгресу, Министарству одбране и Трезору Беле куће, док у истом периоду службе безбедности САД нису имале ни једног агента у Москви. На основу наведеног, није никакво чудо што се током Другог светског рата, скоро све што су прикупиле службе безбедности САД, посебно њена Канцеларија за стратешке услуге (енг. *Office of Strategic Services*), слило у Москву. Припадници служби безбедности РФ (тада Савеза Совјетских Социјалистичких Република) су тако ефикасно продрли у Атомски програм САД да су могли унакрсно да провере своје извештаје. Заиста, Савез Совјетских Социјалистичких Република је располагао са више података о пројектима на Менхетну, САД, него тадашњи Рузвелтов потпредседник. Тада је Савез Совјетских Социјалистичких Република имао агенте који су могли да усмеравају политику (агенте од утицаја) на кључним политичким позицијама. Навешћемо неколико агената за које се тврди да су били агенти Савеза Совјетских Социјалистичких Република: Хари Декстер Вајт, високи званичник Трезора и високи званичник САД на конференцији у Бретон Вудсу 1944. године, главни архитекта Међународног монетарног фонда и Светске банке; високи званичник Стејт департмента Алгер Хис, кључни играч на конференцији на Јалти и био је укључен у успостављање Уједињених нација. Спремност да се верује теоријама завере учинила је Русе стручњацима за преваре, али мање вештима у разумевању култура са другачијим начином размишљања (Sipher, 2018). Квалитетнија заштита, одбрана, одвраћање од асиметричних напада било које државе, односно њених служби безбедности следи уколико разумемо њихову историју и обрасце понашања (што је чувени амерички дипломата Џорџ Кенан

/*George Kennan/* саветовао сваког новог амбасадора САД у Москви, да узме историјске књиге о конкретном народу у више библиотека и да прочита).

Политичка служба безбедности је традиционална врста спољне службе безбедности која је постојала у различитим владама и у различитом временском периоду, а у РФ постоји до данас. Разлог постојања политичке службе безбедности је подршка приликом доношења како политичких, тако и спољнополитичких одлука. Александар Орлов је *дипломатску обавештајну службу* назвао најбитнијом службом и описао је као службу чија је сврха: „…да обавештава совјетску владу о тајним пословима између влада капиталистичких земаља и о правим намерама и планираним потезима сваке од њих, те владе према Савезу Совјетских Социјалистичких Република" (Riehle, 2022, p. 109). Када ово појмовно одређење упоредимо са оним које је три деценије касније дао Олег Гордијевски, пребег из Комитета државне безбедности, тврдећи да „информације обавештајне службе морају помоћи нашим властима да донесу оптималне спољнополитичке одлуке", није уочљива велика разлика. У Великој Британији званични представник Службе безбедности, Војног обавештајног одељка 5, изјавио је 2011. године да РФ дефинише политичку обавештајну службу као целину надлежну за стварање информације која би: „омогућила РФ да формулише политику која ће остварити максималну предност у светлу увида стечених из обавештајних података." За разлику од Велике Британије и њених служби безбедности, у САД, односно њеној Обавештајној заједници се то назива *предношћу одлуке* (Riehle, 2022, p. 103). Приоритети за службе безбедности РФ у вршењу политичких активности су следеће: „праћење развоја западног наоружања и одбрамбене политике, праћење планова оружаних снага САД према РФ, праћење дипломатске спољне политике САД и њених савезника према РФ, праћење спољне политике САД и њених савезника према блиском иностранству, развијање односа за везу са земљама Блиског истока и Јужне Азије, праћење унутрашње политичке ситуације у САД, задржавање Кине као блиског савезника, праћење Африке, Латинске Америке и Блиског истока" (Riehle, 2022, p. 111). Прикупљање политичких обавештајних података је првенствено усмерено на институције које доносе политичке одлуке на највишем државном нивоу у страним земљама, Министарство спољних послова (Riehle, 2022). Службе безбедности се баве доласком до обавештајних података о стратешким плановима и будућим способностима страних земаља, укључујући планове за изненадни напад и главне аспекте стратегије баш као у приоритетима Комитета државне безбедности из 1984. године, ради што правовременијег реаговања у превентивном смислу према политичком руководству РФ о могућим потезима које би држава, РФ, односно њено политичко руководство могло да предузме ради отклањања и/или ублажавања одређених последица које су наступиле или ће наступити. Можемо констатовати да службе безбедности имају задатак да прате актуелне теме, оне најбитније које су у вези са националним интересима РФ како би припремила своје политичке руководиоце за адекватне одговоре у јавности. Улога политичке обавештајне службе у операцијама које спроводе даље је илустрована у бази података коју је Савет за спољне односе[53] сакупио од преко 350 инцидената компјутерског упада и инцидената на рачунарској мрежи које је спонзорисала влада и који датирају из 2005. године, од којих се 84 инцидента приписују претњама који су повезани са Владом РФ, 129 инцидената се приписује

[53] *Council on Foreign Relation,* енг. – Савет за спољне послове (америчка, непрофитна организација), са седиштем у Њујорку и Вашингтону.

Кини, 36 Ирану, 28 Северној Кореји, док се 41 приписује другој држави (укупно 24 државе, различите). Циљ прикупљања политичких података служби безбедности је усмерен у прикупљање података одбрамбене, дипломатске, изборне и других владиних компјутерских система или лица који саветују владе (Riehle, 2022).

5.2.2. Карактеристичне политичке активности

Веома је важно разграничити прикупљање обавештајних података служби безбедности од тајне манипулације изборима, мада су у тесној вези, јер врло често сакупљање података претходи необавештајним активностима. Мешање у изборе, као што су у САД, Великој Британији и Шпанији, су важна мета политичке обавештајне службе РФ, јер се идентификују ставови нове администрације о РФ, појединци у новом тиму који би могли бити подложни руским погледима или стратегијама или који би могли да служе као агенти од утицаја, потенцијално штетне личне информације које би се могле користити ако РФ одлучи да дискредитује страног лидера или пуштања дезинформација о истом, као и разне теме и поделе које би се могле искористити у кампањама дезинформисања (Riehle, 2022).

Политичка обавештајна служба, са својим основним усмерењем рада на дипломатске субјекте, и даље има високи приоритет. Политичке активности служби безбедности имају за циљ добијање унутрашњих информација о политичким потезима страних земаља, посебно када је у питању РФ, али и савезници РФ и дипломатски партнери, као што су Кина, Венецуела, Сирија и Иран. Када говоримо о тајним методама које предузимају службе безбедности РФ у политичким активностима, доласка до сазнања, података, информација у министарствима спољних послова, ради се о следећим: регрутовање (рад) људи[54], приступ подацима пресретнутим из комуникационих система и електронске емисије[55] и прикупљање

---

[54] Рад са људима је доминантан метод који РФ користи у политичким активностима служби безбедности широм света. Службе безбедности РФ негују политичаре који не само да имају приступ осетљивим политичким информацијама, већ су и спремни да представе интересе РФ из угла како то одговара РФ. Следећи су карактеристични примери. У 2018. години, Бела Ковач, мађарски политичар, десничарска Јобик партија, ухапшен је и оптужен за шпијунажу у корист РФ. Званично је саопштено да је он наводно дао „информације о низу питања Европске уније у вези са РФ, укључујући детаље о енергетским преговорима, односима са Белорусијом, будућности европског банкарског сектора и могућем укидању виза Европске уније за Русију." Следећи је случај Николаја Малинова, бугарског политичара, ухапшеног 2019. године због наводног пружања информација о бугарском политичком одлучивању у вези са РФ и Европом. Наводно, један од докумената које је Малинов дао „оцртава кораке које је потребно предузети да би се у потпуности променила геополитичка оријентација Бугарске од Запада према Русији". Одговор РФ на ово хапшење је било да се радило о шпијунској фикцији коју спонзорише САД (Riehle, 2022, p. 116).

[55] Врло ретка појава је хватање припадника служби безбедности у чину блиског приступа, подацима пресретнутим из комуникационих система и електронске емисије у операцијама. Навешћемо неколико карактеристичних примера политичких активности служби безбедности, по овој методи рада. Наиме, 1999. године служба безбедности САД, Федерални истражни биро, ухапсила је Станислава Гусева, службеника амбасаде РФ који је ухваћен како сервисира предајник уграђен у шину столице у конференцијској сали Стејт департмента САД у Вашингтону. Након привођења Гусева, Федерални истражни биро је запленио сву опрему коју је Гусев користио за контролу уграђеног микрофона и протерао га из САД. Наведеним активностима, службе безбедности РФ су долазиле до низа политичких поверљивих података. Међутим, оно што је остало као интересантно констатовати је то да се нигде никада није појавила информација о начину постављања овог микрофона као и када је исти постављен. Приликом одржавања дипломатског скупа, Светски економски форум у Давосу, Швајцарска, 2019. године, Швајцарска полиција је ухапсила двојицу лица из РФ који су поседовали дипломатске пасоше РФ. Један од њих се представљао као водоинсталатер, а све се догодило у непосредној близини одржавања форума и у швајцарској штампи је описана активност двојице мушкараца како су се припремали за шпијунирање Светског економског форума електронским надгледањем самита. Следећи

података преко компјутера[56] (и/или мреже). Све ове активности спроводе припадници „првенствено две службе безбедности РФ и то Спољне обавештајне службе и војне службе безбедности Главне управе" (Riehle, 2022, p. 114). Без обзира на методу којом се служба безбедности РФ користи за долазак до података, пресретањем из комуникационих система и електронске емисије, прикупљање података од људи или рачунарске мреже, обавештајне активности РФ, усмерене су на министарства спољних послова по читавом свету са приоритетом праћења спољнополитичких институција.

Утицај емоција у одвраћању, како од стране одвраћача тако и одвраћаних, истраживао је Бијлсма (*Tom Bijlsma*), који констатује да је доношење одлука у стварности суштински одступило од претпоставки модела рационалног учесника. Утицаји на одвраћање су разни, па осим организационих утицаја, постоје и политички интереси, процеси, рутине и групно мишљење, где одвраћање може бити угрожено или чак пропасти због погрешне процене, перцепције на једној или обе стране кризе. Узроци таквих погрешних схватања су у хеуристици (базирано на искуству) и пристрасности (системске грешке као што су склоности или предрасуде). Хеуристика доступности се односи на менталне пречице. Стереотипизација и профилисање су облици ове хеуристике. Хеуристика афекта представља чињеницу да људи имају тенденцију да буду позитивнији, склони ономе што воле. Ако је идеја елегантније презентована, већа је могућност да ће се озбиљно размотрити, без обзира на то да ли или није логична. За стратегију одвраћања важан је сегмент како се лидери носе са ризиком. Свако различито процењује вредност губитака и добитака. Лакше је одвратити актера да започне инвазију него приморати некога да се повуче са територије коју је већ заузео. Лидери су склони да преузму више ризика како би задржали своје позиције, репутације и друге принадлежности које остварују својим местом рада, него да унапреде своје позиције, што је битно за динамику одвраћања. Бијлсма даје закључак да што су улози већи, то је већи ризик да будете ухваћени у психолошку замку (Bijlsma, 2021).

Развојем побуњеничке организације, политичка структура се развија како би комуницирала са *домородачким* становништвом, спољним присталицама и незадовољним члановима непријатеља. Вође у овом политичком штабу усмеравају акције војних операција

примери ангажовања служби безбедности РФ по овој методи рада, представљају два блиска приступа прикупљања података који су се догодили 2018. године, један у Норвешкој и један Холандији. Тада су припадници служби безбедности РФ ухваћени са техничком опремом за пресретање сигнала у или близу зграде парламента у Норвешкој и *Организације за забрану хемијског оружја,* Холандија (Riehle, 2022).

[56] Активности служби безбедности усмерене на рачунаре су посебно распрострањене у политичким активностима служби безбедности, првенствено против министарстава спољних послова широм света. У периоду 2015. и 2016. године, парламенти у Немачкој, Норвешкој и Турској пријавили су компјутерске упаде који потичу из РФ. У мају 2015. године регистрован је упад на интерни сервер Бундестага и губитак података. Званично саопштење Владе Немачке је било да је радник на одржавању електричне енергије предао планове зграде Бундестага официру војне службе безбедности РФ Главне управе (раније Главне обавештајне управе) који је радио под дипломатским надзором у амбасади РФ у Немачкој. Немачка влада је у мају 2020. године издала налог за хапшење Дмитрија Сергејевича Бадина због његове умешаности у хаковање немачког Бундестага 2015. године, а Влада САД је оптужила истог официра војне службе безбедности РФ, Главне управе 2018. године за упад у Демократски национални комитет 2016. године. Након упада у компјутерску мрежу Владе Норвешке 2016. године, Влада Норвешке је оптужила РФ за продор и крађу података из система електронске поште норвешког парламента у августу 2020. године. У 2018. години, норвешке власти су ухапсиле Михаила Бочкарева, из РФ, највероватније због спровођења активности блиског приступа подацима пресретнутим из комуникационих система и електронске емисије (Бочкарев је ухапшен због сумње да је користио лаптоп за надгледање *Wi–Fi* мреже у згради). Бочкареву је суђено пред норвешким судом, али је касније пуштен и дозвољено му је да се врати у РФ, а Влада РФ је демантовала те наводе (Riehle, 2022).

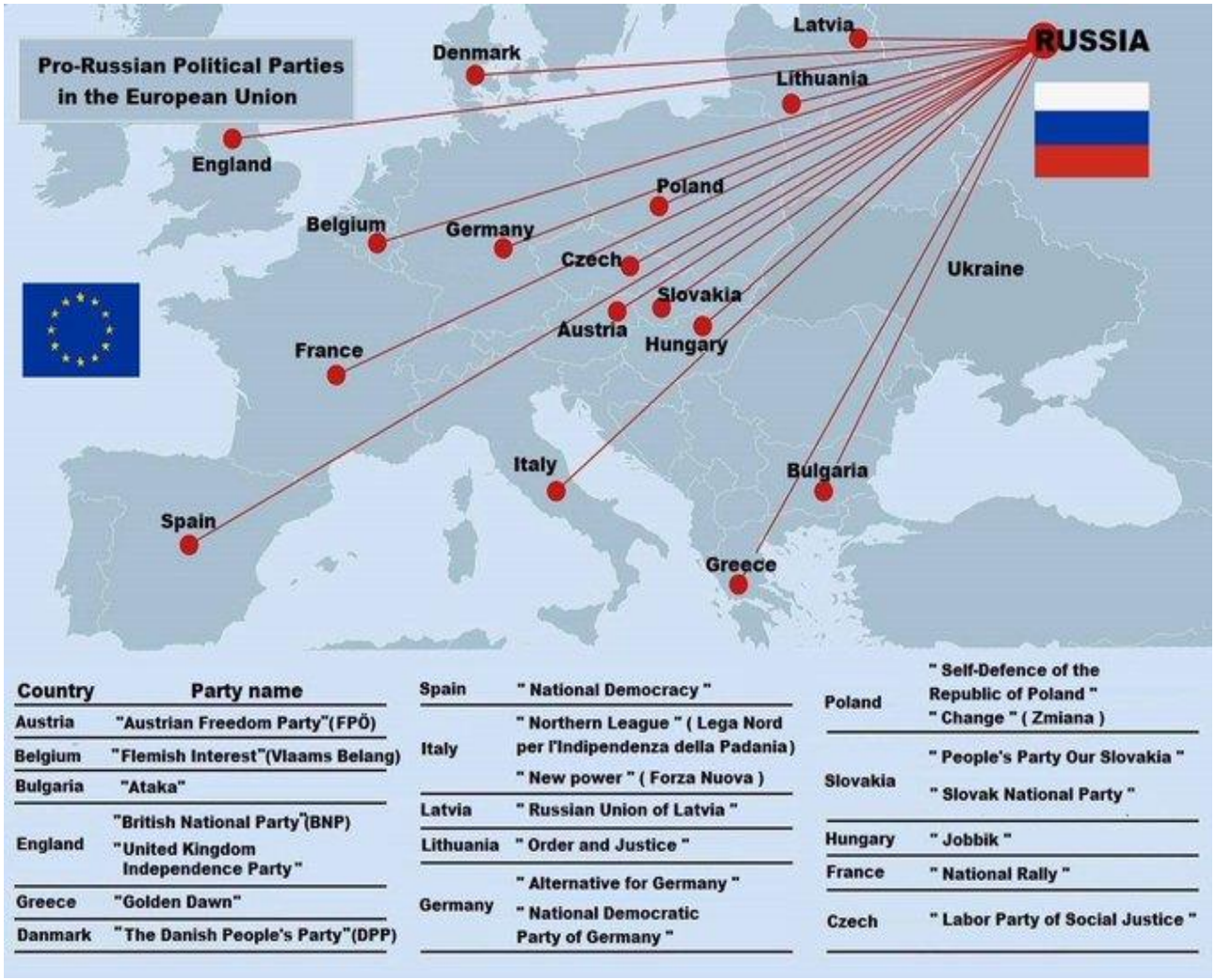
како би се осигурало да побуна остане усредсређена на постизање својих дугорочних циљева. Политички штаб усмерава побуњеничку организацију кроз низ политичких штабова нижег нивоа заснованих на географској локацији и демографији становништва. Политичком штабу потчињен је централни војни штаб устаничке организације (Training and Doctrine Command G2 Handbook No. 1.08, 2010).

За разумевање националног информационог окружења једне државе, неопходно је разумети културне вредности, интересе и проблеме локалног становништва, моралне и етичке вредности, карактеристике локалног законодавства, изазове везано за планирање операција у страном језичком окружењу. Поступање у ситуацијама када постоји реална претња да становништво стране државе може изгубити поверење у националну владу: тада САД (када је то у интересу владе или деловање у тотално супротном смеру – обарање владе) предузима информационе операције како би ојачали ауторитет владе. Када говоримо о *ојачању* ауторитета, тада мислимо на одређена средства за постизање овог циља. Средства нису универзалне природе, већ се предузимају након анализа сваке државе посебно, али начелно обухватају ангажовање дипломатије, информативних медија (медији, друштвене мреже), војне информационе операције (односи с јавношћу, војне информационе подршке операцијама, дезинформације и др.), економске инструменте утицаја (санкције, инвестиције и др.), комерцијална, културна и друга приватна ангажовања средстава. Како циљ оправдава средства, тако и у овом случају нема много избора око начина за постизање циљева. Методе убеђивања или принуде, убедљиве комуникације или присиле, затим телевизијско и радио емитовање, блокирање информативних средстава непријатељског, владиног или комерцијалног ресурса везаног за интернет и *укључивање кључних националних лидера – Key Leader Engagement* (Шариков, 2020).

Део теоретичара је као приоритет, односно примарни облик, задржао агентурни рад служби безбедности, док је други ешалон одмах иза овог рада, субверзивно деловање служби безбедности против неке земље, радом са *агентима од утицаја*. Агенти од утицаја испољавају изузетно штетна дејства на друштво и државу. Ради се о особама које су свесно ушле у агентурно деловање против своје државе против које предузимају субверзивне активности у име страних служби безбедности, држава. Ангажовање таквих агената се спроводи из убеђења, материјалне заинтересованости или посредством присиле. То су људи које скоро свакодневно гледамо у медијима, а вршећи своју професионалну дужност, они спроводе пропагандне активности у корист страног наредбодавца. Агенти од утицаја имају следеће задатке, да утичу на промену вредносне оријентације грађана у свим сегментима који су били присутни и цењени до сада (идентитета, религије, породичних вредности, културе, патриотизма, праведности, поштења, односа према породици, величање настраности, урушавање кључних националних институција – поготово безбедносног сектора са нагласком на службама безбедности, полицији, војсци) и многе друге системске активности, како би се извршило прекодирање базичних вредности и погледа на свет грађана једне државе (Деспотовић и Јевтовић, 2019). Када говоримо о средствима комуникације и медија, тада мислимо о најбржим начинима утицаја на ментални концепт неке нације, ревизије историје, традиције, културе и других прихваћених норми, чињеница, али морамо бити свесни да уређивачку политику медија спроводи неко ко је за то надлежан под *контролом* служби безбедности (говоримо о организацијама чија је специјалност извршавање тајне делатности, па је самим тим и присуство њених припадника и утицају на

уређивачку политику углавном скривено), како би обавезе биле реализоване у складу са интересима државе, политике (Деспотовић и Јевтовић, 2019).

У септембру 2022. године Центар за стратешке комуникације и информациону безбедност, Министарства културе и информационе политике Украјине (енг. *Stratcom Centre UA*) је објавио мапу (*Слика 6*) на којој је илустративно приказано у којим све државама Европске уније и преко којих политичких партија је наводно РФ до сада испољавала утицај – у 16 држава у Европи (Stratcom Centre UA, 2022). Већи део ових приближавања политичким партијама РФ су медији у периоду након ове објаве доводили у везу са службама безбедности РФ.



Слика 6. Проруске политичке партије у Европској унији.
Извор: Stratcom Centre UA, 2022.

Стратком центар је нагласио да РФ преко агената од утицаја, врбованих у наведеним партијама, спроводи свој утицај широм Европске уније. На овој мапи су приказане партије у следећим државама: Аустрија (Партија слободе), Белгија (Фламански интерес), Бугарска (Атака), Енглеска (Британска национална партија и Независна партија Уједињеног Краљевства), Грчка (Златна зора), Данска (Народна партија), Шпанија (Национална демократија), Италија (Северна лига и Нова снага), Летонија (Руска унија Летоније), Литванија (Ред и правда), Немачка (Алтернатива за Немачку и Национална демократска

партија Немачке), Пољска (Самоодбрана Републике Пољске и Промена), Словачка (Народна партија наше Словачке и Словачка национална партија), Мађарска (Јобик), Француска (Национални скуп) и Чешка (Радничка партија друштвене правде).

Савремени начин информационог утицаја који користе субјекти политичке комуникације је заправо скуп традиционалних облика како информационог тако и психолошког притиска, као и манипулације јавном свешћу и нових облика присутних услед развоја мрежних технологија, метода комуникације са сопственом и страном публиком. Појединци, групе или чак читави народи на такав начин лако постају жртве информационих клопки које су посебно припремљене за њих као посебне врсте информационог програма само за ту намену. Резултат таквог утицаја је више хаоса и нестабилности на планети и све више *обојених револуција*, егзодуса (то је прави термин, зато што лица морају избећи у другу државу да би добила статус избеглице[57]), бежања од сукоба, ратова, уопште разарања, губитак могућности да се буде господар чак и своје куће. Наведено се остварује ширењем психолошког, идеолошког и пропагандног утицаја на масе у интересу доминације појединих актера, како у виртуелним тако и у реалним политичким и другим односима (Мельникова, 2020).

Улога емоција у теорији одвраћања је велика, често и пресудна. Емоције нису само последице поступака нападнуте стране, већ се појављују и кроз изазивача, нападача. Када се једном покрену, специфичне емоције утичу на когнитивне процесе и деловања или неделовања. Емоције су одговорне за различите врсте предрасуда, што утиче на перцепцију. Емоције у различитим конфигурацијама обликују процесе доношења одлука. Емоције су, у ствари, од суштинског значаја за сваку одлуку, рационалну или не. Емоције треба схватити као један од битнијих сегмената у одвраћању и истраживања одвраћања би требала да буду посвећена и овом феномену. Тако би се омогућило разумевање узрочних механизама који објашњавају како се перципирају претње одвраћања код другачијих култура. Тако да за овај део утицаја на одвраћање можемо да кажемо да представља један ток емоционалног живота који поседује одређене утицаје, а ти утицаји су насилне природе, насилна средства (Zilincik & Duyvesteyn, 2021). Данашњи спектар претњи нуди нове могућности за приказ моћи, као и нове рањивости алата за пројекцију моћи. Вишеструкост учесника и понекад непрозирна природа претњи додатно компликује одвраћање, што у комбинацији са новим увидима из психолошких истраживања, како наводе многи аутори, отежава одвраћање, и неопходно је да буде допуњено другим приступима који укључују присилу, принудност и убеђивање. Неопходно је схватити да постоје и други, тзв. незападни приступи одвраћању, те да у некима поступања могу бити суштински различита (Osinga & Sweijs, 2021). У времену када све већи број људи све мање и мање учи, чита, образује се и уопште констатује чињенице (тачне податке), а светом владају пропаганда, фејк вести, лажи, обмана, дубоке лажи, и када се трајање неке вести мери у секундама, колико пажња данашњег човека може држати концентрисаног, оно што после свега тога остаје или можемо да кажемо да је на врху

[57] Конвенција о статусу избеглица, у Глави I, Члан 1. дефинише израз *избеглица* где се у једном делу појмовног одређења наводи следеће: „…нађе изван земље чије држављанство оно има и које не жели или, због тога страха, неће да тражи заштиту те земље; или које, ако нема држављанства, а налази се изван земље у којој је имало своје стално место боравка услед таквих догађаја, не може или, због страха, не жели да се у њу врати" (Уредба о ратификацији конвенције о статусу избеглица са завршним актом конференције опуномоћеника уједињених нација о статусу избеглица, 1960, Члан 1).

параметара за одлучивање у одвраћању, представља управо *емоција* којом се води обичан, мали човек, па до државника, владара (или обрнуто).

Унутрашњи политички атентати, у раном периоду Савеза Совјетских Социјалистичких Република, решавани су кроз чувене *тројке* (радило се о тројним вансудским екипама особља служби безбедности) које су у том периоду биле овлашћене да наређују погубљења. Постоје подаци да је касније било довољно једноставно натерати некога да нестане. Овај вид злочина је био редак, јер су биле доступне друге методе[58] за неутрализацију оних који су прешли политичку линију. У постхладноратовском периоду, вероватно због интензивнијих активности Запада, овај вид активности је повећан. Када говоримо о лицима[59] која су прешла црвену линију по процени РФ, тада најчешће говоримо о водећим опозиционим личностима, антикорупцијским активистима, критички настројеним новинарима и сл. Нигде није дефинисано конкретно шта је то што баш представља моменат када је неопходно реализовати атентат према службама безбедности РФ, али оно што је дефинитивно одређено и јасно у овим активностима, првенствено политичким активностима, јесте да постоје активности које су блажег ранга, испод оних које би покренуле операцију атентата (види *Табелу 11*). Како расте интензитет политичке активности коју сагледава служба безбедности, тако се редни број повећава и приближава моменту када ће бити донешена одлука о ликвидацији (Riehle, 2022).

Табела 11. Процене Владе РФ за акцију против унутрашњих опозиционара.

	Ниво опозиционе активности	Одговор државе – владе РФ
5	Постаните симбол опозиције и привуците друге да вас следе	Хапшења и осуде на продужени затвор, али размислите о атентату
4	Водите опозициону групу; стећи истакнутост као опозиционар или критички новинар	Хапшење и казна, продужени затвор
3	Придружити се опозиционој групи или активно учествовати у опозиционим активностима; писати критички материјал о Путиновом режиму	Ухапсити и задржати кратко време у притвору
2	Учествујте у опозиционим дискусијама онлајн или лично	Покрените праћење
1	Прочитајте опозициони материјал	Нема тренутне реакције

Извор: Riehle, 2022, p. 219.

Осим убистава унутрашњих политичких опозиционара и других издајника, за блаже форме преступа (које не заслужују хапшење и сл.) могу се предузети и предузимају се појачана праћења комуникационих канала. Није искључена и контраобавештајна операција за ову врсту лица, првенствено ради регрутовања појединца као двоструког агента или агента провокатора. Можемо констатовати да се атентати разматрају само у најекстремнијим случајевима. Вође антируских милитантних или терористичких организација су за РФ

[58] Осуђивање лица на нехумане услове у поправним, радним логорима или у неке од психијатријских болница. Без обзира што се не ради о директном атентату, али врло често се радило о поступку који је у суштини, посредно представљао смртну казну.

[59] Међу њима су лица попут либералног политичара Бориса Њемцова, новинарке Ане Политковске и опозиционог лидера Алексеја Навањног. Важно је нагласити да смрт великог броја новинара који су убијени у РФ, нема директну везу са службама безбедности, односно да њихова смрт често није долазила директно од централне власти, већ вероватно по налогу појединих моћних елита или криминалних вођа – на пример, када се новинар превише приближио истини у вези са злочиначким или корумпираним подухватом, мада и ту је врло тешко искључити присуство служби безбедности, напротив.

оправдане мете атентата где год да се налазе, што се води под интерним операцијама војних[60] атентата (Riehle, 2022).

Када говоримо о спољашњим атентатима, атентати РФ у иностранству су мање присутни, него унутар РФ, зато што су потенцијално политички штетнији за РФ и морају се спроводити опрезно. По дефиницији, атентати које спонзорише држава ван државних граница су тајне операције. Учешће Владе РФ у операцијама атентата изван РФ би требало, углавном, да остане скривено. Влада РФ је 2006. године усвојила нови федерални закон о борби против тероризма којим се дозвољавају вансудска убиства. Наиме, у овом закону у члану 22. предвиђено је *Законито наношење штете* (рус. *Статья 22. Правомерное причинение вреда*) где је децидно прописано да: „Лишавање живота лица које изврши терористички акт, као и наношење штете здрављу или имовини тог лица или другим законом заштићеним интересима појединца, друштва или државе у сузбијању терористичког акта или спровођење других мера за борбу против тероризма радњама које су прописане или дозвољене законодавством РФ, законито је" (О противодействии терроризму, 2006). За спољна политичка убиства, РФ процењује последице ако буде ухваћена у атентату на некога у иностранству и важно је нагласити да су она ретка. Један од карактеристичних примера у Хладном рату било је убиство Георгија Маркова, антикомунисте, које је реализовано убодом кишобрана са отровним врхом у сред Лондона 1978. године, а ставља се на терет бугарској влади уз помоћ и савет службе безбедности, Комитета државне безбедности. У постхладноратовском периоду, спољна политичка убиства РФ, за која у сваком случају постоје сумње у околности су следећа: Борис Березовски 2013. године преминуо под сумњивим околностима у Уједињеном Краљевству, наводно је његова смрт самоубиство (Riehle, 2022). Неколико сумњивих покушаја убистава у САД, можда може да се доведе у везу са РФ, као што је напад на америчког безбедносног аналитичара Пола Џојала у фебруару 2007. године, убрзо након јавног прозивања Путина за умешаност у атентат на пребега из службе безбедности РФ, Федералне службе безбедности, Александра Литвињенка. У САД, у новинама *Њујорк тајмс*, октобра 2019. године, наведено је следеће: јединица 29155 која се налази у саставу војне службе безбедности РФ, Главне управе (некада Главне обавештајне управе) је највероватније била ангажована у неколико необавештајних активности, тајних операција. У чланку у овим новинама су доведени у везу официри војне службе безбедности Главна управа из Јединице 29155 са догађајима везаним за покушај убиства Емилијана Гебрева 2015. године, затим наводним покушајем државног удара, како су га окарактерисали представници Владе Републике Црне Горе 2016. године и наводним покушајем убиства председника Владе Републике Црне Горе (вероватно због позива за приступање Североатлантском савезу) и покушајем атентата на Сергеја Скрипала 2018. године у Уједињеном Краљевству. Активност припадника ове јединице није била ништа мања ни током преузимања Крима 2014. године, као и у дестабилизацији Молдавије исте године. Иза сваког од ових поступака стоји одређени политички циљ, наравно у складу са циљевима спољне политике државе (Riehle, 2022).

[60] Државне оружане снаге РФ су гађале одређене вође милитаната ради реализације атентата, третирајући их као легитимне војне мете (од 1996. до 2017. године, преко 60 чеченских и дагестанских милитантних вођа били су мета у атентатима на Северном Кавказу).

5.2.3. Руско мешање у изборе у САД 2016. године

Руска Федерација, као и њен совјетски претходник, има историју вођења утицаја фокусираних на председничке изборе у САД које су користиле припаднике служби безбедности, агенте и штампу за омаловажавање кандидата који се доживљавају као непријатељски расположени према РФ. Службе безбедности РФ спровеле су сајбер операције против циљева повезаних са америчким председничким изборима одржаним 2016. године, укључујући мете повезане са обе главне политичке странке у САД (Sipher, 2018).

Када говоримо о председничким изборима спроведеним у САД 2016. године, службе безбедности у САД напомињу да су активности утицаја наводно РФ према изборима у САД били вишеструки. Та вишеструкост је обухватала читав низ предузиманих активности и то почев од ангажовања служби безбедности, друштвених медија – енг. *trolls*, наводно медијске организације под покровитељством РФ као што је енг. *Russia Today* – Русија Данас, и неруске организације, као што је енг. *VikiLeaks* (Radin, Demus & Marcinek, 2020).

Дезинформација (рус. *Dezinformatsiya*) је пракса обмањивања противника (и других) са лажним информацијама, обично за успоравање, деградирање или заустављање ефективних одговора повезане активности, као што су саботаже, сајбер напади или ограничени војни упад РФ. Дезинформације су пре свега пратећа мера, а не самостална тактика. На пример, РФ је манипулацијом избора у САД 2016. године користила комбинацију дезинформација, компјутерског хаковања и сајбер напада на гласачке мреже у САД и друге уређаје. Дезинформације су једна од непријатељских мера (Connable et al., 2020).

Руководство Конгреса САД је потврдило процену обавештајне заједнице САД. Наиме, према извештају америчког специјалног саветника Роберта Милера (*Robert Mueller*), Обавештајна заједница (енг. *Intelligence community*), као и накнадне истраге од стране обавештајних одбора Представничког дома и Сената су констатовале следеће: „РФ је уложила опсежне напоре да се умеша у председничке изборе у САД 2016. године" (Bowen, 2021, p. 18). Према Милеру и истрагама Сенатског комитета за обавештајне послове, Јединице 26165 и 74455 су биле директно одговорне за операцију (енг. *Hack – and – leak*) РФ. Јединица 26165 је хаковала мејлове и системе Демократског Конгресног одбора за кампању, Демократског националног комитета и председничке кампање Хилари Клинтон. Јединица 74455 је одговорна за објављивање десетина хиљада украдених докумената путем разних фиктивних онлајн особа и у координацији са Викиликсом (енг. *WikiLeaks*). Почевши од марта 2016. године, војна служба безбедности Главне управе је наводно спровела опсежну кампању лажних превара и малвера како би хаковала мреже и налоге е – поште кампање. Војна служба безбедности Главна управа (некада Главна обавештајна управа) је украла десетине хиљада докумената и мејлова са ових налога најмање до септембра 2016. године, користећи бројне псеудониме на друштвеним мрежама, укључујући енг. *DCLeaks* и *Guccifer 2.0*. Јединица 74455 је координирала објављивање украдених докумената како би се умешала у Изборе 2016. године. Наводно је војна служба безбедности РФ Главна управа (раније Главна обавештајна управа) користила ове псеудониме да комуницира са Викиликсом за преношење украдених докумената ради објаве 2016. године (Bowen, 2021).

Све наведено нема смисла уколико систем безбедности нема одговарајуће мере које предлаже и/или предузима на побољшању контраобавештајне и безбедносне заштите у држави. По завршеним председничким изборима 2016. године, Министарство правде САД подигло је три оптужнице против укупно 21 службеника војне службе безбедности Главне

управе (некада Главне обавештајне управе) за злонамерне сајбер активности, укључујући мешање у председничке изборе у САД 2016. године, кампање дезинформисања, информисања и увредљиве сајбер операције које су нанеле губитке од више милијарди долара. Важно је нагласити да су у овим оптужницама подигнутим 2018. године детаљно наведени припадници јединица, идентификоване су њихове јединице, детаљно описане операције, активности и методе које користи војна служба безбедности Главне управе (некада Главне обавештајне управе). Влада САД је увела санкције 21 официру војне службе безбедности РФ Главне управе за исте и додатне злонамерне активности у иностранству. У медијским извештајима се наводи да су службе безбедности САД предузимале и контрамере у последњих неколико година и то операције којим су ометале приступ интернету са наводне руске *фарме тролова* и вршиле упаде и надзор руске електроенергетске мреже. Овакве акције могу имати за циљ да дају сигнал упозорења за евентуалне трошкове, ако би РФ наставила да спроводи сајбер операције. Медији су наводили да се чини да Влада САД такође повећава своју комуникацију и координацију са актерима из приватног сектора како би се супротставила сајбер активностима РФ. У оптужници из октобра 2020. године, званичници америчког Министарства правде су се захвалили компанијама „*Google,* укључујући *Threat Analysis Group – TAG; Cisco,* укључујући *Talos Intelligence Group; Facebook* и *Twitter*, за помоћ коју су пружили у овој истрази" (Bowen, 2021, p. 21). Поред тога, важно је напоменути да су медијски извештаји сугерисали да је америчка сајбер команда блиско координисала са приватним компанијама у операцијама против дезинформација и сајбер операција продукта РФ (Bowen, 2021).

Операције прикупљања података и дезинформације су две различите категорије активности и спроводе се одвојено, али понекад и кооперативно. Према оптужници Министарства правде САД из 2018. године, официри војне службе безбедности РФ, Главне управе, оптужени су као одговорна лица за хаковање и цурење информација које су наводно утицале на ток избора у САД 2016. године. Хакерски део операције је спроведен од стране једног елемента који је другачији од другог дела елемента који је коришћен за цурење, прикупљање података. Када се говори о цурењу података (ради се о примени активности најчешће обавештајног карактера) тада се мисли на спровођење операција којим се могу прикупити подаци интересантни за потребе реализације активности служби безбедности, а путем нормалног, редовног политичког прикупљања података, затим коришћењем метода пресретнутих из комуникационих система и електронске емисије, прикупљања података од људи или компјутерски заснованих. Такви подаци се преводе у информације које се затим уступају појединцу, групи, јединици која реализује тајну акцију (мада исти или део података могу бити искоришћени уколико има елемената угрожавања националне безбедности или су битни за државу да буду искоришћени за доношење одлука руководства државе, под условом да не угрожавају тајне операције, необавештајне активности), односно која врши операционализацију задатака неопходних за планирање, организовање и спровођење тајних акција, необавештајних активности. Јединица 26165 је елемент војне службе безбедности РФ, Главне управе, и представља јединицу која сакупља податке пресретнуте из комуникационих система и електронске емисије, као и информације за различите кориснике (и друге јединице Главне управе одговорне за тајне операције). Јединица 26165 је означена као главни осумњичени за продор у мејлове повезане са председничком изборном кампањом Хилари Клинтон и Демократским националним комитетом 2016. године. Из ове јединице су

ухапшени официри Главне управе у Холандији док су наводно спроводили тајну операцију блиског приступа методом сакупљања података пресретнутих из комуникационих система и електронске емисије према лицима и средствима из Организације за забрану хемијског оружја у Хагу 2018. године. У медијима је саопштено да је наводно Јединица 26165 била ангажована и у операцијама компјутерског упада у Холандски одбор за безбедност 2015. године, а све ради објављивања извештаја о паду авиона на лету број 17 Малезијског авиопревозника и резултата о допингу спортиста из РФ од стране Светске антидопинг агенције 2018. године. Избори у САД 2016. године су били главна вест о утицају необавештајних активности РФ према САД. За ове активности је наводно одговорна Јединица 74455. Ради се о јединици која је смештена у московском предграђу, а саставни је део војне службе безбедности РФ, Главна управа. Према доступним сазнањима, ова јединица је одговорна за акције саботаже и акције дезинформација. Када би се правила одређена компарација ове јединице (74455) и јединице за инфилтрацију диверзионо – обавештајних група, можемо да кажемо да оно што је група за инфилтрацију диверзионо – обавештајних група по својој методи рада, то Јединица 74455 представља у компјутерско – мрежном еквиваленту. Јединица 74455 спроводи саботаже и тајне операције (необавештајне активности) иза противничких линија. Када говоримо о карактеру задатака и описа послова које обавља Јединица 74455, она је поред доласка до података, тзв. цурења[61] података, ангажована и на деструктивним[62] задацима. Битно је нагласити да припадници ове јединице углавном своје задатке реализују на даљину, а не и из непосредне близине као Јединица 26165 (Riehle, 2022).

Руска Федерација политичке активности служби безбедности схвата као највиши приоритет, чак их сматра и битнијим од одбрамбених, економских и обавештајних активности других земаља. Влада РФ сматра да уколико се могу разумети политички покретачи других земаља, РФ се може заштитити и у свим другим сегментима. Руски и совјетски лидери ретко су били толерантни према служби безбедности која им даје информације које су у супротности са њиховим чврстим политичким ставовима. Стаљин је захтевао истраге о изворима података који су давали нетачне податке, а Горбачов је покушао да прекине тај тренд захтевајући објективније информације ослобођене хладноратовских политичких претпоставки. Председник Комитета државне безбедности у време Горбачова, Владимир Крјучков, био је умешан у заверу 1991. године за смену Горбачова са власти. Подаци који данас продиру до председника РФ не одражавају нужно стварност, колико одражавају председникове личне жеље и намере (Riehle, 2022).

Да ово није крај репресије служби безбедности великих сила у случају Трамп, не само према другим државама већ и према својим држављанима, поготово опозиционим у САД, па чак и према бившим председницима САД, говори репресија која се спроводи од стране службе безбедности, Федералног истражног бироа и других служби безбедности према Доналду Трампу 2022. године. Наведено су спроводиле применом (или можда злоупотребом) овлашћења служби безбедности, и то: претресима, привођењима великог броја Трампових

[61] Операција цурења информација из 2016. године, председнички избори у САД.
[62] Деструктивни компјутерски напади, укључујући оне који су утицали на критичне елементе инфраструктуре у Украјини и напад *Олимпијски разарач* који је циљао Олимпијске игре у Сеулу у Јужној Кореји 2018. године (Riehle, 2022).

сарадника и слично, што је већина медија окарактерисала као освету због објављивања онога што је наводно син председника САД, Хантер Бајден, радио у Украјини и на другим местима, супротно важећим прописима и законима.

Велика је неизвесност у којој мери је субверзија РФ ефикасна. Када се говори о војним (паравојним) активностима у Украјини, ефекти напора РФ су очигледни, видљиви. Када говоримо о другој врсти утицаја, политичких, информационих и економских активности, можемо констатовати да је ова област слабије разумљива, односно схваћена (нпр. неизвесна ефикасност наводног мешања РФ у председничке изборе у САД 2016. године то јасно показује). Док се не схвате стварни ефекти субверзије, тешко је осмислити рационалан пропорционалан одговор. Приликом оваквих одлучивања мора бити присутан податак да сваки одговор на субверзију почињену од оне друге стране, производи додатне трошкове по буџет државе. Вредновање учинка субверзије РФ је од суштинског значаја да би се утврдило да ли да се наведени трошкови прихвате или не. Таква евалуација може бити тешка, али је могућа кроз даље проучавање и анализу друштвених медија и истраживања извршених анкета. Брзо реаговање на критичне догађаје чини велики проблем за даље негирање својих радњи. Приписивање чињења одређеног догађаја некој страни, ограничава крајњу ефикасност планиране субверзивне активности (нпр. ако је кампања коју води Агенција за интернет истраживање брзо окарактерисана као активност РФ, ефикасност њених порука би вероватно била умањена). Уколико се не располаже одређеним подацима тј. информацијама битним за спречавање или умањење дејства одређене субверзивне активности у потребно време (ради превентивног деловања), и та активност нерасполагања битним подацима може бити готово једнако штетна, као и недостатак приписивања субверзије другој страни (Radin, Demus & Marcinek, 2020). Овде сагледавамо место и улогу служби безбедности у примени све три врсте активности – обавештајне, контраобавештајне и необавештајне – без којих је немогуће квалитетно спровести одређену субверзивну активност или јој се супротставити. Правовременим тајним и квалитетним планирањем, припремама и реализовањем необавештајне активности, постиже се пуни ефекат у реализацији једне необавештајне активности, док на супротној страни (државе која се напада), уколико службе безбедности квалитетно обављају своје послове, могу правовремено да дођу до података које могу искористити да умање или чак спрече реализацију нежељених дејстава. Морамо нагласити да је за ове врсте активности јако битно време када се дошло до одређених података везаних за необавештајне активности, а истовремено и шта је то што се предузима по питањима тих сазнања. Поседовати податак, а не предузети адекватан одговор или меру је скоро исто вредно као и да служба безбедности тј. њени политички руководиоци уопште и нису успели да дођу до тог податка, информације.

5.3. ОДВРАЋАЊЕ И ЕКОНОМСКЕ АКТИВНОСТИ

Веома је битно нагласити да нико не сме да порекне утицај служби безбедности на економске активности и просперитет једне или више држава. Тако се не може пореći водећа улога коју је у распаду Савеза Совјетских Социјалистичких Република, једне тако велике силе, одиграо најмоћнији директор Централне обавештајне агенције (после Алена Далеса */Allen Dulles/* или у истом или вишем рангу, није толико битно за ово истраживање), Вилијам Кејси (*William J. Casey*), који је лично формулисао и спровео доктрину о економском уништењу Савеза Совјетских Социјалистичких Република о чијем исходу је сувишно било

шта даље коментарисати (Шаваев & Лекарев, 2003). У медијима се данас наводи велики број малверзација економске природе од стране агената америчке Централне обавештајне агенције и британског Војног обавештајног одељка 6, који су наводно ангажовали велики број лица ради подривања економске стабилности РФ (између осталих већ наведених, помиње се и Алексеј Навални коме је наводно задатке издавао извесни *Brauder* из Велике Британије, оснивач фонда *Hermitage Capitol*, затим бивши премијер РФ Михаил Касјанов, чија је помоћница имала британски, можда и амерички пасош, снимљени у кревету и пуштен снимак на телевизијском каналу *НТВ Москва*, човек са надимком *Миша 2%* и други индикативни подаци изнети у медијима). Низом усмерених поступака од стране служби безбедности наставили су оно што је још Кејси поставио као својеврсну доктрину, али операција *Потрес – Quake* изгледа да и даље није затворена од стране наведених служби безбедности (Факултет за дипломатију и безбедност, 2016).

Пензионисани официр руске Спољне обавештајне службе Сергеј Воронцов (*Sergey Vorontsov*) дефинише економску активност служби безбедности као: „Примање информација о свим областима економске активности страних политичких актера и њиховим економским и финансијским структурама, условима на тржишту валута, сировинама, племенитим металима и др., које су од интереса за РФ, као и организовање и управљање предузећима усмереним ка стварању профитабилне околности за руске спољноекономске интересе, за развијање ефективне спољноекономске сарадње, закључивање профитабилних трговинско – економских послова и споразума, итд.” (Riehle, 2022, p. 156). Пошто је нафта тако значајан елемент економије РФ, руска незаконита активност на тржишту нафте је посебно истакнута, наводно уз подршку служби безбедности.

Службе безбедности РФ своје економске активности, а које се односе на економски аспект националне безбедности државе, могу да поделе у три области деловања: *научно – технолошка* област, *економско – обавештајна* област *и економско – контраобавештајна* област. У последњих неколико деценија за РФ *научно – технолошка* област интересовања за активности служби безбедности (оно што је Орлов назвао *индустријска активност служби безбедности*) представља прикупљање података о страним технолошким производима за подршку развоју науке и технологије у РФ. Ова врста активности служби безбедности РФ врло често захтева тајно заобилажење санкција или страних закона који забрањују извоз технологија у РФ, посебно циљајући опрему или енг. *Know – how* за подршку војној или безбедносној индустрији РФ. Овде препознајемо једно велико ангажовање служби безбедности кроз необавештајне активности у реализацији обавеза државе у овој области, јер службе безбедности само обавештајним и контраобавештајним активностима нису у могућности да реализују овакав вид задатака, међутим, необавештајне активности су директно зависне првенствено од обавештајних и од контраобавештајних активности. *Економска обавештајна* област обухвата прикупљање података о економским активностима страних влада, економским и финансијским организацијама, тржиштима сировина, метала и валуте, који су приоритети за РФ (Riehle, 2022). У овој области, службе безбедности и друге институције подршке које стварају повољне услове за РФ да постигне своје спољноекономске визије, циљају на економске активности страних земаља које негативно утичу на РФ. *Економска контраобавештајна* област је механизам којим Влада РФ користи економске полуге интерно да би спречила финасијску и друге врсте економских штета држави. Економска контраобавештајна област деловања служби безбедности има два

примарна правца, да спречи долазак до података о економским информацијама у иностранству, па чак и када је та информација она коју већина земаља отворено објављује, и коришћењем економских полуга за кажњавање оних за које је процењено да би требали бити кажњени од руководства државе и/или службе безбедности (Riehle, 2022). Можемо слободно констатовати да је општи циљ свих ових области деловања служби безбедности јачање економске и војне снаге РФ. Важно је након угрубог сагледавања ове три области интересовања служби безбедности констатовати да је већ одавно напуштен концепт ангажовања држава, а поготово великих сила, да раде поштено и по закону, већ оно што је одмах након Другог светског рата констатовала администрација САД, да више нема поштене, фер игре са Истоком подразумева првенствено ангажовање служби безбедности у необавештајним активностима ради спровођења задатка добијених од највишег државног руководства.

Како би се сагледала деловања нечега што је било у прошлости и могућности онога што можемо очекивати у будућности у односу на субверзивне активности РФ, поделили смо могуће одговоре на две заједничке категорије и то одвраћање *порицањем* и одвраћање *казном*. *Одвраћање порицањем* обухвата радње које чине субверзије РФ мање вероватним за успех или се ради о скупој активности. Одвраћање порицањем је синоним за одбрану. У САД, одвраћање порицањем се односи на политике које су осмишљене да смање рањивост САД као и њених савезника, па и партнера за читав низ субверзивних активности РФ. То се односи на побољшање сајбер одбране, смањење зависности од енергената из РФ, јачање безбедности граница у земљама које су суседне РФ и пружање медијске обуке како би се смањила осетљивост људи на информационим активностима. Главна предност одвраћања порицањем је у томе што је мање вероватно да оспори интересе РФ па представља мањи ризик од изазивања нежељених одговора РФ. Улагање у одбрамбене активности вероватно не може да доведе само до елиминације свих слабости које са собом носе субверзивне активности. Програмима за побољшање одбране, а тиме и одвраћања порицањем, треба извршити процену на основу најмање пет фактора и то: смањење ризика, постизање других друштвено пожељних циљева, трошкови предложеног програма, усклађеност између предложеног програма и западне норме и вредности, обликовање одлучивања РФ. Сагледавајући субверзије РФ, *одвраћање казном* се састоји од радњи или претњи које се намећу као директни трошкови за РФ који би били већи од потенцијалних добитака постигнутих субверзијом која би била спроведена. Велики је број примера који укључују економске санкције које су САД и друге државе увеле РФ након анексије Крима према РФ, затим дипломатске санкције које су уследиле после тровања бивших припадника служби безбедности (двојног агента) РФ и Уједињеног краљевства, Сергеја Скрипала у Лондону, затим оптужнице против припадника служби безбедности РФ. Више фактора доприноси ефикасности и пожељности одвраћања казном, и то брзина и извесност атрибуције субверзије РФ, тежина казне, јасноћа у описивању услова казне, схватање казни од стране РФ, трошкови у вези са казнама. Наглашена је потреба за ефикаснијим развојем казне која би имала ефекта на одвраћање. На пример, након што је РФ заузела Крим почетком марта 2014. године, САД су увеле санкције као одговор на нарушавање *суверенитета и територијалног интегритета Украјине*. Након што је РФ предузела даље акције за анексију Крима, САД су проширила своје санкције. Тако је Председник САД, Барак Обама, у марту 2014. године довео у директну везу санкције које је САД увела на предузете акције РФ и то незаконит

референдум на Криму, нелегитимни потез РФ да припоје Крим, опасни ризици од ескалације како би САД наметнуле додатне трошкове РФ. САД и Европска унија у јулу и септембру су санкционисале физичка и правна лица РФ замрзавањем имовине РФ у САД, забрањујући путовања, блокирајући приступ западном капиталу, спречавајући извоз енергетске технологије и блокирање увоза у Крим. Оптужнице САД против појединаца из 2018. године повезане са Агенцијом за истраживање интернета и војном службом безбедности Главне управе биле су јасно повезане са њиховим криминалним активностима 2016. године током спровођења председничких избора у САД. Санкције компанији *Русал* могле би значајно да утичу на извоз алуминијума РФ. Кључни текући изазов за политику САД је да развије довољно ефикасне одговоре на субверзију РФ и да се осигура да су ови одговори заиста повезани са РФ и да неће предузимати субверзивне акције у будућности (Radin, Demus & Marcinek, 2020).

Како РФ има све већи утицај у светској економији и другим активностима на планети, лако је уочити све веће притиске од Запада са циљем смањивања утицаја РФ. Обарање авиона из Малезије који је летео изнад Украјине је искоришћено да се РФ искључи из Г8 (Групе осам најразвијенијих индустријских држава). Економске активности према РФ су настављене кроз различите санкције. Долази до смањивања цена нафте и других активности ради смањивања утицаја РФ. Руска Федерација је стекла велико страхопоштовање Запада у периоду од 2008. године, након *блиц крига* изведеног у Грузији, затим заузимања Крима 2014. године, па активностима у Сирији 2015. године, чиме је РФ дала до знања свим светским актерима да се ради о озбиљној великој сили која би требало да се пита за многе спољнополитичке теме.

5.3.1. Карактеристике и обележја економских активности

Инструменти моћи једне државе су дужи временски период били сагледавани и примењивани у светлу моћи дипломатије, информација, војне и економске моћи. У литератури која се бави одвраћањем, војни и дипломатски инструменти су били доминантни у прошлости. Актуелна збивања на планети указују да је дошло до огромних промена у овом пољу и да савремени стратешки теоретичари говоре о концептима хибридних претњи, неограниченом ратовању, активностима сиве зоне, информационом и финансијском ратовању, културном, идеолошком, политичком, виртуелном и сајбер рату. Неопходно је нагласити финансијске инструменте, употребу служби безбедности, правне инструменте, културу и знање, како бисмо у потпуности схватили методологију, начин спровођења и вршења моћи на геополитичкој сцени данашњице. Економска моћ, као инструмент, може се регистровати у различитим облицима, од договорне, консензуалне (давањем зајмова) до принудне (увођења санкција). Обухвата оба пасивна елемента, државне макро – економске карактеристике као и активне мере (замрзавање имовине, инвестиција и др.). Међународни економски односи, као што су заједничка тржишта, са својим механизмима и процедурама на месту, обухватали би друго гледиште ове моћи (Ducheine & Pijpers, 2021).

Велика је листа спроведених бројних агресивних, злонамерних и широких сајбер операција од стране војне службе безбедности Главне управе (некада Главне обавештајне управе) против више мета. Службеници Главне управе су наводно 2015. године хаковали Бундестаг, немачки национални парламент. Немачка је издала налог за хапшење официра Главне управе Дмитрија Бадина, који је оптужени припадник Јединице 26165 и оптужен од

стране САД за његову улогу мешања у изборе у САД 2016. године. У октобру 2020. године, Европска унија и Уједињено Краљевство санкционисале су Бадина и шефа војне службе безбедности, Главне управе, Игора Костјукова због хаковања. У САД током истог периода, октобар 2020. године, Министарство правде је оптужило 6 официра Главне управе за неколико сајбер напада, где је у оптужници Јединица 74455 идентификована као енг. *Sandworm*. Наводи се да је одговорна за вишеструке сајбер нападе и то: „нападе на електричну инфраструктуру Украјине, Министарство финансија и државни трезор из 2017. године, па покушај хаковања и пропуштања података усмерених на председника Француске, е – поруке (енг. *emails*) Емануела Макрона и мешање у француске председничке изборе, напад малвера 2017. године, познатији као *NotPetya*, који је заразио рачунаре широм света и проузроковао штету од 10 милијарди долара, хакерски напад 2018. године на Зимске олимпијске игре у Пјонгјангу у Јужној Кореји, у којем су хакери војне службе безбедности РФ, Главне управе (некада Главне обавештајне управе) покушавајући да се преруше као севернокорејски хакери користили злонамерни софтвер да ометају церемонију отварања, затим хакерска кампања 2018. године против истраге Велике Британије, Европе и Организације за забрану хемијског оружја о нападу нервним агенсом на Сергеја Скрипала и његове ћерке, па у периоду од 2018. до 2019. године сајбер кампања против грузијских медијских компанија и грузијског парламента" (Bowen, 2021, p. 17).

Сајбер напади против Украјине имали су значајне економске ефекте на Украјину, укључујући последице напада рансомвером (енг. *ransomware*) и замену технологије услед сајбер напада на електричну мрежу. Ситуација у Украјини је показала да, иако су сајбер напади у Украјини били све јачи, напади су остали испод одређеног прага који би покренуо међународну интервенцију, „сива зона". Економске активности регистроване од јануара 2017. године у Украјини биле су ограничене на физичку штету узроковану *деструктивним малвером* и све већом употребом софтвера рансомвер од стране државних актера. Штета настала нападима *деструктивних малвера* од јануара 2017. године, учинила је рачунаре и друге уређаје неупотребљивим. Главни трошкови се састоје од замене оштећених рачунара и др. уређаја као и ангажовања фирми за сајбер безбедност како би се обезбедило уклањање преосталог злонамерног софтвера и да се онемогући даља рањивост. Два напада на електроенергетску мрежу и деструктивни ефекти *NotPetya* изазвали су значајне трошкове (оштећено је око 17.000 рачунара широм света, а око 60% се налазило у Украјини). Рансомвер је врста напада коју све чешће користе државни актери. У 2017. години државни актери су стајали иза неколико напада рансомвера. Док је *WannaCry* привукао значајну пажњу медија, други напади попут *NotPetya, XData, PSCrypt* и *BadRabbit,* такође су били на мети рачунара у Украјини. Други сајбер актери, као што је Северна Кореја, користили су рансомвер за генерисање прихода. Занимљиво је да су се алати који циљају на Украјину маскирали као рансомвер, али у ствари нису имали за циљ финансијску добит. Државни актери су користили рансомвер да би одвратили и скренули пажњу са својих правих мета (Baezner, 2018).

Економија РФ се ослања на спољну трговину да би преживела, а њен бруто друштвени производ је уско повезан са тржиштима нафте и гаса. С обзиром на ову зависност од трговине, један од спољнополитичких приоритета РФ је стварање повољног спољног окружења које би омогућило економији РФ да напредује (Riehle, 2022). Економија је важна тема националне безбедности, према којој РФ усмерава рад и ангажовање својих служби

безбедности. Руска Федерација користи тајне методе, а понекад и криминалне, тамо где не може да се ангажује легално, као на пример у куповини многих добара које држава не може да набави због међународних санкција. Стране службе безбедности, па и оне из РФ, користе различите методе да одреде и регрутују изворе економских или технолошких података. Понекад наведене методе подсећају на класичне активности припадника службе безбедности у раду са људским изворима података. Међутим, ради се о циљаном ангажовању припадника службе безбедности на приближавању и вербовању, регрутовању човека са позиционирањем и приступом циљаним економским подацима, информацијама или другим људима са положајем и приступом како економским, тако и научно – технолошким подацима битним за националну безбедност државе. Први годишњи извештај Конгресу о економском прикупљању и индустријској шпијунажи 1995. године идентификовао је *методе* које су користили припадници службе безбедности (*методе људских извора, техничке методе и корпоративне методе, за прикупљање економских и научних и технолошких информација*). *Методе људских извора* које су коришћене 1995. године у економским и научно – технолошким активностима службе безбедности су: „регрутовање агената, прихватање волонтера, задатак запослених у страним фирмама, лов на главе, запошљавање запослених код конкурената, надзор и тајни улазак (у хотелске собе, канцеларије и друге просторије), регрутовање емиграната; позивање емиграната да се врате кући, задатак страних студената, извлачење током међународних конференција и сајмова, дебрифинг посетилаца страних земаља, ангажовање брокера информација и консултаната.” Упоредимо ово са 2019. годином када су коришћене следеће методе у нападу службе безбедности РФ на технологије у САД: „искоришћавању односа, експлоатацији стручњака, искоришћавање инсајдерског приступа, подношење резимеа и надзор” (Riehle, 2022, p. 143). Следе *методе техничке природе* или *техничке методе* прикупљања података и/или предузимања одређених радњи на другим системима техничке природе ради спровођења необавештајних активности. Ради се о компјутерским упадима, обавештајним подацима о страној техничкој активности и прикупљању отвореног кода, укључујући тајно прикупљање јавно доступних информација како би се прикрило порекло истраживања и др. У области економске контраобавештајне службе унутар саме РФ укључено је праћење компјутерске мреже, али службе безбедности РФ и даље у први план стављају човека који делује у интересу Владе РФ. У извештају Конгресу САД 1995. године, следеће методе су апострофиране као примењиване у економским активностима службе безбедности РФ: хаковање, пресретања комуникација, базе отвореног кода, тајно прикупљање материјала отвореног кода. Наспрам овога, у 2019. години су коришћене следеће методе у нападу службе безбедности РФ на технологије у САД: експлоатација сајбер операција и експлоатација безбедносног протокола. Руска Федерација такође користи *корпоративне методе* за предузимање економских активности службе безбедности. Ове методе обухватају прикупљање економских и научно – технолошких обавештајних података, као што су искоришћавање капиталних инвестиција, спонзорисање страних истраживачких активности, позивање страних компанија да успоставе истраживачке центре и подршку образовним институцијама у РФ, оснивање заједничких фирми или предлагање корпоративних спајања и аквизиција и др. У последњих пар година, РФ истиче потребу за истраживањем вештачке интелигенције и аутономних система од стране иностраних фирми (из Кине, Јужне Кореје, сада актуелна потрага за формирањем центара из Турске за производњу дронова и др. држава) за које настоји да дођу у РФ и отворе

истраживачке центре. Формирањем тих центара, те фирме су донеле и своју технологију за производњу у РФ, па су затим спонзорисале едукацију за истраживаче из РФ и развиле заједничке истраживачке пројекте које РФ није могла до сада самостално да реализује. Мада, када се сва ова ангажовања наведу, делују као легалан начин успостављања економске сарадње. Овакве активности су у најмању руку праћене контраобавештајним надзором од стране служби безбедности РФ усмерених према гостујућим страним истраживачима који су стационирани у РФ ради регрутовања извора података унутар стране компаније. Интеграција отворених корпоративних активности са тајним операцијама за обавештајне и контраобавештајне активности је класичан начин рада служби безбедности у РФ. Врло је важно нагласити да је тешко или можда немогуће раздвојити економске активности служби безбедности од обавештајних и контраобавештајних активности. У 1995. години, у извештају припремљеном за Конгрес САД, наведене су следеће методе које су примењиване од стране служби безбедности: стране владе користе организације приватног сектора, лажне компаније и заједничка улагања, корпоративна спајања и аквизиције, уговори о корпоративној технологији, спонзорство истраживачких активности. За разлику од наведених, у 2019. години су коришћене следеће методе у активностима служби безбедности РФ усмерених према технологијама у САД: потрага за технологијама, експлоатација пословних делатности, покушај аквизиције, економске дезинформације, експлоатација ланца снабдевања. Економске и технолошке активности служби безбедности РФ показују коришћење великог броја ових метода, од људских извора података до техничке и корпоративне методе ангажовања служби безбедности. Применом ових и сличних метода служби безбедности РФ, исте се користе против страних циљева, као и против политичких опозиционара унутар саме РФ (Riehle, 2022).

У наредном делу истраживања, наведен је део јединица укључених у активности служби безбедности РФ. Јединица 26165 је основана као 85. главни центар за специјалне службе током Хладног рата, одговорна за криптографију војне службе безбедности, често називана АПТ28 или *Fancy Bear*. Влада САД је ову јединицу идентификовала као одговорну за хаковање Демократског Конгресног одбора за кампању, Демократског националног комитета и председничке кампање Хилари Клинтон. Јединица 74455 створена је да помогне у подршци и проширењу сајбер способности војне службе безбедности Главне управе (некада Главне обавештајне управе). Јединица 74455 је такође позната као Главни центар за специјалне технологије и у извештајима медија и Владе САД је обично називају пешчаним црвом. Ову сајбер јединицу доводе у везу са неким од најбезобразнијих сајбер операција РФ, као што је напад *NotPetya* у Украјини 2017. године. Дана 19. октобра 2020. године, Министарство правде САД открило је оптужнице против шест чланова Јединице 74455 за нападе на различите међународне мете. Јединица 54777 позната и као 72. центар за специјалне услуге, наводно је одговорна за психолошке операције војне службе безбедности Главне управе (некада Главне обавештајне управе). Сајбер јединицама војне службе безбедности Главне управе даје подршку и деловање на тактичком нивоу путем вођења електронског ратовања и психолошких операција. Медији повезују Јединицу 54777 са онлајн кампањама дезинформација, посебно у вези са пандемијом *COVID – 19* (Bowen, 2021).

5.3.2. Циљани економски поремећај

Модерна, високотехнолошка друштва су подложна концепту комплексног тероризма и нападу нерегуларних снага. Зависност од електронских мрежа, концентрисање критичне имовине на малим локацијама, посматрајући географски, могу представљати уносне мете за терористе или друга лица која имају за циљ економски поремећај. Како би имале ефективну моћ у пропадајућим државама, многе од нерегуларних снага виде тероризам или други вид чињења недозвољених делатности као ефикасан начин сукоба. Податак је да је Ал Каида уложила само 500.000 америчких долара у напад који је спроведен 2001. године док је само економска процењена штета за Владу САД износила више од 125 милијарди долара одштете и трошкова опоравка. Након тога, за све значајније терористичке нападе није било потребно ни неколико хиљада долара. У САД, електрична мрежа би могла бити главна мета нерегуларних снага, терориста и других непозвних лица. Нестанак струје 14. августа 2003. године оставио је 50 милиона људи око Великих језера без струје на одређени период и коштао је економију земље око једну милијарду долара. У иностранству, амерички интереси, па самим тим и рањивост приступа, могу се фокусирати на нафту. Инфраструктура за производњу нафте има критичне тачке на Блиском истоку које услед евентуалног квара (намерног или не) у инфраструктури током одређеног временског периода могу направити велике проблеме многим светским економијама. Један пример је Саудијска Арабија где је арапско постројење за производњу нафте у Абкаику у једном тренутку управљало са око две трећине дневне производње сирове нафте Саудијске Арабије. У Нигерији се побуњеничке фракције, влада и нерегуларне снаге боре око приступа и контроле над нафтом тог региона из делте Нигера. Велики број убистава и отмица и уништавања инфраструктуре, значајно ометају нигеријску производњу нафте. Циљеви и методе напада ће највероватније наставити да се фокусирају на економске циљеве као што је комерцијална авијација, енергетски сектор или масовни транспорт, што би имало и друштвено дестабилизујући ефекат. Пошто мере безбедносне заштите отежавају напад на такве циљеве (штите их читави системи безбедности), због сложености таквих задатака, могу бити одабране и друге мете као што су велики јавни скупови или симболичне локације споменика или значајних грађевина и слично, што у датом геополитичком моменту погодује прављењу што већег медијског и економског поремећаја (Training and Doctrine Command G2 Handbook No. 1.08, 2010).

Када говоримо о РФ, тада не говоримо само о великој сили, већ о великој економској сили. Такав економски утицај долази највише од великог присуства РФ на енергетском тржишту и то кроз државне фирме *Газпром*, *Росњефт* и *Лукоил*. У протеклом периоду, како Европска унија тако и САД су нагласиле потребу да се диверзификују од снабдевача РФ, јер наведено виде као претњу од утицаја економских активности РФ. Чињеница је да РФ представља поузданог снабдевача енергентима, али је истина и да се ове полуге моћи могу искористити ради присиле других субјеката. У 2006. години, када је влада Литваније одлучила да прода Рафинерију *Мазеикиаи* пољској компанији Пољски нафтни концерн *Орлен* уместо руским понуђачима (*Лукоил* и Тјуменска нафтна компанија – *Британски Петролеум*; Тјуменска нафтна компанија – *Британски Петролеум* купљена од стране енергетске компаније *Росњефт*), РФ је прекинула испоруку нафте нафтоводима према тој компанији. Проблем цурења је наводно изазван несрећом (званично образложење званичника РФ), док власти Литваније тврде да је пријава несреће била покушај да се саботира договор о контроли над тржиштем нафте Литваније. Наводно је РФ у Бугарској ангажована да

прошири своју контролу над енергетским тржиштем и да одврати диверзификацију. Део теоретичара тврди да су економска улагања РФ првенствено усмерена на прикупљање обавештајних података или у друге политичке сврхе, али не може се искључити примарни циљ РФ да одржи своје присуство и економске интересе у региону. Када говоримо о Немачкој, најчешће помињан у медијима је Герхард Шредер, неформални утицај бившег канцелара Немачке на владу своје државе, који је именован за председника одбора заједничког немачко – руског гасовода Северни ток и председника одбора *Росњефта*. Кроз само неколико примера видимо колико је моћно оруђе у рукама РФ економска активност и колико РФ, па и службе безбедности, користе ове полуге моћи у решавању задатака добијених од политичког и војног руководства РФ. Утицај РФ је много већи на државе у које се извозе енергенти из РФ и чине значајан део укупног енергентског потенцијала државе, док када постоје и други алтернативни добављачи, ту је утицај РФ преко економских активности доста ослабљен (Radin, Demus & Marcinek, 2020). Безбедносно је интересантан и догађај везан за наводну хаварију (пуцање цеви) на *Северном току 1* и на *Североном току 2* у Балтичком мору у исто време у непосредној близини острва Борнхолм, Данска. Наиме, оператери у гасоводу су 26. септембра 2022. године приметили пад притиска на гасоводу, да би 28. септембра након већег броја подводних експлозија велики број западних медија објавио како је РФ учинила саботажу на гасоводу (без ваљаних доказа), док је РФ демантовала наведено (и оптужила Велику Британију), а у делу медија објављена су сазнања да су на порталу Флајтрадар24 (енг. *Flightradar24)* регистровани налети у више наврата (наводно 1, 2. и 3. септембра, па 22/23. и 25/26. септембра) војних хеликоптера оружаних снага САД изнад те локације (непосредна близина острва Борнхолм у Балтичком мору) где се догодио инцидент. Доналд Трамп је 28. септембра 2022. године на својој платформи *Друштвене истине* (енг. *Truth Social*) објавио снимак из фебруара 2022. године у којем је његов наследник на месту председника САД, Џозеф Бајден, рекао новинарима да „ако РФ изврши инвазију (мисли на Украјину, прим. аут.), више неће бити *Северног тока 2*, ми ћемо томе стати на крај, обећавам вам, моћи ћемо то да урадимо". Када се овакве појаве сагледавају, јако је битно у чијем је интересу да се нешто тако догоди где би, уколико се ради о саботажи, економска активност била та која је пресудна у овим и сличним догађајима. Руска Федерација и Немачка реално немају економски интерес да саботирају своју материјалну и другу врсту добити тј. интереса. Да би се реализовала евентуална саботажа овог типа, неопходна је посебна опрема којом располаже јако мали број држава на планети. Руска Федерација је оптужила Велику Британију као одговорну, а познати новинари су оптужили САД и Норвешку за саботажу.

Одвраћање казном: САД би можда могле боље да одврате РФ уколико би јасније повезивала конкретну казну са конкретним субверзивним активностима. Казне субверзије РФ треба запретити и спроводити постепено, на начин да се са сваким додатним елементом јасно доведе у везу казна са идентификованом субверзивном акцијом РФ. Да би одређена казна испољила утицај и довела до промене понашања руководства РФ, казна мора бити довољно значајна или смислена да убеди ове актере у одређено поступање. Најчешће нема ефекта гонити починиоце субверзивних радњи, јер обично су недоступни надлежним органима, док друга велика сила вероватно неће никада прихватити да испоручи своје припаднике служби безбедности или њихове извршиоце одређених активности уколико је она носилац тих активности. Уколико је мало вероватно да ће одређена казна испољити

утицај на циљну групу – ентитет, можда вреди размислити о развоју неких нових санкција које се могу додати или уклонити у зависности од мање или више кооперативног понашања РФ. Казне субверзије РФ треба да се фокусирају посебно на прикривене или порицане активности РФ, али и на отворене економске активности или информационе активности које не би штетиле САД, првенствено. Сигурно је да отворене активности, нпр. *Русија Данас* или енергетске инвестиције РФ могу штетно деловати по интересе САД. Када се врши примена овог вида кажњавања, долазимо до констатације да наведено олакшава РФ да поверују и да убеде друге да САД су против свега што је од РФ у стилу Хладног рата. Примена казни, санкционисање отворених активности доводи у опасност паралелне активности САД у РФ или њеним суседима, као што су америчке друштвене медијске компаније, друга пословна улагања и фондације САД (нпр. *Eurasia Foundation,* 2019; *Petroff*, 2017). Могући пут за реаговање према субверзији РФ од стране САД је интензивирање напора САД да подметне РФ као да је она нешто реализовала. Међутим, појачана америчка субверзија може довести до нежељене ескалације од стране РФ као и до евентуалне војне акције против САД, њених савезника или другим партнерима (Radin, Demus & Marcinek, 2020).

Мала је граница између политичке и економске активности, односно можда је прецизније одредити да је врло често политичка активност везана за економску активност и обрнуто. Као пример бисмо могли навести ситуацију када политичка активност исцрпи своје могућности и сматра да ће применом присиле у другој области активности (нпр. економској) успети да оствари своје углавном спољнополитичке циљеве. Наиме, у случају односа Украјине и РФ свима је познато покретање питања дугова које Украјина има према РФ првенствено што се тиче гаса. Нису само дугови ти који чине могућност, начин, метод присиле политичког режима једне државе, овде конкретно режима у Украјини, већ ту се појављивало и појављује се у одређеним моментима битним за политички опстанак, одређене одлуке, неке власти и подизање цене гаса или других енергената. У Украјини је у јануару 2006. године цена гаса подигнута пет пута. Овај поступак је према већини аналитичара довео до утицаја на ток избора у марту 2006. године у Украјини када је на власт дошао проруски орјентисан политички представник на место премијера, Виктор Јанукович. Следећи пример је поступак руске фирме *Газпром* која је уочи састанка министара спољних послова држава чланица Северноатлантског савеза, 2–3. децембра 2008. године, где је главна тема требала да буде улазак Украјине и Грузије у Северноатлантски савез, покренула питање дуга за гас од стране Украјине. Украјина нафту и гас добија из руских извора преко нафтовода и гасовода, мада представља и транзитну област према Европи и другим државама. Своје интересе РФ види у Украјини и свима је јасно да РФ неће дозволити да ова држава постане члан било каквог војно – политичког савеза или да се учлани у неку економску организацију, а да нису прво заштићени интереси РФ (Кусовац, 2021).

Дана 12. августа 2022. године председник Републике Србије је гостујући у емисији у 21 час на телевизијском каналу *Прва* у Београду изјавио да је Република Србија разорена активностима страних служби безбедности и нагласио тај сегмент разарања у економском смислу. Као пример за то је председник навео ангажовање у необавештајним активностима страних служби безбедности (не наводећи о којим се тачно службама ради) приликом организовања протеста ради раскида уговора са фирмом *Рио тинто* која је требала да експлоатише литијум на територији Западне Србије, околина Лознице (тачније дуж реке Јадар, у близини села Горње и Доње Недељице, Рађевина, Цикота, Ступница и др.) и да је то

чист губитак за државу, Републику Србију. Председник је закључио да је то намерна активност страних служби безбедности ради слабљења економске моћи Републике Србије.

5.4. ПРОПАГАНДНЕ АКТИВНОСТИ И ОДВРАЋАЊЕ

5.4.1. Пропаганда као средство

Пропаганда (*propaganda* – латинска реч са значењем ширити се), односи се на активности за отворено ширење ставова, чињеница, аргумената и других материјала за формирање одређеног јавног мњења, популаризације и за ширење одређених идеја у масовној свести који се спроводе углавном путем медија. Развој нових информационо – телекомуникационих система утицао је на промену традиционалних метода пропаганде у спољној политици, а разлог је употреба нових информационо – телекомуникационих система у комуникацији на међународном нивоу. Како би било формирано одређено мишљење међу неком циљном групом или друштвом у целини, усмеравајући пажњу публике на било које питање, користи се тактика *пуњења информацијама*[63] – циљна, свесна, намерна, планска пласирања конкретних, компромитујућих (најчешће лажних) информација (када постају дезинформације) или објављивање познатих чињеница, али из одређеног угла посматрано, које су повољне за извор да буду објављене. Данас, најспецифичнију улогу у простору информационо – телекомуникационих система имају *лажни* (енг. *fake*, што у преводу има значење „лажни", „патка", „фалсификат"), посебно пројектовани, осмишљени (лажни) докази о фиктивним догађајима. Лажни су веома разноврсни (псеудовести, лажне фотографије, лажни налози, лажни сајтови са лажним коментарима непостојећих стручњака, итд). Разлика између лажних и пуњења информацијама је у присуству визуелног материјала у виду фотографије или видео снимка снимљеног на сасвим другом месту. Пример су фотографије које се користе у медијима, осмишљене да илуструју догађаје који су се одиграли на једном месту, а заправо снимљени на сасвим другом месту. Тако је британски енг. *The Times,* 5. маја 2017. године објавио чланак *Путинова пропаганда*, где се наводи мешање руских специјалних служби и руских хакера у изборни процес у Француској и САД (преко новинских агенција *Русија данас* и *Спутњик*). Француски лист *Монд* је 14. јула 2017. године објавио чланак извесног Б. Виткина под називом *Лажни репортер, прави убица*, највеће француске новине, које су ширили неосноване вести, правећи спекулације о наводној умешаности руских дипломата и обавештајних службеника у масакре противника шефа Чеченске Републике Р. А. Кадирова у иностранству. У РФ такође, употреба *језика мржње* и етикетирања карактеристична је и присутна поготово у руском медијском дискурсу, према Украјини где су постали познати термини *бандеровци, хунта, евромајдан* и други слични изрази. Једна врста информационе агресије је *тролловање,* које представља циљану провокацију на друштвеним мрежама. Често је конципирано тако да се састоји од јавних

[63] Пример оваквог *пуњења информацијама* може се приписати следећем: филм (који је приказала корпорација енг. *British Broadcasting Corporation*) *Трећи светски рат: на командном месту*, према чијој радњи Русија врши инвазију на Летонију и Естонију. Североатлантски савез долази у одбрану балтичких држава, а након његове интервенције распламсава се нуклеарни рат. Други пример је норвешка телевизијска серија *Окупација*, приказана у јесен 2015. године. Приказала је хипотетичку ситуацију заузимања Норвешке од стране Русије *ради заштите енергетске безбедности*. „Пуштање оваквих виртуелних сценарија, заједно са стварним редовним вежбама Североатлантског савеза које се одржавају на територији ових земаља, може се сматрати методом наменског формирања имица непријатеља, тако гајећи страх од претње из РФ" (Мельникова, 2020, р. 78).

увреда или неког другог понашања на интернету. Разне врсте *истинитих доказа*, прикривање циљаних, критичних чињеница, затим имплементација вредних, битних тачних информација у низ информативног смећа, где се оваквим поступцима омогућава манипулација јавним мњењем и то у жељеном правцу који је користан за наредбодавца, политичку или другу елиту друштва. Уколико је потребно, наведено може да оправда и паравојну или војну интервенцију једне државе према другој. Тактику заташкавања одређених чињеница користе медији да нивелишу погрешне процене спољне политике своје државе (Мельникова, 2020). Овим и сличним поступцима се напада психа људи, мења њихова свест. Када говоримо о средству, тада мислимо на информацију (односно све њене варијације) и она је у овом случају главно средство психолошког деловања. *Обојене револуције* у овом контексту заслужују посебну пажњу, јер спроведени и неуспешни покушаји смене режима, замене актуелне власти са демократским режимом, нису прошли без коришћења информационо – телекомуникационих система. Представља врсту стратегије индиректног деловања, на становништво земље и особље органа за спровођење закона у циљу подривања моћи.

Трансформативни потенцијал вештачке интелигенције је толико велики да ће довести у питање дугогодишње, темељне принципе ратовања. Такмичење (ратовање) великих сила у развоју индустрије сели се у област информација у којој ће прикупљање, коришћење и дистрибуција информација бити најважнији аспект „борбених операција". Некада давно је изговорена реченица да када почне сукоб (рат), тада нестаје истина, то је нешто што нам и данас може бити водиља у светлу актуелних сукоба на планети (Hoadley & Sayler, 2020).

У РФ, међу главним задацима активности државе у информационој сфери је концепт који обухвата јачање позиција руских масовних медија и масовних комуникација у глобалном информационом простору и приближавање тачке гледишта РФ о међународним процесима (Мельникова, 2020). *Стратешке комуникације* према већем делу теоретичара у РФ представљају изузетно широке делатности које се односе на постизање државних циљева на стратешком нивоу, са потребом да се обједине, успостави синхронизација активности за решавање постављених задатака, за промоцију или промену културних (идеолошких) вредности у свести конкретне циљне групе, као и за побољшање имица државе у међународним круговима (Мельникова, 2020). Према тумачењима истраживача у РФ, стратешка комуникација има три главна облика: односе с јавношћу, јавну дипломатију и информативне операције. Синхронизованост деловања у свим наведеним областима доводи до најбољих резултата. Један од облика стратешке комуникације су *информационе операције*, које се односе на: „интегрисану употребу електронског ратовања, операције рачунарске мреже, психолошке операције, војну обману и оперативну безбедност, укључујући њихове повезане и примењене аспекте, са циљем утицаја, ометања, корумпирања или пресретање процеса људског или аутоматизованог доношења одлука од стране противника..." (Мельникова, 2020, p. 39).

Влада РФ покушава да контролише информације као средство утицаја на публику и исходе одлука на начине који служе интересима РФ. Велики број теоретичара из РФ види контролу над информацијама као централну ставку за постизање политичких циљева. РФ је уложила знатна средства у развој свог алата за субверзију вођену информацијама, посебно у развоју канала информација са циљем да промовишу циљеве РФ у иностранству. Део теоретичара је одредио пропаганду РФ као *ватриште лажи*, констатујући да је велики обим

комуникације сведен на бесрамну спремност на ширење делимичних истина или директне фикције. У 2018. години информативне активности РФ су се знатно појачале што је укључивало употребу мреже друштвених медија за ширење антивладине реторике у Украјини, попут позивања на *Трећи Мајдан* и слично. Истраживачки новинари су открили (вероватно се ради о страним службама безбедности, не о новинарима) да је мрежа која је тврдила да ради у Украјини заправо била физички размештена у Москви и вероватно је била повезана са службама безбедности РФ. У скорије време, РФ је информације примењивала као средства за субверзију против циљева у иностранству, пре свега на политичке кампање у Европској унији и САД. *Санкт Петербург – Агенција за интернет истраживање* тајно је маскирана у САД, а основана ради председничких избора 2016. године са покушајем да искористи и продуби постојеће друштвене поделе у САД, раси, политичкој идеологији и класи. Агенти служби безбедности РФ су могли да упарују поруке са сегментима популације са којом су вероватније резонирали или подстицали их. РФ такође запошљава трол налоге којима управљају људи (лажни налози) и аутоматизовани ботови као множитељи силе да прошире домет и видљивост својих размена порука. Службе безбедности РФ могу радити у договору са отвореним државним медијима, организацијама као што су *Русија данас* и *Спутњик*. Друге недржавне организације су вероватно повезане са државом, РФ, преко личних (приватних), политичких, или финансијских веза, иако врло често (или готово увек) држава не признаје ове везе. Присутно је неговање односа са појединцима или организацијама који нису ни свесни да су у интеракцији (тзв. корисни идиоти) са службама безбедности РФ у склопу информационих активности. Појачавање порука битних за РФ, ретвитовањем, репостовањем или *свиђањем* субверзивних порука без сазнања о њиховој истинитости је врло присутно у овим активностима. Данас је комплетан информациони простор презасићен информацијама које све велике силе, врло често посредством служби безбедности, излажу безбројним порукама ради разних стимулативних дејстава. Онлајн информационо окружење омогућава корисницима анонимност и приступачност на мрежи, где окружење омогућава актерима РФ да директно истражују западну популацију без неких старих обичаја (неговања односа са новинарима као што су то радили некада припадници служби безбедности Савеза Совјетских Социјалистичких Република). Међутим, као што је у овом сегменту олакшан један вид активности припадницима служби безбедности, истовремено је отежан други вид, односно спознаја да популација може приступити широком спектру медијских извора тако да мање зависе од било ког медијског канала, тј. конкуренција је присутна, па која служба безбедности буде квалитетније организовала своје присуство у информационом подручју, то ће имати веће ефекте у информационим активностима (Radin, Demus & Marcinek, 2020).

Док су пропагандни и дезинформациони напори РФ усмерени на широку популацију, кампање *преваре, обмане* су више фокусирани напори да се утиче на мисаоне процесе и акције непријатељске елите. Циљ обмане коју спонзоришу службе безбедности је да се преваре непријатељски доносиоци одлука, руководиоци и службе безбедности стварањем лажне стварности, привида и на тај начин испољи утицај на политику. Дезинформације и лажне вести могу бити ефикасно средство да се дезоријентише противник и ослаби његово унутрашње јединство. С друге стране, стратешка обмана је тајни, офанзивни покушај службе безбедности да створи алтернативни наратив који служи интересима РФ. У прошлости је

коришћен за заштиту идентитета агената РФ у САД и откривање претњи режиму (Sipher, 2018).

У нормативима Министарства одбране САД *стратешке комуникације* су одређене као „циљани напори Владе САД да разуме и ангажује циљну публику како би створила, побољшала, одржала окружење погодно за унапређење интереса, политика и циљева Владе САД кроз коришћење усаглашених програма, планова, задатака, порука, синхронизованих са деловањем свих инструмената националне моћи". Циљеви стратешке комуникације у САД су наведени у документима оружаних снага САД, у којем се наводи: „Стратешка комуникација је систем дугорочних и координисаних акција које се спроводе на стратешком, оперативном и тактичком нивоу, који вам омогућава да идентификујете циљну публику, одређују ефикасне канале утицаја на њих како би се обезбедило потребно одрживо понашање ове публике". Примери употребе стратешких комуникација од САД су: „рат против тероризма за време председника Џорџа Буша млађег, напори да се прокламује демократија у земљама бившег Савеза Совјетских Социјалистичких Република, опсежне комуникацијске активности Ал–Каиде за регрутовање присталица и усађивање идеје „исламског калифата", акције за ширење утицаја умереног ислама као противтеже исламском фундаментализму у Африци, превенција сиде (*AIDS*), информативне кампање у европским и америчким медијима за искривљење слике о РФ, узимајући облик информационих ратова итд." (Мельникова, 2020, p. 40). Нова достигнућа у развоју електронике, различитих система телевизије, видеа и мрежних комуникација, глобалне интернет мреже, представљају неке од карактеристика данашњице. Постоји свест да је у суштини неограничена могућност утицаја информација на различите публике и са различитим циљевима довела до појаве концепта стратешких комуникација, који подразумева широку употребу информационо – телекомуникационих система за постизање најзначајнијих циљева државе у спољној политици, кроз ширење истинитих и лажних информација. Сајбер простор постаје једна од *најосетљивијих* платформи за политичку комуникацију.

5.4.2. Регистровани облици деловања

Пропаганда је дефинисана на много различитих начина. Тако је у оружаним снагама САД пропаганда одређена као: „сваки облик комуникације као подршке националним циљевима дизајнираним да утичу на мишљења, емоције, ставове или понашање било које групе како би користили спонзору, директно или индиректно" (Lieberman, 2017, p. 96). Једна од категоризација пропаганде је према извору поруке, и то на *белу пропаганду* која се односи на „поруке издате из отвореног и признатог извора, циљање на одређену публику и нескривање извора", затим на *црну пропаганду* која се односи „на поруке из непознатог извора, често засноване на лажима или измишљотинама" и на *сиву пропаганду* која није ни потпуно истинита нити потпуно лажна, и не идентификује се посебно њен извор (Lieberman, 2017, p. 97). Теоретичар пропаганде Харолд Ласвел (*Harold Lasswell*) је дефинисао пропаганду као: „управљање мишљењима и ставовима директном манипулацијом", али с обзиром на то да теоретичари често беже од негативног одређења одређеног појма, тако наводимо и дефиницију Тејлора (*Taylor*), који је пропаганду одредио као: „процес којим се идеја или мишљење саопштавају неком другом са одређеним убедљивим циљем" (Chernobrov & Briant, 2020, p. 2). Ради се о средству које владе традиционално користе за проширење међународног утицаја и унапређење спољнополитичких циљева. Термин јавна

дипломатија (енг. *public diplomacy*) је пласиран када су САД настојале да замене термин *пропаганда* за описивање свог страног утицаја на становништво, како би се разликовале пропагандне активности САД од оних које су коришћене у нацистичкој Немачкој или Савезу Совјетских Социјалистичких Република. САД и РФ представљају два велика међународна актера са супротстављеним политичким интересима, са дугом историјом узајамних пропагандних активности. Односи између САД и РФ, посебно након украјинске кризе, окарактерисани су проширеним пропагандним напорима и падом поверења јавности у новинарство и демократске политике. Руска Федерација је ограничила инострано власништво над медијима, донели су низ закона о сузбијању *лажних вести* и дезинформација, повећано је улагање у сопствене медије, јавну дипломатију и уведена листа *страних агената* (Chernobrov & Briant, 2020).

Комитет за тајну преписку (*кореспонденцију*) је поред информативне функције изводио тајне операције, развијао и дешифровао шифре, финансирао разне пропагандне активности које су биле од користи Конфедерацији (будућој држави САД) и вршио тајне инспекције поште (Юрьевич, 2014).

Једна од мера које су САД донеле током Другог светског рата ради заштите националних интереса САД (за време мандата председника Рузвелта – *Franklin D. Roosevelt*) је било појачање пропагандне активности оружаних снага САД и то оснивањем Канцеларије за ратне информације (енг. *United States Office of War Information*) у јуну 1942. године. Основна разлика од активности Одбора за јавно информисање била је да је пропагандна активност била усмерена не само на обликовање јавног мњења америчког становништва, већ и у другим земљама. Главни инструменти за ширење пропаганде били су медији – штампа, радио, кинематографија (филм). Канцеларија за ратне информације је распуштена завршетком рата, тачније у септембру 1945. године, али важно је нагласити да послови из ове области нису прекинути, већ је даље ширење информација у циљу формирања јавног мњења, као и функције прикупљања података, додељено другим, углавном државним одељењима, па Централној обавештајној агенцији и Информативној служби САД (накнадно трансформисана у новинску агенцију САД). Главно усмерење америчких информација тј. политике је била антисовјетска пропаганда, која се спроводила разним методама ефективно (Шариков, 2020).

Међу субјектима глобалног информационог друштва посебно су битне велике корпорације „*National Broadcasting Company, Sony, Disney, Bertelsmann, Viacom, TCI, Universal* и др., односно њихова могућност испољавања утицаја на међународне токове, процесе који се одвијају у оквиру глобалног финансијског система" (Мельникова, 2020, p. 59). Компаније у САД су водећи играчи на глобалном медијском тржишту, а њихово лидерство је одређено низом фактора (пре свега везаних за степен развоја самих информационо – комуникационих технологија). Информациони простор западног света данас контролише само пет глобалних корпорација: „*Time Warner, News Corporation, The Walt Disney Company, Viacom/Columbia Broadcasting System Corporation* (сада под новим називом – *Paramount Global*) и *Comcast/National Broadcasting Company Universal*" (Мельникова, 2020, p. 59). Ове фирме попуњавају информациони простор за велики број становника глобализованог света чиме одређују шта људи свакодневно гледају, слушају и читају. У РФ, једна од најутицајнијих медијских компанија је *Газпром Медиахолдинг* основана 1998. године. Структура комбинује савезне и регионалне телевизијске и радио компаније, стотине медија на различитим нивоима, продукцијске куће, видео и интернет

сервисе. Дакле, национални и транснационални медији заправо не брину толико о обезбеђивању слободе говора, колико делују као једно од оруђа за управљање друштвом у интересу економски најмоћнијих, политичке елите, одређених друштвених слојева и група. На крају, у збиру активних учесника политичке комуникације треба поменути институције цивилног друштва – невладине структуре, организације за људска права, итд. Ту спадају, на пример, међународне спортске федерације, Репортери без граница, Хелсиншка група итд. Људска права, добротворне и еколошке активности представљају главне области интересовања таквих организација, које првенствено користе интернет за комуникацију (Мельникова, 2020).

Када говоримо о експлоатисању масовних медија у пропагандне сврхе, морамо нагласити да то није феномен савременог доба. Све оно што се региструје у последњих неколико деценија као спектакуларност, сликовито представља вредности ефективног маркетинга и нерегуларне поруке силе која се дистрибуира кроз стратешке комуникације. Неки инциденти су указивали на то да деловање разних нерегуларних снага може бити успешна тактика или оперативна кампања. Неким посматрачима се чинило да су заузимање америчке амбасаде и талачка криза у Техерану (1979 – 1981) и бомбашки напади у Либану 1983. године створили осећај америчког уступка и повлачења или неспособности САД да одговоре. Инциденти морају бити спектакуларни да би привукли медијско праћење. Коришћење медијског извештавања је норма за нерегуларне снаге. Колико је једна информациона операција ефикасна, показаће способност да изазову драматичан утицај страха и неизвесности у конкретној, циљној популацији. Континуирано насиље биће нормално против одређених људи који представљају елементе цивилне или војне контроле и реда. Велики број електронских извора информација и конкуренције са све већим бројем других тема у вестима, нерегуларне снаге често користе за повећану количину насиља или новина како би привукле масовну пажњу. Жеља за сензацијама је склоност великих медија и публике, па иако су врло често трагични и катастрофални, могу подстаћи појачано насиље напада. Једноставан аспект медијског маркетинга (злобног карактера) је индоктринација деце[64] да мрзе и промовишу насиље и терор са једним тотално искривљеним погледима на свет. Неки школски уџбеници палестинске управе одбацују право Израела на постојање, промовишу терор и слично. Нерегуларне операције снага узимају у обзир жељени медијски ефекат и планирају вербално или визуелно извештавање. Догађаји подршке и интервјуи појачавају жељену поруку. Ове поруке могу представљати дезинформације и лажне перспективе. Побољшање квалитета електронских публикација представља издање часописа *Инспајр* (енг. *Inspire*) за лето 2010. године, најављено као периодични часопис Ал–Каиде на Арапском полуострву. Документ је објављен на енглеском језику, користи графички дизајн налик комерцијалном и садржи примарне чланке који промовишу екстремистичку верзију светских догађаја испресецаних темама и визуелним детаљима или наративним упутствима о томе како да се спроведу врсте напада (Training and Doctrine Command G2 Handbook No. 1.08, 2010). Потешкоће оружаних снага САД ће се огледати у суочавању са сукобима који

[64] Телевизија Хамас Ал – Акса емитовала је церемонију дипломирања вртића Исламске асоцијације у Гази где су између осталих, одрасли постављали и следећа питања деци: „Која је ваша најузвишенија аспирација?", деца одговарају: „Смрт за име Алаха". Поред ових питања и одговора, мали дечаци обучени су у такву одећу да подсећају на палестинске милитанте и марширају пред очима и падају на под да пузе по њима на стомаку као војници извршавајући тактичке задатке (Training and Doctrine Command G2 Handbook No. 1.08, 2010, p. 200).

захтевају темељно разумевање како политичких, географских, економских, културних, верских, политичких и историјских контекста у којем ће се водити нерегуларни сукоби, операције, ратови.

5.4.3. Дезинформације

Када говоримо о провери извора података, односно да ли је људски извор валидан, тада се говори о питањима сврхе и технике вођења операција против опозиције, а како би се контролисале њихове активности, дезинформисале, ухватиле у замку или их натерале да открију своје оперативне технике и способности. Почетком 1920. године, државна политичка управа Савеза Совјетских Социјалистичких Република је, уместо да их елиминише као једну од понуђених варијанти у то време, прибегла продору (контроли дела политичке опозиције) у постојеће антикомунистичке организације. Оперативни назив акције службе безбедности био је *Поверење* (енг. *The Trust*). Обмане и дезинформације су током Другог светског рата играле виталну улогу у операцијама против Немачке. Пре инвазије на Нормандију 1944. године, Британци су користили ухапшене нацистичке шпијуне, заједно са масовном кампањом дезинформација, која је укључивала стварање потпуно фиктивног савезничког армијског корпуса, да би убедили Немце да ће инвазија бити усмерена према *Pas de Kalais*, а не на *Нормандију*. Овде се радило о врхунским британским операцијама контраобавештајне службе, која је идентификовала и неутралисала све нацистичке изворе података у Великој Британији, ради што потпуније контроле информација. Интересантан је случај дезинформисања од стране Британаца у Другом светском рату – операција у којој су савршено припремљени лажни ратни планови који су се налазили уз леш наводно утопљеног британског официра, а који је испливао на обали у Шпанији. Ова обмана је навела Немце да мисле да савезници намеравају да нападну Сардинију и Грчку уместо Сицилије. Вештина дезинформисања, једне од сложенијих активности служби безбедности, контраобавештајног карактера, овде је толико водила рачуна о детаљима, где су чак и приликом избора леша користили исти од особе која је умрла од упале плућа, где овај узрок смрти показује патолошке знакове сличне утапању. Служба безбедности тј. Комитет државне безбедности, након што је 1985. године добила податке од Олдрича Ејмса (*Aldrich Ames*) о скоро свим људским операцијама које води америчка Централна обавештајна агенција против Савеза Совјетских Социјалистичких Република, убрзо је почео да хапси ове изворе, што је довело до угрожавања Ејмса. Обавештајна заједница САД није се истакла у вођењу контролисаних извора против опозиције током Хладног рата. Били су неуспешни, док су у постхладноратовском периоду оружане снаге САД наводно имале успеха у вођењу операција *управљања перцепцијом* против Ирака пре операције Пустињска олуја. Војна политика САД је да се *Офанзивне контраобавештајне операције* воде ради заштите и унапређења националне безбедности које се спроводе углавном посредством двоструког агента са следећим циљевима: контролисање противниковог система шпијунаже и на тај начин приморавање да ради за вас, идентификовање, неутралисање или потискивање нових агената и шпијуна, добијање информација о особљу и методама противничке службе, обезбеђивање приступа шифрама противника, прибављање доказа о намерама противника, испољавање директног утицаја на оперативне намере непријатеља и систематског обмањивања непријатеља. У својим сопственим операцијама и у сарадњи са војним службама, Федерални истражни биро је настојао да убеди опозицију у вредност клацкалице у настојању да наведе

непријатељске обавештајне службе да воде операције у САД, што би Федералном истражном бироу дало веома вредне информације о методологији, начину рада страних служби безбедности у САД. Наводно, Централна обавештајна агенција, са веома ретким изузецима, није покушала да води контролисане операције него је углавном вршила координацију таквих операција које воде друге службе безбедности САД у иностранству. Недостатак успеха САД у овој области током Хладног рата и прве две деценије постхладноратовског периода, може се делимично приписати успеху Комитета државне безбедности и војне службе безбедности Главне обавештајне управе у офанзивном деловању руских служби безбедности према службама безбедности САД. Ејмс и Хансен (*Robert Hanssen* који је ухапшен тек 2001. године), двоструки агенти, допуњени другим мање познатим изворима у војсци, пружили су Комитету државне безбедности и Главној обавештајној управи детаљне информације о методологији рада двоструког агента, целокупној доктрини, комплетно начину *играња* оперативних техника и многим, ако не и свим, специфичностима вођења таквих операција. Очигледни успех операција обмане против Ирака пре Пустињске олује говори о великом побољшању рада служби безбедности САД, јер показује да Садам Хусеин није имао квалитетне изворе у оквиру служби безбедности САД које су службе безбедности Русије дефинитивно имале (Redmond, 2010).

Необавештајне активности служби безбедности које су из године у годину све више примењиване у сукобу великих сила, са посебним освртом на информационе операције, у овом периоду учесталих сајбер напада, затим толики број (дез)информација од стране Запада и Истока везано за сукобе у Украјини, тзв. енг. *fake news*, довео је до *бомбардовања* обичног посматрача огромним бројем података који су углавном нетачни и/или су испродуковани приликом вршења пропагандних активности. Напредне технологије су довеле до њихове употребе за потребе служби безбедности првенствено за долазак до безбедносно интересантних података, као и до припрема *дубоких лажи* (енг. *deep fakes*) код којих је готово немогуће установити чак и форензичким алатима да ли се ради о лажним (монтираним, пласираним) материјалима или не. С обзиром да службе безбедности већ одавно користе вештачку интелигенцију за реализацију својих активности, за очекивати је да ће модернизација технологија на овом пољу бити једна од нових еволуција у овој области рада (Марјановић, 2022).

Сваки владар, сваки војсковођа је још од давнина поштовао правило да уколико није информисан и обавештен, да је сигурно осуђен на губитак рата, битке, операције, реализације неког задатка. Међутим, данас вештачка интелигенција омогућава толико реално спровођење фалсификовања (фотографија, аудио, видео записа и других евиденција) до тог нивоа да је за очекивати (уколико се већ није догодио) напредак технологија до те мере да ни алати форензичке анализе неће моћи установити да се ради о фалсификатима. Ови и слични фалсификати, који су познати под именом *дубоке лажи* (енг. *deep fakes*) доводе до могућности коришћења ових и њима сличних фалсификата као део информационих операција. Наведено би било употребљено за генерисање лажних извештаја вести, утицаја на јавни дискурс, нарушавања поверења јавности и уцењивања лица, дипломата, организација и слично. Супротстављање дубоким лажним технологијама се спроводи кроз пројекат медијске форензике (енг. *MediFor*), који настоји да аутоматски открије манипулације, пружи детаљне информације, о манипулацијама изведеним на медију и да пружи образложење укупног интегритета медија. Идентификација фалсификата произведених од стране вештачке

интелигенције је кључни проблем, као и то што машинско учење може довести до тога да се надмаше форензички алати. Циљ је развијање алгоритама који ће аутоматски откривати, идентификовати као злонамерне, различите врсте дубоких лажирања. У свету служби безбедности, вештачка интелигенција би могла бити коришћена за израду дигиталног профила начина живота одређеног лица (био то припадник службе безбедности или не), где би се дигитални запис појединца спајао са забележеним дигиталним подацима о местима куповине, артиклима, кредитним извештајима, локацијама, рачунима – износима, претплатама, обавезама и др. У случају дубоких лажирања, ове и њима сличне информације би се могле користити за потврђивање одређених података, одбацивање података или као циљане операције ради спровођења необавештајних активности, првенствено присиле, утицаја, компромитације, уцене и сличних поступака (Hoadley & Sayler, 2020).

Активне мере обухватају активности од обмањивања, дезинформисања јавног мњења до обмањивања, дезинформисања Западних служби безбедности. Мада су произвођачи лажних вести свесни да документ, информација, лаж која се појави у медијима, штампи, једног дана или одмах, наводни аутор може порећи њену аутентичност, међутим гледиште произвођача таквих обмана је да порицање никада неће у потпуности надокнадити штету коју је нанела лажна вест. Идеје слободе говора, позивање на морално узвишење у информацијама и борбу са Западом, и нудећи приступ алтернативним гледиштима преко медија[65] у власништву РФ, постали су темељни концепти пропаганде РФ. Фабриковање дезинформације је према новинару Солдатову (*Andrei Soldatov*) у РФ увек било засновано на око 95 посто објективних информација којима је нешто било придодато како би се подаци претворили у циљане информације или дезинформације. Постоје чак формиране и организације (једна од њих: енг. *StopFake.org*) која је наводно открила око 500 случајева дезинформација од стране медија РФ за две године (2014–2016). Није била реткост дистрибуције дезинформација и кроз новине[66] које нису настројене РФ (Fedchenko, 2016).

Када говоримо о методама које су користиле и *Окхрана*[67] и *Чека*[68] (ради спровођења дезинформисања како државног и војног руководства тако и јавности, где је човек извор

---

[65] У Путиновом говору за отварање *RT Spanish* 24/7 емитовања у Аргентини у јулу 2014. године, он је навео да нација сада добија угледан, и што је најважније, поуздан извор информација о догађајима и развоју у РФ и широм света. Право на информације једно је од најважнијих и неотуђивих људских права (Fedchenko, 2016).

[66] Ради се о следећим новинама (листовима): „*The Morning Star – British socialist newspaper, L'Humanite – daily newspaper of French Communist party, and Rude Pravo – the newspaper of the Communist party of Czechoslovakia*" (Fedchenko, 2016, p. 152).

[67] Окхрана, Царска тајна полиција. Руски цар Александар II је убијен 1881. године када се показао озбиљан пропуст система обезбеђења цара. Овај догађај је приморао његовог сина цара Александра III да предузме нешто како би се он заштитио и тако ствара *Окхрану* или безбедносне снаге. Када се говори о Окхрани, тада се мисли на прву модерну руску тајну полицију, претечу данашњих служби безбедности РФ. Бивши директор службе безбедности, Федералне службе безбедности и актуелни Председник РФ, Владимир Путин, а поводом 100. годишњице руске Спољне обавештајне службе у 2020. години је нагласио да руски припадници службе безбедности настављају традицију не само њихових бољшевичких претходника, него и оних који су служили предреволуционарној Русији (Riehle, 2022).

[68] Чека (рус. *Всероссийская чрезвычайная комиссия по борьбе с контрреволюцией и саботажем* – Сверуска комисија за борбу против контрареволуције и саботаже) била је главна тајна полиција у Савезу Совјетских Социјалистичких Република од децембра 1917. године, за време Владимира Лењина, коришћена првенствено у борби против политичких противника Лењинове политике (Riehle, 2022). Касније су настале Државна политичка управа (рус. *Государственное политическое управление*) формирана у фебруару 1922. године наследивши на том месту Чеку, па Обједињена државна политичка управа (рус. *Объединенное Государственное Политическое Управление*) настаје новембра 1923. године, како би објединила сва одељења и јединице Државне

података), оне су сличне, као и код наследница (службе безбедности) совјетских служби, односно РФ и ради се о: *агенту провокатору, дезинформацијама* и *двоструким агентима*.

Охрана је ограничено користила *агенте провокаторе* (енг. *agents provocateurs)*, тј. агенте који су тајно упућени, послати, у име непријатеља, противника, да изазову физичку штету, немире, а који се затим може искористити за дискредитацију непријатеља, противника. Уз помоћ агента провокатора, Охрана је направила фиктивну заверу за убиство цара Александра III, у Паризу, а затим пренела информације француским властима, које су ухапсиле заверенике. Само је агент провокатор побегао, уз помоћ Охране. Слично наведеном примеру Охране, Чека је такође створила сопствену опозициону групу коју су окривиле за насиље, познату као *посланичка завера*, у којој је улогу играо британски авантуриста Сидни Рајли. Та измишљена завера укључивала је контрареволуционара (официра Чеке), који је обавестио британске и француске изасланике у Москви да је летонски пук у Кремљу спреман да предводи антибољшевички устанак. За реализацију завере био је неопходан новац који је Рајли обезбедио (преко британске тајне обавештајне службе за коју је радио) агенту провокатору, који је новац предао директно Чеки (која је званично обелоданила ову акцију, да је ликвидирана завера коју су организовале англо – француске дипломате, док је у стварности највероватније сама Чека сковала заверу). Важно је напоменути да су од самих почетака активности служби безбедности још у Савезу Совјетских Социјалистичких Република, па до данас, прилагођавале своје напоре *дезинформисања* градећи их још од тактике Охране, чија су обележја била карактеристична по подметању медијских прича да би збуниле непријатеље Русије и намамиле их у замке агената, служби. Један од примера још из тог периода (Охране) је убацивање припремљених материјала – текстова у новине са запада са детаљима о терористичким нападима (који се стварно и реализују, али са минималном штетом) унутар Русије са циљем убеђивања западне службе безбедности у револуционарну претњу и како би се потврдили већ пласирани извештаји агената. На овакав и сличан[69] начин, службе безбедности Савеза Совјетских Социјалистичких Република су у великој мери користиле дезинформације ради реализације циљева тадашње спољне политике државе и како да спроведу манипулацију страним перцепцијама. Василиј Митрохин, официр Комитета државне безбедности који је пребегао 1992. године, *активне мере* је још у доба Савеза Совјетских Социјалистичких Република

политичке управе на територији Савеза Совјетских Социјалистичких Република. У 1934. години формиран је Народни комесеријат унутрашњих послова (рус. *Народный комиссариат внутренних дел*) што је био назив за бившу јавну и тајну полицију Савеза Совјетских Социјалистичких Република, која је постојала до 1946. године (Riehle, 2022). Наследиће је Министарство унутрашњих послова Савеза Совјетских Социјалистичких Република и Народног Комитета државне безбедности (где је тајна полиција и даље била део Народног комесеријата унутрашњих послова) од 1953. године, а од 1954. године Комитет државне безбедности постаје потчињен Савету министара, да би Комитет државне безбедности био распуштен 1991. године, након неуспелог пуча вођеног од стране Владимира Крјучкова, шефа тада Комитета државне безбедности (Riehle, 2022).

[69] Петр Михајлович Карпов, први официр Обједињене државне политичке управе који је пребегао на Запад 1924. године, описао је операције дезинформисања Обједињене државне политичке управе раних 1920–их које су биле осмишљене да окриве монархистичке армије за погроме у Русији које су, у стварности, извршили војници Црвене армије и бољшевици. По сличном рецепту, Карпов и његов партнер Владимир Орлов су ухапшени од немачких власти, 1929. године које су га оптужиле да је фалсификовао документе службе безбедности Савеза Совјетских Социјалистичких Република и да их је продао штампи. Део тих докумената које су Карпов и његов партнер Владимир Орлов продали је био везан за два америчка сенатора, Вилијам Бора и Џорџ Нориса, да су наводно добили од режима Савеза Совјетских Социјалистичких Република по 100.000 долара да промовишу промосковску политику у Вашингтону (Riehle, 2022).

одредио као стварање услова повољних за успешно спровођење спољне политике Савеза Совјетских Социјалистичких Република. Открића дезинформационих операција које је спроводила Русија тек у другој деценији овог миленијума показују континуирано наслеђе од времена Окхране, до данас (Riehle, 2022). Из наведеног се може доћи до закључка да се одређени *рецепти* понављају, обликују, дорађују.

Када се говори о *двоструким агентима* служби безбедности РФ, историјски посматрано још од доба Окхране и царске ере, овај метод рада служби безбедности је активно примењиван. Наиме, начин стварања оваквих агената је врло комплексан и обухватао је најчешће лица, агенте непријатеља који су били ухваћени у недозвољеном раду, делатностима, и били су окретани или приморавани да прију својим првобитним спонзорима док су радили све за потребе руског руководства. Најчешћи задаци овим агентима су били да идентификују руководиоце и уопште непријатељске агенте, а поред тога, они су били ти који су представљали главни канал за дезинформације које би биле пласиране директно руководиоцима непријатељских служби безбедности, владајућег државног апарата ради утицаја на доношење одређених одлука. Након хапшења агената од стране Окхране (мада постоје и други[70] примери), често је покушавала да их удвостручи, најчешће присилом, мада и подстицајем (Riehle, 2022). Опрез са којим су припадници служби безбедности још царске Русије прилазили раду са оваквим агентима говори управо о комплексности рада са двоструким агентима и великим бројем проблема, могућих ризика и претњи које овакав вид ангажовања лица носи са собом, као и *добит* која се може остварити са њиховом употребом. Након Окхране, Чека је на сличан[71] начин схватила колико су битни двоструки агенти и каква је то вредност и моћ поседовати их. Један од примера је током Руског грађанског рата, када је спровођена операција *Трест* (започела пресретањем писма 1921. године од руског монархистичког агента Александра Јакушева који се залагао за побуну против бољшевика унутар Русије, а не од стране емиграната), којом је Чека идентификовала и неутралисала антибољшевичке активности. Какав је резултат уколико је квалитетан овакав рад служби безбедности, најбоље говори то да је *Трест* нанео непоправљиву штету моралу и способностима антибољшевичког покрета у Европи где се исто најбоље види у цитату Владимира Бурцева, антисовјетског активисте у Европи, који је писао у децембру 1927. године: „на овој удаљености је практично немогуће знати ко од ових људи ради за, а који против бољшевика, а још је теже сазнати ко можда подржава Стаљина против опозиције, а ко је опозиција против Стаљина" (Riehle, 2022, p. 28). С обзиром да је ова операција, колико год успешна била, завршена управо одавањем од стране двоструког агента, наведено потврђује

[70] Хозе Марија Гидис пришао је русу, тада војном официру у Кини 1904. године и понудио се сам да пружи информације о Јапану (тада главни спољни непријатељ Русије). Руски официр је сумњао да је Гидис у контакту са јапанском службом безбедности. Опрезно је затим радио са њим и од њега примао војне податке. На крају је удвостручио агента против Јапанаца непосредно пре избијања руско – јапанског рата (Riehle, 2022).

[71] Чека је ухапсила Јакушева и вербовала користећи га да подржи њихове напоре против контрареволуционарних активности заснованих у иностранству. Службе безбедности су оформиле за потребе *Треста* фиктивну анти – бољшевичку организацију под називом Монархистичка организација Централне Русије. Чланови ове организације су наводно укључивали совјетске званичнике који су били спремни да сруше бољшевички режим. Операција је започела 1921. године и трајала је све до почетка 1927. године. Разлог прекида ове операције је предаја другог двоструког агента, Александар Упењинш, емигрантима које је обавестио да ову организацију контролише служба безбедности Савеза Совјетских Социјалистичких Република (Riehle, 2022).

горе поменуту комплексност и ризик коју овакви видови активности могу донети служби безбедности, односно држави.

Примарне разлике између Окхране и њених бољшевичких наследничких организација биле су у необузданој моћи служби безбедности из доба Савеза Совјетских Социјалистичких Република, посебно током Стаљинове владавине (када су спровођена протеривања, насилним смештајем у психијатријске установе, чак и погубљења спровођена по пресуди службе безбедности). Важно је нагласити да службе безбедности РФ у постхладноратовском периоду до данас немају неограничену моћ као службе безбедности из Стаљиновог доба, али не треба заборавити да за највеће преступе, поготово агената РФ (нарочито ту мислимо на категорију двоструких агената), ликвидација агента као метод рада служби безбедности је враћен назад што се више пута догодило неколико година уназад. Велики број података указује на ову констатацију (Riehle, 2022).

У САД и РФ сматрају пропагандне и дезинформационе активности као оруђе спољне политике. Велике силе су страну пропаганду представиле као претњу држави, кроз угрожавање националне безбедности, затим постојећих међународних савеза, изборних система као и поверења у демократију и дестабилизацију власти кроз разне врсте немира. Претње од пропаганде, дигиталног мешања и манипулације заузимају велики део дискурса о односима великих сила, САД и РФ. Можемо констатовати да како САД, тако и РФ следе домаће политичке интересе представљајући критичко медијско извештавање као *лажне вести* и позивајући на повећање издатака за одбрану државе у *информационом рату*. Уколико дође до великог страха од све софистицираније и дигиталне пропаганде, може се подстаћи позив за јачом државном регулативом о употреби информација и интернету и покренути пропаганда у *трци у наоружању* како покушавају да надмаше другог (Chernobrov & Briant, 2020).

У књизи *Рат на Балкану – џихадизам, геополитика и дезинформација*, коју је написао генерал – мајор Карлош Бранко[72], како сам каже ради мирне савести, наводе се три критична догађаја која су се догодила у периоду док је он био ангажован у Организацији уједињених нација на простору Републике Хрватске и Босне и Херцеговине, и то: први догађај који се догодио 1995. године био је масакр над српским становништвом у Републици Хрватској и етничко чишћење током акције *Олуја* коју су реализовале оружане снаге Републике Хрватске потпомогнути необавештајним активностима САД, затим други догађај, који се такође догодио 1995. године – бомбардовање пијаце *Маркале* у Сарајеву у Босни и Херцеговини (стари део града настањен тада већински муслиманским становништвом), и готово тренутна аматерска идентификација кривца тог бомбардовања (да је то наводно српски народ, што је касније доказано да је било немогуће) и трећи догађај, у *Сребреници*, Босна и Херцеговина где су се догодили многи злочини са обе (српске и муслиманске) стране, али није било геноцида, према писању Карлоша (Karloš, 2019). Можемо констатовати да се ради о класичном потпису служби безбедности где је низом дезинформација оправдаван поступак увођења санкција, убијања, бомбардовања, сукобљавања два и више народа који су до јуче живели заједно, сатанизовања читавог народа без чињеница о неком догађају, већ све са

[72] Карлош Бранко, генерал – мајор, оружане снаге Португалије, био је у периоду од 1994. године до 1996. године заменик шефа мисије војних посматрача у Организацији уједињених нација за Републику Хрватску и Босну и Херцеговину, а књигу је објавио 2016. године.

унапред исфабрикованим дезинформацијама, што посматрамо и 2022. године у Украјини где постоји велики број сличних или готово идентичних дешавања, обмана, дезинформација и ангажовања служби безбедности великог броја држава присутних у овим активностима.

5.4.4. Медији и друштвене мреже као основно оруђе пропаганде

Оптужбе између великих сила за дигитално мешање, дезинформације, лажне вести и пропаганду, посебно после украјинске кризе и председничких избора у САД 2016. године су све веће. Велике силе, у овом случају САД и РФ представљају међусобну и сопствену пропаганду, своју претњу и моћ над публиком на следећи начин.

Када говоримо о дигиталним медијима у Украјини, и политика коришћења друштвених медија у протестима на Евромајдану је одиграла важну улогу у претходном великом политичком преокрету у Украјини, односно наранџастој револуцији 2004. године, па крајем 2013. и почетком 2014. године. Важно је нагласити да друштвене медије у периоду Евромајдана и током припрема за анексију Крима карактеришу три важна механизма која су друштвени медији испољили да би могли утицати на учешће и развој протеста, и то: пружањем алата за организовање протеста, олакшавањем ширења информација везано за протесте и изградњом мрежа које би могле одржати континуитет и усмеравати протестно кретање (MacDuffee & Tucker, 2017).

Медији и друштвене мреже као основно оруђе у пропаганди постали су популарно средство за информационе операције и друге недозвољене онлајн активности као што је прикупљање података за службе безбедности, пропаганду, дезинформације, обману, као и регрутовање и прикупљање средстава за одређене активности. Када говоримо о друштвеним мрежама и медијима, ради се о једном погодном алату за изузетно брзу дистрибуцију повезаних текстова и фотографија ради подржавања одређене теме са огромним бесплатним множењем. Наводно је било неколико примера да РФ покушава да контролише друштвене медије у вези са кризом у Украјини. Било је случајева отпуштања уредника популарне руске интернет странице вести *Lenta.ru* и директора *Vkontakte* и њихове замене лицима везаним за РФ. Велике силе настављају да предузимају кораке ка ограничавању слободе медија и слободе говора на интернету. Друштвени медији су посебан феномен XXI века где једна објава појединца може постати подједнако моћна и равномерна, па чак и распрострањенија од података које је објавио канал који контролише држава (Bērziņš et al., 2015).

Према медијским извештајима, Конгрес САД директно финансира такозвани *Управни одбор за радиодифузију*, који заузврат издваја новац за отворено *субверзивне медијске* пројекте на руском језику (*Глас Америке, Радио Слобода, Садашње време*). Сврха ових ресурса је да критикују било које активности власти РФ, текуће реформе у РФ и спољну политику РФ (Мельникова, 2020).

Електронске друштвене мреже представљају активног учесника у процесу политичке интеракције, а једна од специфичности је то што немају званични правни статус. Друштвене мреже карактерише неформалност, мобилност, флексибилност, независност од бирократских процедура, анонимност. Активности на мрежама нису много инферiорније у односу на друге велике субјекте мрежне комуникације (на пример, пословне структуре или државе). Добре особине друштвених мрежа би могле бити следеће: „способност уједињавања појединаца (више не причамо само о колективним субјектима већ и о појединачним – физичким лицима) према њиховим интересима и на тај начин формирања релативно хомогених група; широк

обим утицаја; способност изградње комуникацијског процеса без обзира на државне и друге врсте граница; брзо активирање присталица за друштвено значајне активности; висок степен мотивисаности учесника и друге; лоше особине или можда да их наведемо као слабости друштвених мрежа би биле: нејасна организација, ограничени ресурси, недостатак подршке званичних структура (првенствено државе) и сл." (Мельникова, 2020, p. 62).

Током Евромајдана, друштвени медији су били кључни алат који је коришћен за организовање. Вршена је координација превоза на великим удаљеностима и коришћена је могућност генерисања широко распрострањене подршке из целе државе, па и света. Организовање покрета је било углавном без вође (видљивог, прим. аут.), али оно што је можда најважније јесте то да је успело да сруши владу. Дигиталне мреже имају способност (где нема цензуре) да заобиђу релативно репресивно медијско окружење, па чак и да изнуде уступке неким медијима о њиховом извештавању о догађајима. Још увек знамо изненађујуће мало о покретима прожетим друштвеним медијима (MacDuffee & Tucker, 2017). Чим се о нечему јако мало зна, ту се одговор врло често проналази у службама безбедности као организаторима, подршци или реализаторима.

Велики број блогера и тролова[73] има РФ у друштвеним медијима. Упоредимо медије са запада и истока: на пример, 2012. године часопис *Гардијан* је објавио да је из РФ одређена група задужена да ласкаво извештава о председнику Владимиру Путину и да дискредитује опозиционе активисте и медије током кризе у Украјини и да се број активности тролова повећава од фебруара 2014. године. У РФ, независне истраживачке новине *Новаја газета* су известиле о раду тзв. *фарме тролова* у септембру 2013. године, наводећи да је наводно у августу те године почело масовно регрутовање тролова где се очекивало да се објави 100 интернет коментара по дану. Поред овога, тролovање укључује и одржавање више Фејсбук и Твитер налога, уз добијање нових пратилаца, који учествују у дискусијама. Пруски налози су све видљивији на друштвеним мрежама од краја фебруара 2014. године, а једна од кампања је била *Пристојни људи* која је промовисала инвазију фотографијама трупа РФ где се позира поред младих девојака, мајки са децом, старијих особа и кућних љубимаца. Дезинформације, ширење гласина или фалсификовање чињеница (фотографија, прича, догађаја…), улазак у дискусије и преплављивање веб простора повезаних са темама (странице догађаја на Фејсбуку, форуми за дискусију, *hashtag*[74]) са својим сопственим порукама или једноставно злоупотребљавањем главне тематике, представљају основ рада тролова. За регрутовање пруских бораца[75] у источну Украјину коришћени су друштвени медији (Bērziņš et al., 2015).

---

[73] Интернет трол (енг. *Internet troll*) је особа која подстиче раздор на медијској мрежи покретањем тема које доводе до расправа, узнемиравања људи, објављивањем запаљиве, стране поруке или поруке ван теме онлајн заједница са намером да изазове читалаоца на емоционални одговор или да иначе ремете нормалну дискусију на тему. Лажни или анонимни профили су они које користе тролови. Када се говори о спонзорисаним троловима то су тролови који делују у име одређене групе, организације, држава или неких других ентитета и обично одржава више лажних профила (Bērziņš et al., 2015).

[74] *Hashtag* – симбол са ознаком # почиње сваки хештаг, прво је почео да се користи на твитеру, па и на осталим друштвеним мрежама *Instagram, Linkedin, Facebook, Pinterest, Youtube* и сврха му је лакша подела садржаја са другим корисницима.

[75] Дана 13. јула 2014. године, Радио Слободна Европа је објавила интервју са извесним Артуром (*Artur Gasparyan,* 24 године стар, из Јерменије) који је наводно један од регрутованих лица преко друштвених мрежа на руском језику, конкретно преко сајта *Vkontakte* (Bērziņš et al., 2015).

Да се друштвени медији користе за обману, најбоље илуструју случајеви измишљеног доктора из Одесе, задављене трудница у згради синдиката у Одеси, злочини украјинских екстремиста у источној Украјини и сл. *Случај измишљеног доктора из Одесе* је откривен од стране Радио Слободне Европе/Радио Слободе[76], који је известио о овом случају трола који користи лажни *Фејсбук* налог након трагичног пожара у згради синдиката у Одеси. *Фејсбук* пост[77] је наводно креирао доктор Игор Розовскии (*Igor Rozovskiy*), који је покушао да уђе у запаљену зграду да пружи помоћ, али наводно проукрајински екстремиста му је забранио улазак и злостављао га. Друштвена мрежа на руском језику, *Vkontakte*, тада је сакупила више од 5000 активности постова у првом дану након његовог појављивања. Пост Росовског је одмах преведен на енглески, немачки, и бугарски. Наводно су блогери, који су истраживали докторову причу на Фејсбуку, открили да је слика са профила др Розовског у ствари са Севера Кавказа, од зубара који се користи у рекламној брошури стоматолошке клинике Џегмиска (*Ust Dzhegmiska Dental Clinic*). Убрзо након откриħа Радио Слободне Европе/Радио Слободе, *Фејсбук* налог Розовског пренео је саопштење да *овај садржај више није доступан* (Bērziņš et al., 2015). *Задављена трудница у згради синдиката у Одеси.* Појава фотографија наводно трудне жене коју су наводно задавили проукрајински екстремисти у Одеси. Ова информација је нашироко кружила друштвеним медијима док *KyivPost* није објавио резултате истраге о том питању доказујући њену фалсификованост. Рецензент медија из Москве, Елена Рибковтсева (*Elena Rybkovtseva*), испитивана је у тој истрази о томе зашто није постојала званична евиденција о преминулој трудници или део породице која тугује због тог догађаја. Лекар је прокоментарисао фотографију на којој је очито да се ради о старијој особи, женског пола, која је фотографисана у таквој пози да би вероватно био створен потребан ефекат. Лекар је наводно позвао медицинско особље, које је потврдило да нема трудница међу мртвима (Bērziņš et al., 2015). *Злочини украјинских екстремиста у источној Украјини.* У дужем временском периоду, друштвене мреже су биле преплављене гласинама о злочинима које су планирали проукрајински екстремисти. Радило се о следећој врсти прича: о затрованим залихама воде, концентрационим логорима који се граде изван Доњецка, фашистима, наоружаним људима који вребају у шуми и проукрајинцима који круже, циркулишу са отровом који се упија додиром. Првобитни продуцент ове вести је био државни *TV Channel One* у РФ који је приказао наводни исказ очевица како је трогодишњи дечак мучен и разапет од стране припадника оружаних снага Украјине на тргу у Славјанску.

---

[76] *Radio Free Europe/Radio Liberty*, енг. – организација основана од стране владе САД ради пропаганде спровођене у корист САД, а углавном против Руске Федерације, раније Савеза Совјетских Социјалистичких Република.

[77] Пост је имао следећу садржину: „Здраво. Моје име је Игор Росовскии. Имам 39 година. Живим у граду Одеси. Радим као лекар хитне помоћи 15 година. Јуче се, као што знате, догодила страшна трагедија у нашем граду, неки људи су убијали друге људе. Убили су их на зверски начин тако што су их живе спалили, не у пијаном стању, не да добију наследство своје баке, али зато што деле политичке ставове националиста. Прво су брутално тукли своје жртве, а затим их живе спалили. Као лекар, пожурио сам да помогнем онима које сам могао спасити, али су ме борци зауставили. Они ме нису пустили код рањеника. Један ме је грубо гурнуо, обећавајући да ћу и ја доживети као и други Јевреји што су доживели сличну судбину. Видео сам младића кога сам могао спасити да сам могао га превести у болницу, али моји покушаји убеђивања су наишли на ударац у лице када сам изгубио наочаре. За петнаест година мог рада видео сам много, али јуче сам хтео да плачем, не од ударача и понижења, већ због моје немоћи и неспособности да урадим нешто. У мом граду се такве ствари нису дешавале чак и за време најгорих времена нацистичке окупације. Питам се зашто свет ћути" (Bērziņš et al., 2015, p. 23).

У извештају је жена по имену Галина Пишњак (*Galina Pyshnyak*) тврдила да је била сведок наведеног злочина заједно са осталим становницима Славјанска, који су насилно доведени на централни трг од стране припадника оружаних снага Украјине како би пренели јавности све о извршењу овог злочина. У то време је разговарала за Први канал из избегличког кампа у руском региону Ростов. Овај снимак је широко распрострањен на друштвеним мрежама и убрзо су га пратиле контраинформације (на руској *TV Dozhd*) које оспоравају ову вест, па настоје доказати да је лажна. Руски новинар Јевгениј Фелдман из листа *Novaya Gazeta* отишао је на место наводног догађаја да провери – пита становнике, било да су били сведоци или чули о таквом зверству. У деветоминутном видеу објављеном на платформи *YouTube,* локални становници Словјанска доследно су негирали сазнање о било каквом сличном инциденту (Bērziņš et al., 2015). *Анализа твитера о кризи. Strategic Communications Centre of Excellence*, енг. – Североатлантског савеза је анализирао објаве на Твитеру у којима преовлађују осећања о ситуацији у Украјини за период од 15. априла до 15. јула 2014. године анализирана[78] су 26.254 твита на руском језику, да покрива Украјину (поготово Крим) и РФ. Твитови показују све већу поларизацију између проукрајинског и пророског Твитер корисника. Емоционална напетост на Твитеру се повећала, посебно након трагичних догађаја у Одеси и како је војна акција ескалирала. Идентификовано је 12,2% твитова као агресивних. Најагресивнију реакцију су изазвали извештаји људи жртве, употреба назива попут *фашиста* или *русиста*. Могуће је да су неки од агресивних твитова намерно пуштени да изазову мржњу. *Пророски корисници Твитера* имају доминантан утицај у следећим темама и областима, за ширење информација о кризи у Украјини са посебним акцентом на Твитер налозима јавних личности (телевизијски водитељи, глумци, новинари, опозициони лидери и др.), доминирање председника Путина и његове политике и ограничавање активности опозиције и независних медија, утицај пророских државних институција, невладиних организација, често коришћење активних облика твитовања (дељење мишљења, коментарисање, позивање на акцију, коришћење пропаганде, укључивање у дискусије и сл.). *Проукрајински корисници Твитера* су постали јачи у супротстављању пророским порукама стварањем нових информационих канала са значајним утицајем Твитера (нпр. *Stop Fake*) и више изражавања мишљења активног и убедљивог. Анализа је довела до закључка да је број лажних налога креирала група корисника, при чему сваки од њих има незнатан број пратилаца. Идентификована је и мрежа корисника Твитера са прилично високим утицајем Твитера који поново твитују и коментаришу једни другима твитове у циљу повећања видљивости. Пример једне такве групе коју формирају антиукрајински корисници (*swarog09, tohub, simonovkon*) који су стварали измишљене дискусије како би производили више твитова. Корелација између идеолошке базе, затим употребе традиционалних медија и развијене мреже корисника Твитера представља три кључна елемента за стицање утицаја у Твитер окружењу (Bērziņš et al., 2015). Можемо да констатујемо да тешко да је Украјина

[78] Твитови су одабрани на основу конкретних кључних речи које се односе на кризу у Украјини, користећи алат за аутоматско праћење друштвених медија – енг. *WebRadar*. Анализа је била фокусирана на твитове на руском језику пореклом из Украјине и РФ, као и било коју другу државу, ако је твит био на руском језику (нпр. Белорусија, Молдавија, Казахстан, Летонија итд.). Статистика о држави порекла била је заснована на информацијама које су дали корисници Твитера у њиховим рачунима (не мора бити тачно). Велики број корисника Твитера не наводи своје државе порекла, па се твитови могу постављати од стране сваког ко може да комуницира на руском језику (Bērziņš et al., 2015).

могла да са својим утицајем у информационо – телекомуникационим системима спроведе стварање надмоћи проукрајинских корисника твитер налога, тако да већ можда можемо да препознамо трагове ангажовања служби безбедности Запада у овом сегменту.

5.4.5. Резултат испољених активности

Званични документи на доктринарном нивоу у САД постављају за циљ супростављање пропаганди РФ. У буџету САД за 2016. годину, приоритет у европском правцу је јачање суверенитета и просперитета Украјине, а ради супротстављања Русији. Управни одбор телевизијског и радио емитера усваја образложење буџета наводећи да ће главни фокус рада у 2015. години бити „против Руске пропаганде која се ширила преко новинске агенције Русија Данас" (Шариков, 2020, p. 9). Управни одбор телевизијског и радио емитера тражио је да скоро четвртина (9 милиона долара у 2015. години) буде предвиђена за повећање трошкова емитовања на руском *Радио Европа*, у поређењу са 7,3 милиона колико је било одобрено у 2014. години. Стратегија извођења специјалних и информационих операција се заснива на блиској сарадњи, пре свега између делова Министарства одбране, Владе, Информационе агенције (енг. *United States Information Agency*) и служби безбедности САД. Прилагођавање заштите новим модерним условима светске политике – информационим технологијама, новим интернет могућностима и информационом простору, а првенствено недржавним актерима. Информационе операције су заправо израз *паметне моћи*, приказан као национална стратегија САД у будућности. У развоју и вођењу информационих операција постоји утицај како војне тако и цивилне технолошке инфраструктуре и јавних мишљења (Шариков, 2020).

Уколико пропаганда РФ није у стању да пласира њихову варијанту приче у западним медијима, онда ће једноставно измислити лажне цитате, вести. Довођење у љубавну везу познатих политичара[79] или уопште лица које је неопходно дискредитовати у јавности са конкретним особама, а да то није тачно, представљало је један од начина креирања лажне информације. У оваквим и сличним ситуацијама је огромна штета нанета било којој особи (улазак у приватни живот са лажима и обманама), јер је питање да ли деманти о оваквим и сличним вестима уопште имају ефекта након упознавања великог броја лица преко медија са сличним информацијама. Совјетске *активне мере* у пост – хладноратовском (1988–1991) периоду: Совјетски Савез је помогао да се покрене Индијски лист *Патриот* (*Patriot*; служба безбедности, Комитет државне безбедности је наведено реализовао) у циљу ширења совјетске пропаганде и дезинформација[80]. Савремена пропаганда РФ је подмлађена и трансформисана верзија која је примењена на савремену ситуацију са повећаном

[79] Украјински Премијер Арсениј Јацењук (*Arseniy Yatsenyuk*) оптужио је лидера Баткившчине (*Batkivshchyna*) политичке странке Јулије Тимошенко (*Yulia Tymoshenkoo*) за сексуално узнемиравање. Тврдило се да је извор за причу био интервју који је Јацењук дао новинарки руске службе (*Radio France Internationale*), Елени Серветаз (*Elena Servettaz*). Руска служба (*Radio France Internationale*) одмах је демантовала да је направила било какву такву пријаву (Fedchenko, 2016).

[80] Према наводима овог извора, у овим новинама су пласирани подаци о тврдњи да је влада САД била умешана у *стварање* сиде (*AIDS*) као део свог државног истраживања и развоја биолошког ратовања. Операција службе безбедности (енг. *operation infektion*) је тражила да оптужи САД да су намерно креирале вирус сиде у владиној лабораторији и потом га ширили (Fedchenko, 2016). Пре ширења дигиталних платформи друштвених медија за ширење дезинформација, Руси су користили тада омиљени механизам за ширење лажне приче – стављање чланка у новине на енглеском језику у Индији. Затим је, користећи шпијуне и сараднике, Комитет државне безбедности помогао да чланак преузму све кредибилније медијске куће, са циљем да га на крају покупи западна штампа. Једном у оптицају, информација би закомпликовала напоре да се разликује истина од фикције и посејала неповерење код западних лидера (Sipher, 2018). Касније су исте новине лажно тврдиле да су САД охрабривале Турску да заузме северни Ирак и др.

ефективношћу. Могуће је идентификовати 18 одвојених тема[81] дезинформација, пореклом из медија РФ, државних и приватних (Fedchenko, 2016).

5.5. ОДВРАЋАЊЕ ПУТЕМ ПАРАВОЈНИХ АКТИВНОСТИ

Када говоримо о паравојним активностима, у САД се у званичној терминологији користи појам паравојне операције. *Паравојне операције* (енг. *paramilitary operations*) могу бити дефинисане као тајне ратне активности. Оне су део ширег деловања служби безбедности у циљу манипулације догађајима у иностранству, када је то циљ државног руководства. Ове активности су познате под заједничким називом *тајна акција* (енг. *covert action*) или, алтернативно, *тајна операција, специјална активност, тиха опција, трећа опција* и сл. Поред паравојних операција – активности, енг. *covert action* укључује тајне политичке и економске операције, као и употребу пропаганде. Када се користи синергијски, сваки облик има за циљ да помогне у покретању тока историје, у правцу који је погодан за САД (Johnson, 2012). Обично се састоје од обезбеђивања новца, обуке, оружја, других материјала, обавештајних података, подршке руководству, а понекад и додатних бораца недржавним снагама[82] које су нерегуларне. Званичници *Беле куће* паравојну операцију одређују као ону која својом тактиком и својим захтевима за војним особљем, опремом и обуком, приближно подсећа на конвенционалну војну операцију. Може се предузети као подршка постојећој влади пријатељске државе према САД или подршка побуњеничкој групи у настојању да се сврге за САД непријатељска влада. Помоћ за такве операције може се уступити отворено, прикривено или комбинацијом ова два начина (Krishnan, 2018).

Када разматрамо паравојне активности у РФ, незаобилазна целина је војна служба безбедности, Главна управа (или некада познатија као Главна обавештајна управа), као и специјалне јединице оружаних снага РФ (*Spetznaz*) које су стекле значајно искуство у стварању и управљању локалним савезничким приватним војним компанијама (снагама). Ове снаге су врло често састављене од криминалаца, ратних вођа или бивших побуњеника које специјалци најчешће надзиру и обучавају, а по потреби им помажу у стварању нових јединица директно подређених војној служби безбедности Главна управа (некада Главна

---

[81] Анализом 500 ставки разоткривених дезинформација (лажних вести) аутор је идентификовао 18 главних тема које су према његовом истраживању, лажне нарације које су се обично користиле у пропагандне сврхе од стране припадника РФ. Ради се о следећим темама: „1. Државни удар и хунта коју подржава Запад, 2. Украјина као *фашистичка држава*, 3. Украјина као *пропала држава*, 4. Русија није део окупације/рата, 5. Украјинска војска, 6. Добровољачки батаљони, 7. Интерно расељена лица и избеглице у Русији, 8. Територијални распад Украјине, 9. Територијалне претензије од суседних земаља, 10. Лажна легитимизација анексије Крима и окупације Донбаса од стране владе, међународне организације или страних медија, 11. Рат у Украјини заправо воде САД, Североатлантски савез или приватници извођачи радова, 12. Пад подршке Запада Украјини, 13. Манипулисане међународне организације, 14. Украјина и Европска унија, 15. Распад Европске уније, пропадање САД и Запада уопште, 16. лет број 17 Малезија авиопревозника, 17. СИДА/друге приче о болестима, 18. Украјина/Турска/Сирија/ИСИС" (Fedchenko, 2016, p. 158).

[82] *Недржавни актер* означава несуверени ентитет који: врши значајну политичку моћ и територијалну контролу; ван је контроле суверене владе; и често користи насиље у остваривању својих циљева (енг. *22 U.S. Code § 6402 – Definitions*). *Недржавне снаге* су „специфичне паравојне снаге, извођачи радова, појединци, предузећа, стране политичке организације, отпорне или побуњеничке организације, исељеници, транснационални противници тероризма, разочарани припадници транснационалног тероризма, трговци на црном тржишту и други друштвени или политички непожељни чланови са циљем покретања, учествовања или манипулисања (унутрашњим) оружаним сукобом, или постизања неких других политичких, војних или економских циљева" (Krishnan, 2018, p. 1).

обавештајна управа). Током Другог чеченског рата у Русији (1999–2009), Главна обавештајна управа је заједно са другим службама безбедности, као што је Федерална служба безбедности, управљала са неколико локалних проруских чеченских јединица, које су се показале ефикасним против чеченских побуњеника (Bowen, 2021).

Када говоримо о паравојним активностима, у РФ је тешко заобићи сегмент приватних војних компанија више деценија уназад (а поготово једну до две деценије), које су се појављивале широм света у разним сукобима. У званичном извештају конгреса САД наведено је да се верује да Влада РФ све више користи приватне војне компаније ради остварења пројекције своје моћи, на много јефтинији начин. Активности које предузимају приватне војне компаније често делују у спрези са разним недржавним локалним актерима, припадницима полиције, добровољцима, криминалним групама и другим структурама. Раст велике домаће индустрије приватне заштите је настао после 1990. године када је доста припадника система безбедности остало без посла (бивши војници, припадници елитних специјалних снага и припадници служби безбедности). Оваква и њима слична лица су формирала разна удружења са ветеранима својих старих јединица и стварали нове приватне компаније за обезбеђење. У одређеном периоду, ове фирме и удружења почеле су да послују, односно покушавале су да послују на међународном пословном тржишту, међутим, наишле су на оштру конкуренцију западних приватних безбедносних компанија (ову *оштру конкуренцију* западних безбедносних компанија, дефинитивно у овом извештају конгресу САД можемо схватити на више начина – прво, да су западне службе безбедности још доста раније и са већим средствима почеле са овим и сличним пројектима или друго, да се истакне значај већ преузетих активности служби безбедности запада, а можда и трећа варијанта која би представљала комбинацију ова два наведена, прим. аут.). Законом из 1996. године је забрањено држављанима РФ да учествују у оружаним сукобима у иностранству ради остваривања финансијске добити. Приватне војне компаније су наводно и даље незаконите по законима РФ (Bowen, 2020). Колико се наведено примењује, видећемо у наредном делу истраживања, јер је другим нормативима регулисана могућност учешћа у приватним војним компанијама.

Коришћење војних и паравојних снага од стране РФ ради спровођења спољно – политичких државних интереса је интензивирано од 2014. године. На Криму је РФ користила ваздушно – десантне и специјалне оперативне снаге назване *мали зелени мушкарци* или *љубазни људи* да заузму територију у фебруару 2014. године. У источној Украјини је у почетку РФ распоредила оперативце служби безбедности да подрже развој сепаратистичког покрета, да би затим распоредили конвенционалне војне снаге да их подрже. Међутим, поред конвенционалних снага, РФ се ослањала на невладине заступнике РФ, као што је *Вагнер*, приватна војна компанија у Украјини и Сирији. Будуће (пара)војне акције се ослањају на лаке пешадијске снаге, укључујући првенствено ваздушно – десантне снаге оружаних снага РФ, Главне управе – Спецназ. Услови за ефикасну војну активност, предузимање необавештајних активности, захтевају: географску близину, слабу контролу граница, слабу контраобавештајну службу, недостатак јаких савезника, лак приступ ватреном оружју, друштвено – политичке поделе и елемент изненађења (Radin, Demus & Marcinek, 2020).

5.5.1. Историјски приказ паравојних активности

Посматрајући корене паравојних активности у САД, да бисмо размотрили историјски приказ настанка првих (претеча) приватних војних компанија, потребно је сагледати шта је још пре самог формирања САД за потребе ослобађања од колонијалне власти реализовано од стране служби безбедности државе која је тек требало да се формира – САД и Француске. Први агент *Комитета за тајну кореспонденцију*, Артур Ли, лекар у Лондону, 1776. године се као тајни представник северноамеричких колонија састао у Лондону са француским обавештајцем и будућим аутором књижевног бестселера *Фигарова женидба*, Пјером Огистеном Карон де Бомаршеом. Артур Ли је успео да убеди „писца" у потребу француске помоћи побуњеним колонијама у Новој Енглеској. После разговора са Бомаршеом, 29. фебруара 1776. године, послао је поруку француском краљу Лују XVI, у којој је позвао монарха да пружи тајну помоћ северноамеричким колонијама у њиховом рату за независност и закључи тајни трговински споразум са колонијама. Према Бомаршеу, Француска би могла да пружи такву помоћ без нарушавања сопственог угледа, а успех целог догађаја зависио би и од брзине одлуке и од тога колико би у тајности могла да се чува сарадња Француске и побуњених колонија. У Бомаршеовој поруци је изнесен план помоћи Американцима, у којем је први корак био успостављање трговинских односа. Бомарше је предложио стварање трговачке компаније која би трговала са северноамеричким државама. Под маском такве компаније, према писцу, Француска би могла тајно да помаже побуњеницима. Луј XVI је подржао предлог и дао Бомаршеу милион ливра за организовање трговачке компаније. Са овим новцем, Бомарше је наводно основао трговачку фирму под називом *Roderigue Hortalez et Cie*, а радило се у ствари о претечи данашњих приватних војних компанија, којом је руководила, планирала, организовала и реализовала задатке служба безбедности Француске. Преко формиране компаније, Бомарше је снабдевао побуњеничке колоније барутом и муницијом, склапао споразуме са капетанима маркираних бродова и врбовао кандидате из реда француских официра. На северноамерички континент допремано је и француско оружје које је купљено од наводно расположивих „вишкова" француске војске и затим транспортовано трговачким бродовима компаније (Юрьевич, 2014).

Још 1951. године, директивом енг. *National Security Council 10/5* не само да је потврђен и одобрен наставак тајних акција, операција, већ је наређено интензивирање истих са нагласком на слабљење моћи Савеза Совјетских Социјалистичких Република, Кине, затим ојачање оријентације народа и нација слободног света према САД и повећање њиховог капацитета и воље да се одупру совјетској доминацији. Даље, Савет за националну безбедност САД даје задатак службама безбедности (директору Централне обавештајне агенције који ће одлучивати о обиму, редоследу, темпу операција, обезбеђивању адекватног особља, средстава и др.) да развијају подземни отпор како би се олакшале тајне и герилске операције у стратешким областима у највећој могућој мери и обезбедила доступност ових снага у случају рата за употребу у складу са принципима које је утврдио Савет за националну безбедност (National Security Council 10/5, 1951). Савет за националну безбедност је доделио обавезу Одбору за психолошку стратегију да обезбеди да његов стратешки концепт националног психолошког програма укључује одредбе о тајним операцијама које су осмишљене за постизање горе наведених циљева. Савет за националну безбедност тражи да се обезбеде адекватна средства помоћу којих би се директор Централне обавештајне агенције могао уверити у савете и сарадњу у формулисању планова за паравојне операције током

периода хладног рата. Савет за националну безбедност овлашћује спровођење проширених герилских активности у Кини, а према одговарајућим одредбама директиве енг. *National Security Council 48/5* која регулише наведену проблематику (National Security Council 10/5, 1951).

У нормативима оружаних снага САД је прописано да је *нерегуларно ратовање* насилна борба између државних и недржавних актера за легитимитет и утицај на релевантну популацију/е (Training and Doctrine Command G2 Handbook No. 1.08, 2010). Нерегуларно ратовање фаворизује индиректне и асиметричне приступе иако може користити читав низ војних и других способности, како би нарушило моћ, утицај и вољу противника. Нерегуларне снаге интегришу информациони рат у све своје операције. Учесници у савременом оперативном окружењу сведоче о сталном порасту нивоа технологије које се користе у комуникацијама, системима аутоматизације, извиђања и стицања циљева. Да би се обезбедило успешно коришћење информационих технологија и да се непријатељу ускрате предности које пружају такви системи, нерегуларне снаге наставиће да развијају своје способности за вођење информационог рата (енг. *Infowar*). „Информациони рат је посебно планиран и обухвата интегрисане радње које се предузимају за постизање информационе предности у критичним тачкама и времену. Циљ информационог рата је да утиче на непријатеља, његово доношење одлука путем његових прикупљених и доступних информација, информационих система и процеса заснованих на информацијама, уз задржавање способности коришћења пријатељских информација, процеса заснованих на информацијама" (Training and Doctrine Command G2 Handbook No. 1.08, 2010, p. 30). Задаци и ефекти информационог ратовања су следећи: уништити, деградирати, ометати, одбити, преварити, експлоатисати, испољити утицај (информација кроз форме дезинформације и манипулација подацима). Елементи информационог ратовања су: електронско ратовање, обмана, физичко уништење, мере заштите и безбедности, управљање перцепцијом, рат рачунарима и информациони напад (Training and Doctrine Command G2 Handbook No. 1.08, 2010).

Процена је да су службе безбедности САД, првенствено Централна обавештајна агенција, спровеле стотине тајних акција током Хладног рата од којих је у 63 паравојне операције циљ био свргавање *непријатељске владе* (непријатељске по процени САД). У наредном делу истраживања је наведено 25 паравојних операција (битније операције из Хладноратовског – 15 и Постхладноратовког периода – 10, види *Табелу 12*) које су спровеле службе безбедности САД. Поред наведених операција, спроведен је и низ операција (које нису овде приказане) које су обухватале учествовање у борби против нарко – мафије, тероризма и других претњи, према процени служби безбедности САД теже видљивих, па самим тим и теже мерљивих. Велика већина истраживача који се баве овом проблематиком (тајних акција САД) ограничавају се на праћење тајних акција Централне обавештајне агенције током Хладног рата, што може створити погрешан утисак да тајна акција у Постхладноратовском периоду није релевантна појава, тако да ће приказ следећих паравојних активности демантовати ову констатацију. Постхладноратовске (и данашње) паравојне операције углавном следе методологију можда и оних најранијих тајних акција које је Централна обавештајна агенција спроводила средином XX века уз адаптацију нових технологија (Krishnan, 2018).

Табела 12. Паравојне операције разматране у овом делу истраживања.

Држава (период)	Ангажовање службе безбедности – државе у паравојној активности
Албанија (1949 – 53)	Централна обавештајна агенција је убацила агенте у Албанију да створи мрежу отпора и води герилски рат против комунистичког режима под Енвером Хоџом (енг. *Operation Valuable*).
Украјина (1949 – 53)	Централна обавештајна агенција је покушала да поново активира антисовјетске групе отпора у Украјини које су биле активне током Другог светског рата за вођење герилског рата против комунистичке владе.
Бурма/Јужна Кина/Кореја (1950 – 53)	Централна обавештајна агенција је транспортовала паравојне борце са Тајвана у Бурму да се инфилтрира у кинеску провинцију Јунан и дестабилизује комунистички режим (енг. *Operation Paper*), и Централна обавештајна агенција и Пентагон су спровели паравојну операцију против Севера Кореје обучавањем и убацивањем јужнокорејских герилаца на север током Корејског рата.
Гватемала (1954)	Централна обавештајна агенција је регрутовала и обучила неколико стотина плаћеника, трупе под командом *Castillo Armas*, да сврги председника Гватемале *Jacobo Arbenz* (енг. *Operation PBSUCCESS*).
Тибет (1958 – 74)	Централна обавештајна агенција је обучавала и опремала тибетанске борце за слободу како би отерали кинеске трупе са Тибета, који су окупирали 1950. године
Индонезија (1958)	Централна обавештајна агенција је покушала да сврге председника Индонезије *Sukarno* спонзорисањем побуњеничке групе Перместа да води герилски рат против власти (енг. *Project HAIK*).
Куба (1961)	Централна обавештајна агенција је обучила и наоружала Кубанску изгнаничку бригаду 2506, која је слетела у Залив свиња у априлу 1961. године (енг. *Operation JMATE*).
Конго (1960 – 68)	Централна обавештајна агенција је спонзорисала неуспели покушај атентата на *Patrice Lumumba*, затим је подржавала побуњенике сепаратистичке Владе Катанга под *Moise Tshombe*, и на крају је подржан Конгоански моћник *Mobutu* против побуњеничких снага.
Северни Вијетнам (1962 – 74)	*Military Assistance Command, Vietnam,* енг. – *Studies and Observations Group*[83] је обучавао и убацивао Вијетнамске агенте у Северни Вијетнам да изгради мрежу отпора и олакша побуну на северу (енг. *Project TIGER*).
Лаос (1955 – 74)	Централна обавештајна агенција је обучила и наоружала Лаоска племена Хмонг за борбу против комунистичког побуњеника *Pathet Lao* (који је завршио преузимањем контроле над земљом) и да дирigује прекограничне рације у Северном Вијетнаму.
Ирак (1972 – 75)	Централна обавештајна агенција је наоружала и финансирала Ирачке Курде заједно са Ираном и Израелом како би дестабилизовали Ирак и натерали Ирак да направи уступке у својим односима са Ираном. Курди су били напуштени након што су Ирански дипломатски циљеви постигнути.
Ангола (1975 – 90)	Централна обавештајна агенција је обучавала и наоружавала енг. *The National Front for the Liberation of Angola*[84] и касније енг. *The National Union for the Total Independence of Angola*[85] у Анголи да се бори против комуниста и кубанске/совјетске подршке енг. *Popular Movement for the Liberation of Angola*[86] владе (енг. *Operation IA FEATURE*).

[83] *Military Assistance Command, Vietnam – Studies and Observations Group,* енг. – Команда војне помоћи, Вијетнам – Група за проучавање и посматрање је била јединица за специјалне операције САД која је водила тајне, паравојне (неконвенционалне) операције пре и током Вијетнамског рата (Krishnan, 2018).

[84] *The National Front for the Liberation of Angola,* енг. – Национални ослободилачки фронт Анголе, милитантна организација која се борила у рату за независност од португалске колонијалне власти у Анголи, под вођством Холдена Роберта. Национални ослободилачки фронт Анголе су помагале многе владе, па и САД (Krishnan, 2018).

[85] *The National Union for the Total Independence of Angola,* енг. – Национална унија за потпуну независност Анголе друга је највећа странка у Анголи. Основана је 1966. године у току борбе за независност од Португалије када се борила заједно са Народним покретом за ослобођење Анголе против португалске власти, а од 1975. до 2002. године против Народног покрета за ослобођење Анголе, у грађанском рату (Krishnan, 2018).

[86] *Popular Movement for the Liberation of Angola,* енг. – Народни покрет за ослобођење Анголе – Партија рада је партија на власти у Анголи од њене независности од Португалије 1975. године. Чланови Народног покрета за ослобођење Анголе борили су се против португалске колонијалне армије у Анголском рату за независност, а

Држава (период)	Ангажовање службе безбедности – државе у паравојној активности
Јужни Јемен (1979 – 82)	Централна обавештајна агенција је обучила и наоружала малу групу агената из Северног Јемена, који су убачени у Јужни Јемен, који је у то време био савезник Кубе и Совјетског Савеза.
Чад (1981 – 82)	Централна обавештајна агенција је обучавала и наоружавала Чадске борце отпора под командом *Habre* да свргну про – Гадафијеву владу у Чаду и да потисне Либијске трупе из Чада.
Никарагва (1981 – 86)	Централна обавештајна агенција је обучавала и наоружавала бивше припаднике свргнуте *Somoza* владе (познате као *Contras*) да дестабилизују владу социјалистичке и про – совјетску *Sandinistas* у Никарагви.
Авганистан (1979 – 89)	Централна обавештајна агенција је обучавала и наоружавала (преко свог регионалног савезника Пакистана) муџахедине да потисну совјетске окупационе снаге из Авганистана и да збаци про – совјетску владу (енг. *Operation CYCLONE*).
Ирак (1992 – 96)	Централна обавештајна агенција је планирала државни удар и народни устанак против Ирачког моћника Садама Хусеина заједно са Ирачким Националним конгресом (енг. *Project ACHILLES*). Део плана било је наоружавање потлачених Курда и Шитских група.
Босна и Херцеговина (1994 – 95)	Централна обавештајна агенција и Пентагон су давали оружје паравојним формацијама, снагама које је предводио лидер муслимана Алија Изетбеговић, док су америчке приватне војне компаније енг. *Military Professional Resources Inc*[87] обучавале Хрватске снаге, а ради супротстављања Србима.
Судан (1996)	Централна обавештајна агенција је пружила подршку побуњеницима енг. *Sudan People's Liberation Army*[88] под *John Garang* у Јужном Судану од 1983. године и појачала настојања 1996. године да се збаци Влада у Картуму слањем оружја и Делта јединица.
Косово и Метохија (1996 – 99)	Централна обавештајна агенција је обучавала и наоружавала терористичку организацију *Ослободилачку војску Косова* (углавном преко свог регионалног савезника Немачке) да ослаби Србију и евентуално да обезбеде подршку свргавања легално изабраног председника Републике Србије, Слободана Милошевића.
Авганистан (2001)	Централна обавештајна агенција и Пентагон обезбедили су средства, оружје, и особље за специјалне операције Северној алијанси како би збацили Талибански режим непосредно после 11. септембра (енг. *Operation ENDURING FREEDOM*).
Сомалија (2002 – 2006)	Централна обавештајна агенција је плаћала и на други начин подржавала Сомалијске ратне вође ради борбе против џихадиста у Сомалији. Они су формирали Алијансу за обнову мира и борбу против тероризма, који је покренуо војни напад на енг. *Islamic Court Union* владу 2006. године.
Иран (2005 – 2008)	Централна обавештајна агенција је настојала да свргне Исламску Републику у Ирану покушавајући да сарађује са иранским побуњеницима/отпором, групама, пре свега иранска политичко – милитантна организација[89]. Борци иранске политичко – милитантне организације су били доведени у САД на обуку.

после тога су постигли победу и против покрета Национална унија за потпуну независност Анголе и Националног ослободилачког фронта Анголе у Анголском грађанском рату (Krishnan, 2018).

[87] Војни професионални ресурси (енг. *Military Professional Resources*), приватна је војна компанија основана 1987. године у САД од стране бивших високих официра оружаних снага САД. Пентагон је компанију ангажовао 1995. године за обуку специјалних јединица Хрватске војске (Хрвата) и 5. корпуса Армије БиХ (Муслимана) пре почетка операције *Олуја*, која се завршила уништавањем Републике Српске Крајине и протеравањем Срба, који су били присиљени да напусте своје куће и домаћинства како би преживели (Krishnan, 2018).

[88] Суданска народноослободилачка војска (енг. *Sudan People's Liberation Army*) – некада, од 1983. године до 2017. године, основана као герилски покрет против Владе Судана, а од 2017. године дошло је до реструктурирања и Суданска народноослободилачка војска је преузела име Јужне суданске обрамбене снаге, уз још једну промену у 2018. години у Народне одбрамбене снаге Јужног Судана (Krishnan, 2018).

[89] Организација народних муџахедина Ирана или Муџахедин Калк је иранска политичко – милитантна организација (енг. *The People's Mujahedin Organization of Iran, also known as Mujahedin – e – Khalq or Mujahedin – e – Khalq Organization*), заснована на исламској и социјалистичкој идеологији и заговара рушење руководства Исламске Републике Иран и успостављање властите владе (Krishnan, 2018).

Држава (период)	Ангажовање службе безбедности – државе у паравојној активности
Либија (2011)	Централна обавештајна агенција и Стејт департмент су обучавали и наоружавали Либијске побуњенике који су се појавили у сенци Арапског Пролећа са експлицитним циљем да сврге Либијског владара, Гадафија.
Сирија (2012 – 2018; када је објављено истраживање)	Централна обавештајна агенција и Пентагон обучавали су и наоружавали Сиријске опозиционе снаге са двоструком сврхом, рушења председника Асада и за пораз *ISIS*, који се појавио у лето 2014. године као велику претњу миру и безбедности у региону (енг. *Operation TIMBER SYCAMORE*).

Извор: Krishnan, 2018, p. 21–23.

Поред наведених активности, Централна обавештајна агенција је за потребе САД водила тајне акције у Европи, Азији, Африци и Латинској Америци, укључујући пуч против Мохамеда Мосадика у Ирану (Мосадик је свргнут активностима служби безбедности САД и Велике Британије, августа 1953. и уместо њега је постављен генерал Фазлула Захеди, што је Централна обавештајна агенција признала 2013. године, дакле тек 60 година касније), Лумумбино убиство[90] у Конгу, и рат који је био у току у Авганистану током вршења овог истраживања (Соу, 2021). Одражавајући значај југоисточне Азије за операције Централне обавештајне агенције, њени припадници су посебно изучавали: побуну комуниста на Филипинима, дестабилизацију Сукарновог режима у Индонезији, пацификацију у Јужном Вијетнаму и тајни рат у Лаосу, тврдећи да су последње две операције кључне за разумевање савремених сукоба у Авганистану и Ираку (Соу, 2021).

Фелштински и Литвиненко (*Felshtinsky and Litvinenko*) су у свом истраживању дошли до већег броја показатеља тј. примера примене необавештајних активности служби безбедности РФ у периоду после хладног рата. Наиме, 1993. године аутор наводи активности *Узбекистанске четворке*. Радило се о лицима где су сва четворица били Руси, пореклом из Узбекистана, бивши припадници специјалних јединица, обучени у савршеном коришћењу оружја и импровизованих предмета који би се могли користити као бомбе. Према наводима аутора, специјалност ове групе је била реализација наручених убистава и они су спровели двадесетак убистава у Москви, Санкт Петербургу, Липецкну, Тамбову, Архангелску и другим градовима. Жртве унајмљених убица су били мањи тајкуни, банкари, велики бизнисмени и друга лица. Вођа ове групе је имао надимак Ферганец и исти је ухваћен са лажним документима, приликом преласка таџикистанско – киргистанске границе. Према њиховим сазнањима Ферганец је тражен због сумње за убиство. На испитивању Ферганец је упознао истражне органе где су у Киргистану сакривени остали чланови групе. Следеће,

[90] Након убиства 1961. године, Лумумбино тело је раскомадано и уништено киселином. Белгијски званичници деценијама касније одузели су зуб ћерки комесара белгијске полиције који је, према њеним речима, узео зуб кад је надгледао уништавање Лумумбиног тела (Radio Slobodna Evropa, 2022). Пре две године, тужилаштво је саопштило да није сигурно да је зуб заиста Лумумбин, јер нису могли да ураде тест на дезоксирибонуклеинску киселину. Лумумба је за многе симбол борбе афричких народа против колонијализма. У Демократској Републици Конго је након Лумумбиног убиства завладала вишедеценијска диктатура која је опустошила земљу (Radio Slobodna Evropa, 2022). Након што се залагао за окончање колонијалне владавине, Лумумба је 1960. године постао први премијер независне Демократске Републике Конга. Међутим, историчари наводе да је током Хладног рата пао у немилост Белгије и САД, јер је затражио помоћ од Совјетског Савеза у гушењу сецесионистичког покрета у региону Катанге. Када је диктатор Мобуту Сесе Секо преузео власт војним ударом касније те године, западне силе су интервенисале и Лумумба је ухапшен. Иако су га убили сепаратисти, сматра се да су у убиству учествовале Белгија и САД због његових веза са Совјетским Савезом (Radio Slobodna Evropa, 2022).

Петербуршка група: реализован је низ убистава, а посебно битни у структури групе су били бивши поручник, стар 40 година, Владимир Борисов (звани *Легенда*) и бивши капетан тенка Јурий Бириченко (звани *Бирук*). Истрагом је установљено да је тренинг гађања извођен у околини Санкт Петербурга и техника у спољашњем осматрању као и обучавању у порицању, слушању и обради телефонских разговора. Сваки борац Бириченков је био опремљен најновијим средствима и опремом за реализацију субверзивних делатности и то: пејџер, радиотелефон, посебна техничка средства, имали су по неколико комплета докумената, носили су тајне кодове за употребу система као и за комуникацију са другом, пријатељем. Бириченко и чланови његовог тима су ухваћени широм РФ док се Бирченко дуго скривао у Прагу, где је ухапшен уз помоћ Интерпола. Убице су примале плату око 200 – 500 долара месечно, а за сваки и мањи задатак су примали бонус две хиљаде долара. Истрага је теретила Борисова, Бирченка и Кустова за четири наручена убиства, бандитизам, изнуду и друге тешке злочине док је остатак чланова групе био осумњичен за скоро сва убиства високог профила на територији Санкт Петербурга и северозапада, почев од јесени 1997. године. Аутори овог истраживања потврду деловања службе безбедности виде у изјави начелника оперативно – истражне групе, Вадима Поздњака, који је изјавио да „ако бисмо били ослобођени од осталих актуелности, вероватно бисмо имали више од једно десетак епизода криминалног деловања ове банде" (Felshtinsky & Litvinenko, 2002, p. 230). Лазовски је 1995. године по угледу на *Узбекистанску групу* створио нову групу, која се састојала од ветерана. Група је радила четири године. *Извођач радова* групе је по свему судећи био Марат Васиљев који је 1999. године ухапшен и осуђен на 13 година затвора за убиство Алијева 1993. године, власника трговачког реда на пијаци Либлин (ово је једино дело, злочин, за који је Васиљев осуђен). У јесен 2000. године Борисов је приведен, затим и остали припадници групе. Нико од окривљених не признаје наводна кривична дела. Током једне од ликвидација у хотелу у Москви, напуштајући хотел, Борисов се обратио чувару приликом изласка из хотела: „тамо неко пуца, а ти овде спаваш" (Felshtinsky & Litvinenko, 2002, p. 232). У року од пар дана учесници убиства су већ били у Чеченији. У 1998. години рад започиње Моревова посебна група. Морев је служио у Чеченији, у извиђачком батаљону 8. пука специјалних снага (војна јединица). Током реализације војног задатка, Морев је починио кривично дело због којег је војно тужилаштво хтело да га терети, али се тада појавио пуковник из Федералне службе безбедности који Мореву нуди ангажовање за службу безбедности или да иде у затвор. Морев је прихватио ангажовање за потребе службе безбедности и добио кодни назив *Слав*. Отпуштен је у резервни састав и послат кући, у Рославл. Две године није контактиран, све до 1998. године када је позван у Москву. У специјалној групи било је дванаест људи, а сви су наводно прошли поступак врбовања да раде за потребе службе безбедности у замену за опрост грехова. Главни задатак групе је био елиминација посебно опасних злочинаца. Група је задатке извршавала како у РФ, тако и у другим земљама: у Ираку, Украјини, Молдавији и другим. Задатке су извршавали у групама од две или три особе, на високо професионалан начин. Ради обуке, наставе, група се окупљала једном недељно, у московском стану на адреси у стану станара жене са дететом. Групу је на овој адреси дочекао припадник службе безбедности РФ – Федералне службе безбедности, по имену Вјачеслав (никада није поменуо своје презиме). Свим члановима групе су дата лажна имена и презимена ради прикривања доказа. Тако је Морев имао три пасоша (на имена Андрej Алексевич Расторгујев, Козлов

Михаил Васиљевич, Зимин Александр Сергејевич). Група није нигде евидентирана и самим тим формално није ни постојала (Felshtinsky & Litvinenko, 2002).

Отмице становника као један од метода присиле је врло честа појава и иста се спроводи најчешће преко лица из одређених криминалних кругова који су већ дужи временски период лојални служби безбедности, а ради остварења одређених циљева одвраћања на највишем државном нивоу. Планирање, организовање и спровођење оваквих акција, операција се спроводи у највећој тајности у односу на контакте припадника криминалних група и припадника службе безбедности ради лакшег оповргавања евентуалне осуде служби безбедности и државе у спровођењу акција.

Следећи примери би се могли довести у везу са тајним службама безбедности, тачније са Федералном службом безбедности: Мухамед Келигов је рођен 1955. године, а преминуо 15. септембра 1998. године у месту Малагобек. Отет је од стране чеченске криминалне групе из Грус – Мартана и захтеван је откуп од 5 милиона долара. Радило се о криминалној групи браће Вараев који су у једној заседи страдали, па је размена (након годину дана) Келигова извршена 31. августа 1999. године. Други чеченски киднапери су били Арби Бараев из Алхан – Кали (Рмоловки), Ризван Читигов, Апти Абитајев, Идрис Межицов (Абдул – Малик), Аслан Гачајев (Абдула) и други. По мишљењу Руслана Кхусупова, Чечена, бившег официра совјетске, а потом и руске армије, доктор наука у Чеченији, Бараев, без сумње је радио за руске службе безбедности, које су заузврат бринуле о Бараеву и његовим људима. Тако је средином јула 2000. године Усупов Магомет пренео поруку да ко буде желео да контактира Федералну службу безбедности и да проследи информације, да иде код Бараева. Бараев се сматрао одговорним за хватање на десетине талаца. У договору са Федералном службом безбедности, Аслан је пристао да преда Бараева без новца, у замену за амнестију. Након овог догађаја Бараев се појављује у дистрибуцији лажних кинеских долара и више пута је прозиван и у медијима као агент Комитета државне безбедности или Федералне службе безбедности и истицано је да уколико је неком потребна заштита, треба да се обрати Бараеву. Бараев је наводно убијен у периоду између 22. и 24. јуна 2001. године у свом родном селу Алкханкали током једне операције, водећи један тим састављен од више државних структура РФ, а између осталих и Федералне службе безбедности. Бараев је према извештајима медија био најпознатији отмичар, а његову ликвидацију опет доводе у везу са Федералном службом безбедности, наводно зато што се ради о особи која је много тога знала и извршавала доста послова за потребе Москве, чиме је постао већ исувише опасан за појединце и систем. Дописник *Радио Свободе*, руски држављанин Нин Андрej Бабицки је отишао у Чеченију и завршио у логору где је мучен. Затим је 2. фебруара ослобођен и онда пронађен у врећи. Чудна је прича и са смрћу представника америчке добротворне медицинске организације, Кенета Глука, 9. јануара 2001. године у области села Старие Атаги. Тајне службе РФ су презирале Глука, а 18. априла 2001. године на конференцији за новинаре је постало јасно да га званичници РФ сматрају сарадником тајних служби безбедности САД. Глук је прво отет, па је исцењирано његово наводно ослобађање од Федералне службе безбедности. Барата се са податком да је око 120 лица отето у Грозном и било мучено у привременом одељењу унутрашњих послова, а зграду су касније сами полицајци подигли у ваздух да би уништили доказе о мучењу и убијању у згради (Felshtinsky & Litvinenko, 2002).

Приватне војне компаније појмовно се према делу теоретичара из Републике Србије одређују као компаније које извршавају одређене услуге (које су углавном спадале у домен

војних снага) за профит, а обухватају војну обуку, логистику, обавештајне, контраобавештајне и необавештајне активности, извођење борбених дејстава као и пружање других безбедносних услуга у разним зонама на планети (Лабовић, 2015). Данас егзистира велики број приватних компанија у свету, помиње се чак и број од више десетина, па и више од 100 приватних војних компанија. Најчешће, ове компаније[91] долазе из САД, Велике Британије, Северне Ирске, Француске и Израела (Лабовић, 2015).

Приватне војне компаније често ради прикривања учешћа и избегавања последица које следе уколико дође (а врло често долази) до чињења недозвољених делатности припадника оваквих компанија, а за потребе државе, делују у другим државама (нпр. раније у Ираку, Авганистану, а сада у Украјини, Централноафричкој Републици и др.). Приватизација безбедности представља врло плаћен посао, а све више демократских влада жели да смањи ризик губитака људства у евентуалним ратним операцијама (ангажујући спремне, најчешће материјално мотивисане, најквалитетније опремљене и пре свега дискретне припаднике компаније). Медијски најпознатија и може се слободно констатовати једна од активнијих, ако не и најактивнија у протеклом периоду, била је приватна војна компанија *Блеквотер САД* (енг. *Blackwater USA*), сада већ под другим називима, која је учествовала у пословима највишег безбедносног нивоа у земљи и иностранству (Мијалковић, 2010). Врло често су се у медијима помињале оптужбе на рачун ове компаније и то за више масакара цивилног становништва у Ираку. Све ово је правдано под покровитељством заштите дипломата САД у Ираку. Ангажмани ове компаније обухватају милионске цифре изражене у доларима, а сличним активностима се баве и многе друге[92] компаније. Неке од ових компанија из САД су биле активно присутне и у сукобима на Балкану. Наиме, приликом планирања и реализације операције „Олуја" 1995. године, приликом чега је настао највећи егзодус српског народа у новијој историји, ангажована је компанија *Војни професионални ресурси* (енг. *Millitary Professional Resources Inc*[93]) из САД, а 1999. године, иста компанија је вршила обуку

---

[91] Најпознатије приватне војне компаније су: енг. *DynCorp International Inc.* (основана је 1946. године у САД); енг. *Blackwater* (основана 1997. године у САД, која током 2009. године, назив *Blackwater* мења у назив енг. *Xe Services LLC*, а од децембра 2011. године у енг. *Academi* – да би се касније припојила другој компанији под новим именом); енг. *Military Profesional Resources Incorporated – MPRI* – 1987. године основана од стране пензионисаних војних официра оружаних снага САД, са око 3.000 запослених и седиштем у близини Вашингтона (Лабовић, 2015). Ради се о приватној војној компанији која је била присутна на просторима бивше Социјалистичке Федеративне Републике Југославије, односно 1994. године је склопила уговор са Владом Републике Хрватске ради побољшавања способности оружаних снага Републике Хрватске. *Military Profesional Resources Incorporated,* енг. је са овим програмом започела активности у јануару 1995. године); енг. *Vinnell Corporation* (САД); *Armor Group* (Велика Британија); *Erinys International Ltd* (Велика Британија, Јужна Африка); *Control Risks Group* (Велика Британија) и друге (Лабовић, 2015).

[92] Следеће приватне војне компаније су такође помињане као актуелне у овим пословима: енг. „*Armor Group International, Phoenix CP, Cubie Defence Applications, Golan, Kroll, Sandline Internacional, Triple Canopy, Control Risks, Dyc – Corp, Erinys, Executive Out – Comes, Global Strategies Group, Formerly Global Risks Strategies, Olive Group, Vinnell*" где део њих испуњава изузетно високе стандарде за извршавање додељених војних задатака (Мијалковић, 2010, стр. 259).

[93] Војни професионални ресурси, компанија (енг. *Millitary Professional Resources Inc.*) осмислила је стратегију напада на српске положаје и насеља у Републици Хрватској и извршила набавку оружја и оруђа за реализацију ове операције. Такође, ова компанија је вршила лобирање код највиших званичника САД за спровођење подршке државном руководству Републике Хрватске (Мијалковић, 2010). Војни професионални ресурси, компанија је основана 1987. године, као независна компанија, али је 2000. године постала власништво групе Л–3 Корпорације за комуникације (енг. *L–3 Communications Corporation*) која броји преко 60 компанија. Проширила је своје делатности и услуге од војне обуке до управљања у ванредним ситуацијама, стратешко

припадника тзв. Ослободилачке војске Косова да би касније пројектовали тзв. Косовске снаге безбедности, формиране почетком 2009. године (Мијалковић, 2010). Нису ретки ни покушаји свргавања или свргавање државника од стране компанија као што је почетком 2009. године покушала компанија енг. *Sandline Internacional*[94] у Гвинеји. У истој години, осујећен је и планирани атентат на боливијског председника[95] (Мијалковић, 2010).

Можемо да констатујемо да са приватном војном компанијом *Игзекјутив аутками* (енг. *Executive Outcomes*[96]), која је употребљавана у конфликтима у Анголи и Сијера Леонеу 1990. године, али је тек због смртних исхода неколико својих припадника 1993. године доспела у жижу јавности, започиње интензивна, нова страница једне моћне активности држава под параваном приватних компанија (Врачевић и Цветковић, 2019). За потребе Националне нафтне компаније Анголе – Сонангол (*Sonangol*), припадници приватне војне компаније *Executive Outcomes* су ослободили нафтна постројења у лучком граду Соjо (*Soyo*), која су била под контролом побуњеника Националне уније за потпуно ослобођење Анголе[97], а затим извршили ангажовање ове компаније ради реструктурирања и војне обуке (примењујући тактику енг. *Special Air Service,* специјалних јединица Велике Британије) њене елитне 16. бригаде, као саветници за војна питања и активни учесници у борбеним операцијама (Врачевић и Цветковић, 2019). На међународној сцени, у задњој декади двадесетог века су биле активне следеће приватне војне компаније: Ер Скан (*AirScan*), Браун и Рот (*Brown & Root*), која представља претходника компаније КБР (*Kellogg Brown & Root Services, Inc – KBR*), ДинКорп Међународна (*DynCorp International*), Група 4 Фалк (*Group 4 Falck*), данас део Г4С (*G4S*), Војни професионални ресурси (*Military Professional Resources, Inc*), Винел корпорација (*Vinnell Corporation*) и *RONCO* компанија (Врачевић и Цветковић, 2019). Када се говори о пословима које су до сада обављале приватне војне компаније, углавном се радило о следећим активностима: борбене операције, обука, подршка, безбедност, обавештајне – контраобавештајне и реконструкције. У наредном делу

планирање комуникација, обуку на симулаторима за управљање возилима и бродовима као и логистичку подршку (Врачевић и Цветковић, 2019).

[94] Компанија енг. *Sandline Internacional* је унајмљена да изведе насилни превратсвргавањем председника Екваторијалне Гвинеје *Teodoro Obiang Nguema Mbasogo*. Помиње се износ од пет милиона долара да је плаћено за ову услугу. Либанац Калил (*Elly Calil*), који је желео да своју трговину нафтом прошири на тржиште Екваторијалне Гвинеје је све ово испланирао са циљем довођења опозиционара Мотоа (*Severo Moto*) политичара на власт. Планирана активност је пропала, јер је 15 плаћеника са наоружањем и опремом ухапшено на аеродрому у Хараре од стране војске Зимбабвеа (Мијалковић, 2010).

[95] Атентат на боливијског председника Моралеса (*Eva Moralesa)* су требали реализовати плаћеници који су наводно учествовали и у борбеним дејствима у Републици Хрватској у редовима Збора народне гарде (Мијалковић, 2010).

[96] *Executive Outcomes*, енг. је основана 1989. године од стране извесног Ебена Барлоа (*Eeben Barlow*) и наводно престала са функционисањем на међународној сцени дана 31. децембра 1998. године. Компанија је била углавном састављена од људи који су били пореклом из Анголе и Намибије (Врачевић и Цветковић, 2019). Док је приватна војна компанија *Executive Outcomes*, енг. била активна, појављује се термин *приватне војне компаније*. Припадници ове компаније више су ангажовани као војници за борбене услуге него као инструктори за војну обуку (Врачевић и Цветковић, 2019). Поред директног ангажовања у борбеним операцијама, ова приватна војна компанија је пружала и следеће услуге: Барлоу у својој аутобиографији наводи да су те додатне услуге подразумевале војну обуку и саветодавне послове у области обавештајних активности, борбе против трговине дрогом, конвенционалне послове обезбеђења и менаџмент у области управљања ризиком (Врачевић и Цветковић, 2019).

[97] Побуњеници Националне уније за потпуно ослобођење Анголе (португалски језик: *União Naçional para a Independência Total de Angola*).

истраживања наводимо према неколико теоретичара одређене врсте приватних војних компанија. Наиме, Дејвид Ширер (*David Shearer*) је извршио класификацију приватних војних компанија према услузи коју пружају на војну борбену подршку[98], војне савете[99], логистичку подршку[100], безбедносне услуге[101] и превенцију криминалитета[102]. Питер В. Сингер (*Peter W. Singer*) је одредио три врсте приватних војних компанија (компаније које пружају војне услуге[103], војно – консултантске компаније[104] и компаније које обезбеђују подршку војним операцијама[105]). Дебора Д. Авант (*Deborah D. Avant*) не врши поделу приватних војних компанија на основу њихових услуга већ на основу врсте и типа уговора које ове компаније склапају са послодавцима: уговори базирани на спољашњој – војној подршци[106] и унутрашњој – полицијској подршци[107] (Врачевић и Цветковић, 2019). Све је више присутно да приватне војне компаније нису самосталне, већ да су у саставу неких других компанија или су придружене неким другим компанијама: *Универзал Гардијан* (енг. *Universal Guardian Inc*) је приватна војна компанија која, између осталог, поседује и *Сикјур Рискс* (енг. *Secure Risks Ltd.*), компанију из Велике Британије, па је сада ова компанија постала власник још једне британске компаније, компаније Међународна стратешка безбедносна решења (енг. *Strategic Security Solutions International Ltd.*) од 2004. године, која је 2006. године добила уговор који је, поред осталих обавеза, обухватао и обезбеђење особља амбасаде САД у главном граду Авганистана, Кабулу; приватна војна компанија енг. *DynCorp International* са компанијом енг. *McNeil Technologies*, формирала је компанију енг. *Global Linguist Solutions*, намењену за подршку Обавештајно – безбедносне команде оружаних снага САД (енг. *U.S. Army Intelligence and Security Command*) електронским уређајима за превођење; компанија Калифорнијски центар за анализу (енг. *California Analysis Center Incorporated*), наводно повезана са структурама Централне обавештајне агенције, обезбеђивањем преводилаца и иследника за потребе америчких оружаних снага у Ираку, док се у ствари ради о компанији која се бави пружањем услуга из области информационих технологија (Врачевић и Цветковић, 2019); па корпорација Локхид Мартин (енг. *Lockheed Martin Corporation*), авио, електронски и информационо – технолошки индустријски гигант; корпорација Нортроп Груман (енг. *Northrop Grumman Corporation*), још један војно – индустријски гигант, власник је корпорације Винели (енг. *Vinnell Corporation*), која покрива различите сегменте услуга приватних војних компанија. Вероватно се у саставу дела

---

[98] Приватна војна компанија *Sandline International,*енг. данас угашена компанија под овим називом.
[99] *Science Applications International Corporation*, енг. приватна војна компанија.
[100] *Pacific Architects and Engineers*, енг. приватна војна компанија.
[101] *Control Risks Group*, енг. приватна војна компанија.
[102] *Kroll,* приватна војна компанија.
[103] *Executive Outcomes*, енг. пример приватна војна компанија.
[104] Пример приватна војна компанија, Војни професионални ресурси – енг. *Millitary Professional Resources Inc.*
[105] Пример приватна војна компанија, енг. *Kellogg Brown & Root Services Inc.*
[106] Обухвата оружану оперативну подршку – енг. *Executive Outcomes* у Анголи, неоружану оперативну подршку – енг. *Science Applications International Corporation* у првом Заливском рату, неоружане војно саветодавне послове и обуку – Војни професионални ресурси у Републици Хрватској и логистичку подршку – енг. *Brown & Root* у Авганистану (Врачевић и Цветковић, 2019).
[107] Обухвата обезбеђење локација са оружјем – енг. *Blackwater* у Ираку, обезбеђење локација без оружја – енг. *Defence Systems Limited* у Демократској Републици Конго, полицијско – саветодавне послове и обуку – енг. *DynCorp* у Ираку, превенција криминалитета – енг. *Defence Systems Limited* у Демократској Републици Конго и обавештајно – безбедносне послове – енг. *California Analysis Center Incorporated* у Ираку (Врачевић и Цветковић, 2019).

највећих војно – индустријских компанија на планети налазе *уграђене*, одређене приватне војне компаније (Врачевић и Цветковић, 2019).

У наредних неколико примера су наведена места ангажовања приватних војних компанија из РФ у паравојним активностима у постхладноратовском периоду и њихова обележја. Приватне војне компаније су са својим паравојним ангажовањем одиграле кључну улогу приликом уласка у Украјину 2014. године. Та кључна улога је обухватала активности како у директној борби, тако и у сегменту обуке и надзору различитих побуњеничких снага. Већи део особља приватних војних компанија је био високо оспособљен за реализацију војних задатака. Службе безбедности САД износе сазнања да је највероватније војна служба безбедности РФ – Главна управа (раније позната као Главна обавештајна управа) контролисала активности приватних војних компанија и да су припадници ових компанија убили вође побуњеника које је РФ сматрала проблематичним у Украјини. Службе безбедности САД износе податке да је *Вагнер група* (*Wagner*) први пут регистрована управо на територији Украјине (Bowen, 2020). Током сукоба РФ и Украјине 2014. године, војна служба безбедности Главна управа се у великој мери ослањала на своје искуство у управљању приватним војним компанијама где је током сукоба медијски извештај документовао присуство батаљона *Восток*. Тада је наводно идентификован официр војне службе безбедности РФ, Главне управе, Олег Иванников као одговорно лице за транспорт противваздушног система са којим је наводно оборен лет број 17 Малезијског авиопревозника (енг. *Malaisian Airlines*) 2014. године (наведени податак треба узети са резервом). Украјина је такође коришћена као полигон за тестирање других приватних војних компанија, укључујући *групу Вагнер* која је наводно била блиско повезана са војном службом безбедности РФ, Главном управом (Bowen, 2021). Други пример државе у којој је регистровано ангажовање приватних војних компанија је Сирија. У овој држави је било доста активно учешће приватних компанија. То учешће се огледало у заштити нафтних поља у Сирији, директној оружаној борби, другим ангажманима и са америчким снагама. Уочено је да су неке активности чисто комерцијалне природе (заштита нафтних поља), где је приметно и да је људство на таквим задацима слабо оспособљено за било какве озбиљније акције, док се чини да друге активности особља из оваквих компанија, као на пример борбу и обуку локалних савезничких снага, води изузетно обучен кадар, квалификовано особље и у директној координацији са оружаним снагама РФ (Bowen, 2020). *Spetznaz* је такође одиграо битну улогу у сукобу у Сирији, када су вршиле извиђање бојног поља и деловале као инструктори, саветници за оружане снаге Сирије и разне провладине снаге милиције, као што је *5. јуришни корпус* (Bowen, 2021). Следећа држава која представља пример где су се ангажовале приватне војне компаније РФ је Либија. У овој држави је *Вагнер група* имала највише активности и то у подршци лидеру Либијске националне армије Халифи Хафтару од 2018. године. Када кажемо подршка, тада говоримо о директном учешћу у борби, обуци и саветовању. Такође су били ангажовани приликом распоређивања система противваздухопловне одбране и авиона као и надгледања ангажовања. Централноафричка Република је следећа дестинација где се препознају трагови ангажовања приватних војних компанија РФ у периоду од 2018. године. Након добијања изузећа од Савета безбедности Уједињених нација од ембарга за извоз оружја, РФ је продала Централноафричкој Републици оружје, а након тога су регистроване и приватне војне компаније из РФ које су наводно пружале безбедносне услуге, војну обуку и личну заштиту највиших званичника

Централноафричке Републике (укључујући и председника). Фирме повезане са приватним војним компанијама из РФ су закључиле уговоре за експлоатацију рудног богатства из Централноафричке Републике и успоставиле присуство у рудницима дијаманата које држе побуњеници. Судан је следећа држава где су регистроване приватне војне компаније РФ од 2018. године. *Вагнер група* и лица и ентитети са њом у вези су од стране служби безбедности САД документовани да врше обуку локалног безбедносног особља у Судану (укључујући и трупе из Централноафричке Републике) и да обезбеђују, врше заштиту инвестиција у сектору злата. Ангажовање приватних војних компанија из РФ је регистровано и у Мозамбику. Ради се о периоду 2019. године; особље *Вагнер групе* је наводно распоређено на крајњи север Мозамбика да обучава и подржава владине снаге против локалне исламистичке побуне повезане са Исламском државом (Bowen, 2020).

Атентат као и други елементи *активних мера*, дуго коришћено оруђе совјетске и руске државе. Организовани терор и лов на *непријатеље народа* били су карактеристике совјетске службе безбедности од самог почетка Савеза Совјетских Социјалистичких Република. Први директор *Чеке*, Феликс Џержински је то јасно рекао: „Ми се залажемо за организовани терор – то треба искрено признати. Терор је апсолутна неопходност у доба револуције. Наш циљ је да се боримо против непријатеља совјетске владе и новог поретка живота. Судимо брзо. У већини случајева између хапшења злочинца и његове пресуде прође само један дан. Када се суоче са доказима, злочинци у скоро сваком случају признају, а који аргумент може имати већу тежину од признања самог злочинца" (Sipher, 2018, p. 7). Оружје које су користили припадници Комитета државне безбедности се кретало од посуда са пастом за зубе напуњених отровним гасом и прахом за спавање који је убијао унутрашње непријатеље, до употребе радиоактивног полонијума и нервног агенса *новичок* коришћеног наводно против Сергеја Скрипала (Sipher, 2018). Покушаји атентата и атентати нису страни ни у историји српског народа као и Социјалистичке Федеративне Републике Југославије, организовани или потпомогнути од страних служби безбедности. Наиме, поменућемо пар догађаја, почев од *Сарајевског атентата*, убиства аустроугарског престолонаследника Франца Фернинанда, затим три покушаја убиства и на крају и успешног атентата на краља Александра I Карађорђевића у Марсељу, великог броја покушаја убистава Јосипа Броза Тита у периоду док је био председник Социјалистичке Федеративне Републике Југославије, па до убиства председника Владе Републике Србије Зорана Ђинђића, што чини изузетно актуелним наведену проблематику како због обавештајних, тако и контраобавештајних активности, безбедносне заштите *одређених лица* и посебно необавештајних активности служби безбедности. Поруке које се шаљу на овај и сличан начин могу да доведу до тектонских поремећаја у односима циљних држава.

5.5.2. Обележја паравојних активности

Паравојна активност је активност припадника паравојне организације који конкретно није део редовних оружаних снага било које земље, већ личи на њих по организацији, опреми, обуци или мисији (Training and Doctrine Command G2 Handbook No. 1.08, 2010). Ненаоружано невојно особље (нерегуларне снаге) у спровођењу активности може обухватити следеће категорије: „медије, невладине организације, транснационалне корпорације, друге групе цивила – владине службенике, пословне људе, локално становништво, пролазнике, интерно расељене цивиле или избеглице, државне службенике,

као што су полиција, градоначелници, чланови градског већа и особље хитне службе, пословни људи, пољопривредници, адвокати, лекари, свештенство, трговци и др." (Training and Doctrine Command G2 Handbook No. 1.08, 2010, p. 145).

Како би било јасније за разумевање, треба поменути неопходност разликовања паравојне операције која представља активност где су тежишно носиоци таквих операција службе безбедности (*тајне акције*, првенствено Централна обавештајна агенција у САД) од *специјалних операција* или *тајних операција* које предузимају регуларне оружане снаге САД (униформисани припадници оружаних снага САД, Пентагон), мада врло често ту долази до одређених „преклапања" (ради већ инфилтрираних припадника служби безбедности у одређене герилске или друге групе, организације, који морају реализовати са тим лицима задатке, непријатељства). *Тајна акција* је део онога што се шире назива *специјалне активности*, које су у Извршној наредби 12333 дефинисане као „активности које се спроводе у подршци националним спољнополитичким циљевима у иностранству које се планирају и извршавају тако да улога САД није очигледна или јавно призната" (Krishnan, 2018, p. 2). Није вишак поменути да *све тече и све се мења*, тако да и ово појмовно одређење није непроменљиво (поготово у светлу брзих промена данашњице на планети), првенствено мислећи на сегмент „јавног признања" које није стално присутно, односно већ је било случајева да након успешно реализованих тајних акција буде призната таква активност. Ангажовање државног апарата (првенствено служби безбедности) укључује активности попут: „обуке припадника страних оружаних снага, служби безбедности других земаља; обезбеђивање материјала или посебна подршка страним владама од служби безбедности; практично учествовање на терену као подршка оперативној борби против наркотика и ангажовање као противтерористичке снаге; ексфилтрација било којом сфером осетљивог дефекта; или чинећи инертним складиште терористичких експлозива; финансирање; обезбеђивање оружја; другу војну опрему укључујући и моторна возила; кадровска планирања и сл; и др. активности неопходне за помоћ или вршење одређене присиле над неком државом, лицем, ентитетом" (Krishnan, 2018, p. 2). Велики је број подела на врсте активности које обухвата тајна акција, али најчешћа и најприхватљивија код великог броја аутора са запада обухвата следеће активности: пропагандне активности, политичке активности, економске активности и *паравојне активности* (док други аутори посебно издвајају атентате, државне ударе, сајбер ратовање и др. што се све може класификовати под неким од наведене четри врсте). Тајна акција за коју је носилац углавном Централна обавештајна агенција је регулисана према наслову 50 Кодекса САД, а *специјалне* или *тајне операције* америчке војске регулисане су насловом 10 Кодекса САД (*прикривено* се овде односи на тајност спонзора, док се *тајно* односи на тајност саме операције и поред тога важно је нагласити да се тиме одређује и ко ће руководити – командовати операцијом, која су овлашћења, ко врши надзор, начин финансирања и др.). Тешко могу да се уоче разлике између специјалних операција и тајних акција, поготово у време борбе против тероризма, али и историјат говори да је америчка Централна обавештајна агенција (док је још била Канцеларија за стратешке услуге – енг. *Office of Strategic Services*) била војна организација некада док је била у саставу војне команде. Међутим, без обзира што су се специјалне операције и тајне акције, после Другог светског рата формално одвојиле у пракси, оружане снаге САД су често обезбеђивали лица, опрему за паравојне операције које води Централна обавештајна агенција.

Неконвенционалне фазе (*Табела 13*) ратовања према нормативима оружаних снага САД обухватају седам фаза и то: „*Фаза I: Припрема* – обавештајна припрема бојног поља, планирање, предвиђање вероватних непријатељских праваца деловања; *Фаза II: Први контакт* – први контакт са групом отпора ради процене изгледа неконвенционалног ратовања заједно са партнерским нацијама; *Фаза III: Инфилтрација* – војници специјалних снага инфилтрирају се у оперативну зону неконвенционалног ратовања и повезују се са нерегуларним снагама; *Фаза IV: Организација* – специјалне снаге реорганизују елементе отпора или побуњеника у герилце, подземље и помоћне, спроводећи неконвенционалне операције; *Фаза V: Нагомилавање* – ширење герилских операција кроз набавку опреме и залиха; *Фаза VI: Запошљавање* – аутохтоне и друге нерегуларне снаге све више делују у борбеном окружењу неконвенционалних операција које могу бити повезане са конвенционалним операцијама; *Фаза VII: Транзиција* – прелазак из борбе у мир и повратак нерегуларних снага под цивилну контролу" (Krishnan, 2018, p. 19).

Табела 13. Неконвенционално ратовање и одговор друге државе.

Неконвенционално ратовање	Страна унутрашња одбрана
Присилити, пореметити или збацити владу или окупаторску власт: • Опција политике. • Путем или са домаћом силом. • Субверзија/саботажа.	Побољшати безбедносни апарат националне државе: • Обучити, саветовати и помагати. • Пре свега усмерен на борбу против побуњеника.
Деградирати легитимитет и дестабилизовати	Ојачати легитимитет и стабилизовати
Белешка: Омогућено од стране војних снага за специјалне операције, конвенционалне снаге и заједничке, међуагенцијске, међувладине и мултинационалне способности.	Белешка: Сарадња са специјалним снагама за операције војске, конвенционалне снаге и придружене, међуагенцијске, међувладине и мултинационалне способности.

Извор: Krishnan, 2018, p. 18 (In: US Department of Defense 2014. FM 3–18: Special Forces Operations. Department of the Army (May), p. 3–8).

Извршење циљаних напада у иностранству или атентата се доводи врло често у везу са војном службом безбедности Главна управа (или некада познатија Главна обавештајна управа). Део ових напада је откривен због неопрезног или слабог рада агената, што је довело до оптужби за некомпетентност од стране војне службе безбедности РФ, Главне управе (односно некада Главна обавештајна управа), међутим, део аналитичара тврди да је намера иза неких циљаних напада слање поруке лицу, држави, служби безбедности, а не сакривање саучесника (Bowen, 2021). Када говоримо о окрутности активности ових служби безбедности, тада најбоље да прокоментаришемо једно од најозлоглашенијих и најистакнутијих убистава које је реализовала наводно Главна обавештајна управа, 2004. године са судским епилогом. Наиме, аутомобилом бомбом убијени су у Катару (у егзилу су тамо и живели) бивши чеченски сепаратистички председник Зелимкхан Јандарбијев и његов син који је имао 13 година. Поступак који је вођен пред надлежним судом у Катару осудио је два агента војне службе безбедности РФ, Главне обавештајне управе за убиство, док трећег учесника није због његовог статуса – радило се о првом секретару амбасаде РФ, који је имао дипломатски имунитет. Радило се наводно о агентима Главне обавештајне управе који су депортовани у РФ на издржавање казне, али су по повратку у РФ наводно нестали (Bowen, 2021).

У реализацији паравојних активности, службе безбедности РФ обично су у претходном периоду ангажовале војну службу безбедности Главну обавештајну управу (сада Главну управу), односно особље из јединице *Спетсназ* (*Spetsnaz*) за тајне операције, акције (необавештајне активности) чији распоред је тајне природе. Поред активних припадника, ангажују се и бивши припадници Главне обавештајне управе, Спетсназа, који се ангажују као приватне снаге. Дуга је историја реализације руских политичких циљева од стране ове јединице, *Спетсназ*. Владимир Резун (вођен под псеудонимом Виктор Суворов), официр Главне обавештајне управе, пребег (у Велику Британију), био је официр Спетсназа пре него што је постао службеник Главне обавештајне управе. Резун је о својој обуци за вођење диверзантских операција у позадини и тајних инфилтрација доста тога открио. У великом броју случајева ривалитет између служби безбедности или целина које обављају сличне или исте безбедносно – обавештајне активности је присутан у једној држави. Тако се током Хладног рата, Спетсназ такмичио са Комитетом државне безбедности, према речима Резуна, у узимању примата у планирању, спровођењу тајних инфраструктурних напада и других активности. У истом периоду као и у постхладноратовском периоду, припадници Спетсназа су били тајно ангажовани у Анголи, Либану, Вијетнаму, Камбоџи, Авганистану, мада и дејство током чеченских ратова и у рату између РФ и Грузије 2008. године није заобишло војну службу безбедности РФ, Главну обавештајну управу и *Спетсназ* (Riehle, 2022).

На основу података сакупљених из више јавних извора констатовано је да је Јединица 29155 елитна јединица Главне обавештајне управе која води осетљиве стране операције, укључујући атентате и циљане нападе. Према овом извештају, Јединица 29155 је наводно повезана са елитном руском јединицом команде специјалних операција, са седиштем у Сенежу, изван Москве. Командант Јединице 29155 је генерал – мајор Андреј Аверјанов. Анатолиј Чепига, лице осумњичено да је нападач у случају тровања Сергеја Скрипала и његове ћерке у Великој Британији 2018. године, фотографисан је на венчању Аверјановове ћерке 2017. године као и других оперативаца Јединице. Припадници јединице највероватније имају искуство у бригадама специјалних јединица пре доласка у Главну управу (раније Главну обавештајну управу), где је и сам командант јединице Аверјанов био припадник. Следеће су активности које су довођене директно у везу са Јединицом 29155. Ангажовање РФ у региону Крима 2014. године, затим тровања бугарског трговца оружјем Емилијана Гебрева 2015. године, па наводни покушај државног удара 2016. године у Републици Црној Гори да би се свргнуо и заменио прозападни премијер, као и потенцијално спречавање придруживања земље Североатлантском савезу и тровање руског агента који је пребегао у Велику Британију, Сергеја Скрипала 2018. године. Поред наведених активности, директно довођених у везу са Јединицом 29155, медији су доводили у везу и следеће активности које ћемо навести хронолошким редом. Оперативци Јединице 29155 су праћени до Швајцарске отприлике у време када су друге јединице војне службе безбедности Главне управе хаковале Светску антидопинг агенцију и планирале хаковање Организације за забрану хемијског оружја у Хагу, која је истраживала допинг који је спонзорисала држава, РФ, у спорту и употребе хемијског оружја. Шпанија је такође отворила истрагу о путовању познатог оперативца Јединице 29155 Дениса Сергејева у Барселону 2017. године, у периоду када су каталонски сепаратисти организовали незаконит референдум о независности. У Француској је 2019. године, према писању француског листа *Ле Монде*, коме су извор података биле европске службе безбедности, које су наводно пратиле оперативце војне службе безбедности

Главне управе из Јединице 29155 се чинило да припадници Јединице 29155 користе француски регион Горње Савоје у Алпима као базу за вођење операција. У Авганистану, у јуну 2020. године према извештају медија, добијених од служби безбедности САД, агенти војне службе безбедности Главне управе (или некада познатије Главне обавештајне управе) су понудили плаћање милитантима повезаним с талибанима да изврше нападе на америчке и друге међународне снаге у овој земљи. Наводно, извори служби безбедности САД верују да је Јединица 29155 одговорна за омогућавање ових исплата. У Чешкој су у априлу 2021. године чешке власти окривиле Јединицу 29155 за серију раније необјашњивих експлозија у складиштима оружја 2014. године, у којима су погинуле две особе. Као одговор, чешке власти су протерале 18 руских дипломата, а на то је РФ одговорила протеривањем 20 чешких дипломата. На крају, чешке власти су протерале преко 70 дипломата како би се традиционално велико дипломатско представништво РФ у Прагу ускладило са чешком мисијом у Москви. У том периоду је у медијима писано да је оружје припадало бугарском трговцу оружјем Емилијану Гебреву, који је преживео наводне покушаје тровања од стране Јединице 29155 у 2015. години, а да је интерес РФ у читавом догађају био спречавање отпремања оружја и муниције у Украјину. Убрзо након открића, бугарски тужиоци најавили су истраге о серији необјашњивих, *случајних* експлозија у неколико складишта муниције у Бугарској (Bowen, 2021). Можемо констатовати да су ретке случајности у догађајима након оваквих и сличних активности служби безбедности већ да се ради о одговору једне службе безбедности или о довршавању започетог *распламсавања* од стране службе безбедности са супротне стране.

Руска Федерација користи поред владиних снага и невладине снаге којима управљају корпорације из РФ за спровођење тајних активности, операција, паравојног карактера што омогућава РФ да изврши продор у страно, непријатељско окружење. У таквом окружењу може много лакше да искористи, спроведе како економске тако и политичке активности. Када смо поменули 2014. годину, од те године припадници приватних војних компанија делују у Украјини, Сирији, Централноафричкој Републици, Судану, Мозамбику и Либији. Порицање о учествовању у активностима које стварају ове и сличне невладине снаге омогућило је РФ да пружа подршку својој страни у сукобу, док јавно тврди да је поштен посредник. Одрицање од одговорности за жртве и насиље је омогућило РФ овакав вид активности. У 2017. години, Исламска држава је ухватила два припадника групе Вагнер у источној Сирији и снимала их и пуштала снимке у медије. РФ је одбацила њихову припадност државном апарату, тврдећи да се вероватно ради о добровољцима. Са тајним војним снагама испуњавају се спољнополитички захтеви РФ. Наводно је забележено и неколико неуспелих, односно операција са више потешкоћа у спровођењу: 2018. године, снаге *Вагнер групе* су наводно десетковане од стране снага САД у једном нападу у Сирији; у Мозамбику, снаге *Вагнер групе* су брзо биле савладане и приморане да се повуку у базу; у Централноафричкој Републици наводно се суочавају са сличним потешкоћама у раду са локалним становништвом (Riehle, 2022).

Важно је нагласити да поред војне службе безбедности Главне управе (некада Главне обавештајне управе) и Јединице 29155 и друге службе безбедности у РФ наводно руководе одређеним тајним тимовима за осетљиве операције у иностранству. Федерална служба безбедности контролише руске елитне антитерористичке тимове *Алфу* и *Вимпел* (налазе се у оквиру Федералне службе безбедности, центра посебне намене). *Алфа* је примарна руска

антитерористичка снага док је *Вимпел* одговоран за операције у иностранству (саботаже, наводне атентате и тајно праћење). Служба безбедности РФ, Спољна обавештајна служба, наводно има елитну оперативну јединицу познату као *Заслон*. Мало јавних информација постоји о јединици, иако је њено присуство наводно документовано у Сирији (Bowen, 2021).

Алгоритми вештачке интелигенције о акумулираној мудрости или знању о некој појави могу да произведу резултате и у војном контексту могу пружити предност у борби, посебно ако ти резултати изненаде непријатеља. Међутим, друга мишљења наводе да је овакво понашање сувише круто, неприлагодљиво. Примена вештачке интелигенције у војном контексту може имати негативан ефекат уколико предрасуде остану неоткривене и уграђене у системе са смртоносним ефектима (Hoadley & Sayler, 2020). Ово је неопходно имати на уму када би се размишљало о примени овог вида активности у евентуалним паравојним активностима.

5.5.3. Анализа утицаја паравојних активности

Ендру Мамфорд (*Andrew Mumford*) наводи следеће предности паравојних операција: држава може имати сопствени економски или политички интерес; подршка да би одређене паравојне групе могле бити идеолошки мотивисане; понекад се сматра да је велики рат постао застарео начин решавања политичких проблема; и прокси ратовање је привлачно као стратегија управљања ризиком, јер смањује све обавезе према сукобу. Герејнт Хјуз (*Geraint Hughes*) износи следеће предности паравојних операција: „политичка ограничења о директној активности; безбедност; осетљивост на жртве; идеолошка солидарност; избегавање сукоба; помагање у војној кампањи; прикупљање обавештајних података; националистичке/верске везе; освета; очување или јачање сфера утицаја; похлепа" (Krishnan, 2018, p. 10).

Поред класичних војних и/или паравојних активности, једна врста активности служби безбедности обухвата још једну категорију ове активности; ради се о атентатима. Једну од битнијих категорија необавештајних активности, тајних операција служби безбедности РФ представљају атентати. С обзиром на доминацију присутности западних медија и примат који имају, истицање сваке, чак и непроверене назнаке да постоји умешаност РФ у покушај или реализовани атентат, већ поприма озбиљне конотације код публике. Врло често, атентати су главна тема политичких и новинарских дискусија на Западу. Покушај убиства истакнутог опозиционара и антикорупцијског активисте у РФ, Алексеја Навањног у августу 2020. године, као и реализација убистава уназад неколико година, више бивших оперативаца (наведено у истраживању), припадника служби безбедности РФ који су пребегли у државе Запада, што им је била казна од стране Владе РФ зато што су радили за другу, страну службу безбедности, представљају најбољи доказ о повратку старе, добро познате методе рада у необавештајним активностима служби безбедности РФ. Када се направи компарација атентата које спроводи Запад, они су углавном обједињени, „нема посебних класификација, а у РФ када се у теорији наводе атентати, тада се у класификацији (види *Табелу 14*) врши селекција на атентате који се изводе према три групе циљева и то, *политичке*, *војне* и *издајничке*. Поред ове три групе циљева заступљена је и класификација наведених врста атентата према месту реализације атентата и то када се исти реализује у РФ, тада се назива унутрашњи, а атентат који се реализује у иностранству се зове спољни атентат" (Riehle, 2022, p. 216, 217).

Табела 14. Врсте атентата у необавештајним активностима служби безбедности РФ.

Врста атентата	Унутрашњи	Спољни
Политички	Опозиционари, критички настројени, новинари	Мали број антипутиновских политичких активиста
Војни	За време противтерористичких операција	Сиријски опозициони, украјински и чеченски војни лидери
Издајнички	Решене кроз механизме државне безбедности	Мали број посебних случајева

Извор: Riehle, 2022, p. 217.

Процена РФ (као и било које друге државе када делује на својој територији) за реализацију атентата у РФ много је другачија од реализације у иностранству. Осетљивост активности служби безбедности овог карактера изван државе је много већа него што је унутар исте. Убиством Зелимкана Хангошвилија, чеченског милитантног вође, у Немачкој у августу 2019. године, покренути су државни инструменти Немачке где је спроведена правна истрага и мера Владе Немачке што је резултирало протеривањем дипломата РФ (Riehle, 2022).

Када је реч о спољним војним атентатима, тада се углавном мисли на представнике, вође милитаната. Током хладноратовског периода, мете су укључивале украјинске националистичке вође Георгија Околовича, Лева Ребета и Степана Бандера. Сви су били настањени у Немачкој када су били означени за атентат. Ове наведене жртве, с обзиром да су водиле антисовјетске милитантне покрете ван Савеза Совјетских Социјалистичких Република, из наведеног разлога су биле војне мете (Riehle, 2022). У постхладноратовском добу атентати су вршени на најистакнутије чеченске милитантне вође, који су према процени РФ сви били терористи (*Табела 15*). У периоду од 2004. до 2019. године, најмање 20 чеченских сепаратистичких лидера и њихових присталица били су означени као мете операција које је требало да спроведе РФ у иностранству и то 12 у Турској, три у Украјини, два у Аустрији и по једног у Катару, Уједињеним Арапским Емиратима и Немачкој. Наведено је 20 покушаја и реализације атентата, од којих су три пропала и део се није завршио убиством.

Табела 15. Атентати које су планирале и /или реализовале, највероватније службе безбедности РФ, спроведени према чеченским побуњеницима.

Време	Опис необавештајне активности
2004.	Зелимкхан Иандарбиев, вођа чеченских побуњеника, убијен у Катару; Официри Главне обавештајне управе ухапшени у Дохи у Катару
2008.	Гаји Едилсултанов, чеченски војсковођа, убијен у Истанбулу, Турска
2008.	Ислам Јанибеков, чеченски војсковођа, убијен у Истанбулу, Турска
2009.	Умар Исраилов, бивши телохранитељ чеченског лидера Рамзана Кадирова који је оптужио Кадирова да је наредио мучење, убијен у Бечу, Аустрија
2009.	Муса Атајев (ака Али Осајев), чеченски војсковођа, убијен у Истанбулу, Турска
2009.	Салим Јамадајев, чеченски политички лидер и ривал Кадирову, убијен у Дубаију, Уједињеним Арапским Емиратима
2011.	Берг–Хазг Мусајев, Рустам Алтемиров и Заурбек Амриев, чеченски војници убијени у Истанбулу, Турска, а један од атентатора је идентификован као руски криминалац са оружјем типа, врсте коју користе руске специјалне снаге
2011.	Шамсудин Батукајев, чеченски побуњенички свештеник, покушај атентата у Турској
2013.	Медет Унлу, представник чеченских побуњеника у Турској, покушан атентат у Анкари, Турска
2014.	Абдулах Бухари, узбекистански свештеник, убијен у Турској, а везе Федералне Службе Безбедности са атентаторима, као услуга за потребе службе безбедности Узбекистана

Време	Опис необавештајне активности
2015.	Каим Садујев, чеченски војни командант, убијен у Истанбулу, Турска
2015.	Абдулвахид Еделгириев, чеченски опозиционар који је планирао да настави џихад на територији РФ, сматра се у Москви да је играо кључну улогу у завери за убиство Путина, убијен је у Истанбулу у Турској
2016.	Руслан Исрапилов, чеченски опозиционар, убијен у Провинцији Коцаели, Турска
2017.	Адам Осмајев и Амина Окујева, муж и жена чеченски активисти, нападнути у Кијеву, у Украјини, али је узвратио ватру на нападаче и преживео, Москва је оптужила Осмајева за заверу да убије Путина, док је Окујева убијена у заседи касније 2017. године
2017.	Тимур Махаури (ака Али Тимајев), чеченски војсковођа, убијен у Кијеву у Украјини
2019.	Зелимкхан Кхангосхвили, чеченски војсковођа који је пребегао и подржавао грузијске обавештајне службе, убијен у Берлину у Немачкој
2020.	Мамикхан Умаров, чеченски политички активиста и блогер, убијен у Аустрији

Извор: Riehle, 2022, p. 224, 225.

Део сиријских милитаната, односно њихови лидери, били су мете војних операција РФ, унутар Сирије. Када говоримо о Украјини, најмање четири украјинска војна лидера су убијена у Украјини, уз највероватнију подршку Федералне службе безбедности или војне службе безбедности Главне управе. Руска Федерација на ове и сличне мете гледа као на легитимне војне циљеве, а не на политичке мете. У 2021. години је регистрована друга могућа врста војног атентата служби безбедности РФ, а то је када су 2021. године објављени резултати истраге о експлозијама које су се догодиле у два војна складишта оружја 2014. године у Чешкој, и о бугарском трговцу оружјем на којег је извршен покушај атентата само 6 месеци након те експлозије. Наводно је то оружје требало да се дистрибуира у Украјину (званичници Украјине су у априлу 2021. године известили да је Гебрев умешан у набавку оружја уништеног у Чешкој), можда и у Грузију, противнике РФ, што је Гебрев демантовао. Као извршиоце, *Bellingcat* је означио официре војне службе безбедности РФ, Главне управе (Riehle, 2022).

Категорија издајника је у свим бившим социјалистичким режимима била присутна као једна од крилатица коришћених за елиминацију непријатеља, како спољашњег тако и унутрашњег. У РФ се за спољашње издајнике подразумева да нема праштања пребегу, односно бившим или садашњим припадницима служби безбедности, издајницима који су пребегли у иностранство. За њих нема праштања, односно како Руси кажу нема повратка без последица. Служба безбедности, Комитет државне безбедности, а и њени наследници касније, имају мисију да пронађу и неутралишу[108] пребегле припаднике служби безбедности. Када говоримо о постхладноратовском периоду, операције атентата на пребеге припадника служби безбедности догодиле су се бар два пута, и то 2006. године када је мета био Александар Литвињенко, бивши припадник Федералне службе безбедности и 2018. године када је мета био Сергеј Скрипал, бивши припадник војне службе безбедности РФ Главне обавештајне управе (сада Главне управе). Званични државни органи Уједињеног Краљевства су идентификовали припаднике службе безбедности Федералне службе безбедности који су били умешани у операцију Литвињенко, а Влада Уједињеног Краљевства и *Bellingcat* су установили да су припадници војне службе безбедности РФ, Главне управе били укључени у операцију везану за Скрипала. Као што су некада слате поруке пребегу преко породице,

[108] Неутралисати у терминологији служби безбедности је представљало појам који је обухватао поновно регрутовање издајице, да подржи државне интересе, затим киднаповање или намамљивање назад у државу да би се суочио са правдом или у најекстремнијим случајевима, њихова ликвидација.

фамилије, познаника путем поште, писма или усмено, данас се преко новина, комуникацијских мрежа и слично, врло брзо пошаљу поруке пребегу. Последњи карактеристичан пример је када су новинари у РФ (читај службе безбедности РФ, прим. аут.) идентификовали град у који је Олег Смоленков пребегао 2017. године, где је боравио у САД. Само годину дана након покушаја атентата на Скрипала, објављивање Смоленковљеве адресе је била јасна порука сваком пребегу „не можете се сакрити – знамо где сте" (Riehle, 2022, p. 233).

У медијима је објављено да је дана 31. августа 2018. године у кафеу *Сепар* (скраћено од сепаратиста) у Доњецку експлозивном направом убијен лидер самопроглашене Доњецке Народне Републике, Александар Захарченко, када је званична Москва оптужила Службу безбедности Украјине, односно званични Кијев за овај атентат. Наравно, и ова активност служби безбедности (атентат) није била самостално примењивана већ је била пропраћена низом других информационих активности служби безбедности, а једна од њих су и контраоптужбе од стране Службе безбедности Украјине да је овај атентат починила Москва како би се наводно ослободила лица који много знају о почињеним активностима у Украјини.

Александар Литвињенко[109], одбегли агент службе безбедности РФ, убијен је тако што је на њега извршен атентат на најсвирепији начин, да не умре брзо и без болова већ напротив у што већим боловима и мукама (тровањем, радио – активним полонијумом – 210, отровом) и то у сред Велике Британије која је пружила азил овом човеку, што је главна порука сваком следећем који помисли да било шта уради што је супротно званичном једноумљу у хијерархијском поступању. На претресном рочишту у децембру 2012. године, о околностима смрти Литвињенка, бранилац у име Марине Литвињенко, супруге убијеног, изјављује

[109] Александар Литвињенко (*Alexander Litvinenko*) служио је у Федералној служби безбедности више од 20 година где је стекао чин потпуковника, а током 1999. године је ухапшен и затворен због оптужби које су касније одбачене. Након наставка даље оптужбе (једнако одбачене), побегао је из РФ и живео са породицом у Великој Британији где је добио политички азил 2001. године, а отрован је 1. новембра 2006. године у суши ресторану у Лондону, Велика Британија (тек 23. новембра се сазнало да се ради о радио – активном полонијуму 210, што је било пар сати пре него што је преминуо у великим патњама). Литвињенко се састао у хотелу Миленијум (*Millennium Hotel*) са неколико људи који су дошли у Лондон из других земаља: агенти Федералне службе безбедности, Андреј Луговој, Дмитриј Ковтун, Вјачеслав Соколенко (*Andrei Lugovoi, Dmitry Kovtun, Vyacheslav Sokolenko*) са својим бившим колегом, потпуковником Федералне службе безбедности Александром Литвињенком који је том приликом пио зелени чај (Litvinenko & Felshtinsky, 2013). Андреј Луговој је након смрти Литвињенка убрзо постао посланик у парламенту РФ чиме се служба безбедности одужила свом агенту, а јавно је забележен још само један случај да се овако служба одужи свом агенту Рамону Меркадеру (*Ramón Mercader*), убици Троцког (*Trotsky*). Лав Давидович Троцки, право име Лев Давидович Бронштајн (рус. *Лев Давúдович Трóцкий,* енг. *Trotsky*), био је руски револуционар јеврејског порекла и политичар који је имао истакнуту улогу у Октобарској револуцији и Црвеном терору, али је 1927. године разрешен свих дужности док 1929. године је протеран из Савеза Совјетских Социјалистичких Република (Litvinenko & Felshtinsky, 2013). Троцки је добио азил у Мексику 1936. године, где га је највероватније у чисткама као главног завереника против Стаљина, године 1940. године убио шпански комуниста, агент Народног комесеријата унутрашњих послова, Рамон Меркадер (шп. *Ramón Mercader,* енг. *Ramón Mercader*) ангажован од Народног комесеријата унутрашњих послова (претходница службе безбедности, Комитета државне безбедности, Савез Совјетских Социјалистичких Република, регрутован највероватније од официра Народног комесеријата унутрашњих послова, Наум Ејтингтона), тако што га је 20. августа 1940. године тешко ранио цепином – део планинарске опреме (Litvinenko & Felshtinsky, 2013). Испред куће су га чекале колеге из Народног комесеријата унутрашњих послова са аутомобилом, Ејтингтон и још један колега, али пошто није изашао из куће они су отишли. Меркандер је за убиство Троцког одслужио 20 година затворске казне у Мексику, а по изласку је награђен орденом Лењина (Litvinenko & Felshtinsky, 2013).

следеће: „Господин Литвињенко био је низ година редовни и плаћени агент и припадник, службеник службе безбедности, Војног обавештајног одељка 6, чији је руководилац био под псеудонимом Мартин". Даље, бранилац наводи: „да је по налогу службе безбедности, Војног обавештајног одељка 5, Литвињенко такође радио са шпанским службама безбедности, чији је руководилац био под псеудонимом *Ури*, снабдевајући их информацијама о организованом криминалу и активностима мафије пореклом из РФ који делују у Шпанији." Поред наведених констатација, бранилац је тражио да суд размотри да ли служба безбедности Војног обавештајног одељка 6, није испунила своју дужност да заштити Литвињенка од „правог и непосредног ризика по живот" (Litvinenko & Felshtinsky, 2013, p. 10). Индикативна је и смрт одбеглог олигарха из РФ Бориса Березовског који је у Лондону наводно извршио самоубиство под тушем 23. марта 2013. године, што је остало као неразјашњено самоубиство са сумњом рада за две службе безбедности из различитих држава, што је сасвим довољан основ службама за *смртну пресуду*. Редак радиоактивни отров изгледа као неочекиван начин да се изврши убиство бившег (одбеглог) колеге из службе безбедности, али у пракси то није реалност код Савеза Совјетских Социјалистичких Република (односно РФ) где су употребљавани слични отрови више од пола века. Први регистрован случај радиоактивног напада догодио се у Франкфурту 1957. године и укључивао је Савез Совјетских Социјалистичких Република, када је пребегу Николају Хохлову (*Nikolai Khokhlov*), капетану у служби безбедности Савеза Совјетских Социјалистичких Република, дат талијум без мириса у шољици кафе. Ана Политковскаја (*Anna Politkovskaya*) је умало умрла почетком септембра 2004. године када је отрована у авиону за Северну Осетију. Политковскаја је намеравала да учествује у решавању талачке кризе у Беслану, која је почела 1. септембра 2004. године. Веровало се да је Политковскаја, која је уживала велико поштовање међу Чеченима, могла да учествује у преговорима са терористима и омогући ослобађање талаца. Службе безбедности РФ су очито процениле другачије са задатком да је од виталног значаја спречити Политковскају да стигне у Северну Осетију како не би она преузела заслуге. Током пута, у авиону, Политковскаја је затражила од стјуардесе шољу чаја након чега се онесвестила и пробудила у болници. Преживела је, али је закаснила на преговоре са терористима у Беслану пошто је то време провела у болници. Политковскаја је ипак доживела трагичну смрт када је убијена ватреним оружјем 7. октобра 2006. године, само месец дана пре Литвињенка (Litvinenko & Felshtinsky, 2013).

Припадници Јединице 29155 су елемент војне службе безбедности Главне управе (раније Главне обавештајне управе) који су највише оптуживани за спровођење тајних операција, необавештајних активности широм Европе. Ради се о јединици која реализује задатке физичким присуством својих оперативаца на терену (у иностранству), као што је реализација, спровођење атентата (Сергеј Скрипал 2018. године), политичко мешање (у Украјини, Молдавији, Црној Гори, Шпанији и Уједињеном Краљевству) и диверзантске операције – у Чешкој и Бугарској (Riehle, 2022).

Експлозија аутомобила (чији је власник Александар Дугин и који је требао бити у том возилу након завршеног фестивала којем је присуствовао са својом кћерком) десила се на аутопуту код Москве, РФ, дана 20. августа 2022. године (што су пренели сви светски медији) када је у аутомобилу била Дугинова кћерка (*Дарја Дугин*) где је од силине експлозије (највероватније око 400 грама тринитротолуена – експлозива) погинула на лицу места. Ово представља директан атак на политичку елиту РФ, односно најближе сараднике председника

РФ, Владимира Путина. Званичници РФ су дали обавештење да се ради о политичком тероризму Украјине, што је демантовано од стране званичника Украјине, али службе безбедности РФ су врло брзо идентификовале држављанку Украјине коју су довеле у везу са овим атентатом. Ово је уједно била и порука од служби безбедности Запада (не Службе безбедности Украјине) да могу да дођу до било кога и било где уколико буду желели, како би реализовали одређену паравојну активност.

Мали и тајни ратови током хладног рата и у периоду постхладноратовског периода су створили читаву нову индустрију паравојних операција, које функционишу као заступници неколико великих сила (трговаца оружја и сл.) у сукобима трећег света и можда управо ти интереси диктирају употребу истих, а не презентоване процене служби безбедности или неких туђих усмерења. Сасвим је вероватно да су Централна обавештајна агенција и друге службе безбедности учиниле све да неуспеле, покренуте паравојне операције, остану тајне управо зато што су били мали или половични покушаји који никада нису уродили плодом.

Увидом у *Речник српског језика, Матице српске* констатујемо следећа значења речи *диверзија.* Наиме, једно од значења је „да се ради о војној операцији, акцији која се врши одвојено од центра бојишта да би се одвукле противничке снаге и одвратила непријатељска пажња са главног бојишта; други је да се ради о акцији коју врше групе или појединци у непријатељској позадини у циљу разарања и уништавања непријатељских објеката – вршити диверзије; трећи као најбитнији за ово истраживање представља илегалне акције, *саботаже* страних агената у некој држави, онеспособљавање важних војних и индустријских објеката и слично" (Вујанић и сар., 2011, стр. 262). Ради се о вишезначној речи, како у нашој тако и у другим државама. Део држава диверзију сврстава у врсту саботаже, а део је посматра као самосталну активност, затим различите структуре и професије користе у различитом значењу исту реч. Основне карактеристике диверзије су разарање, саботажа коју врше агенти неке стране државе, неслагање у мишљењу, разна размимоилажења, одвраћање, скретање са планираног правца, спречавање реализације одређених намера и друго.

У истом речнику, *Речнику српског језика, Матице српске*, реч *саботажа* је одређена као „потајна, илегална делатност уперена против постојеће власти, а може да представља намерно избегавање вршења одређених радњи и дужности, рушење, кварење производних средстава, прометних средстава и сл." (Вујанић и сар., стр. 1158). Можемо да констатујемо да је реч диверзија у једном од одређења објашњена као „саботажна активност, тако да саботажа представља доста шири појам од диверзије, а сама диверзија представља један од облика саботажних активности." Значење речи *субверзиван* у Речнику српског језика је одређено као „делатност рушилачка, превратничка док *субверзивност* и *субверзија* су дефинисани као превратничке, рушилачке активности" (Вујанић и сар., стр. 1259). С обзиром да у енглеском језику реч енг. *Sabotage,* има значење речи *саботажа*, у руском језику се за овај термин употребљава реч рус. *Диверсия.* Треба бити опрезан приликом употребе ових и сличних термина у различитим државама (нормативног одређења – кривични законици и сл., теоријског одређења у различитим областима су одредили ове појмове као што је то случај са Републиком Србијом), односно различитим језичким подручјима.

У кривичном законику[110] РФ појам *саботажа* (рус. *диверсия*) је одређен у члану 281. на следећи начин „Извршење експлозије, паљевине или других радњи које имају за циљ уништавање или оштећење предузећа, објеката, објеката транспортне инфраструктуре и возила, средстава комуникације, објеката за одржавање живота становништва у циљу подривања економске сигурности и одбрамбене способности РФ" (Уголовный кодекс Российской Федерации, 1996, члан 281.).

У децембру 2022. године, председник РФ је потписао Указ о проглашењу Федералног закона N 586–ФЗ дана 29. децембра 2022. године. Овим законом, односно изменама и допунама Кривичног законика РФ, омогућено је увођење кривичне одговорности за *помоћ, обуку и организовање саботажних активности*. У Кривични закон су уведена три нова члана и то: члан 281.1 – *Помоћ* у субверзивним активностима, члан 281.2 – *Обука* у сврху обављања саботажних активности и трећи члан 281.3 – *Организовање* саботажне заједнице и учешће у њој. За сва ова три придодата члана у федералном закону, максимална предвиђена казна је доживотна робија (Федеральный Закон N 586–ФЗ, 2022). До прописивања ових *вртоглавих – драконских* мера, доживотних казни за ова дела довела је огромна примена саботажних активности на територији РФ где су званични припадници руководства РФ изнели податке да се у 2021. години догодила једна саботажа док је у 2022. години регистровано 20 саботажа, а неки медији наводе и далеко, далеко већи број саботажа од овог броја на територији РФ од периода отпочињања сукоба РФ и Украјине. Овде видимо хитно предузимање једне од мера државе у безбедносној заштити исте. Поред предузимања мера, региструјемо већ добро познату тактику деловања да услед погоршања међународних односа између држава или избијања сукоба, долази до повећања интензитета саботажа као једне од активности присиле над другом државом, савезом и другим ентитетом.

Велики део аналитичара је констатовао велике казне које су уведене овим изменама и допунама Кривичног законика РФ 2022. године, а као основну карактеристику овог федералног закона препознајемо максималну казну – доживотни затвор за починиоце ових дела, међутим о узроку, односно осталим ставовима у оквиру сваког од ова три члана (281.–1,–2,–3) није се детаљно коментарисало, што нас дефинитивно и доводи до одговора зашто је уопште уведен овакав пропис. Разлог је наравно енормно повећање субверзивних активности од стране страних служби безбедности на територији РФ где се и у самом пропису наведено може препознати. Наиме, у члану 281.1 у склопу помоћи субверзивним активностима већ у првом ставу се наводи *врбовање* или *друго укључивање* у извршење дела где се директно ради о спутавању рада стране службе безбедности у врбовању лица. Поред врбовања, предвиђено је и да обука и финансирање је обухваћено овим делом, тако да и лица и фирме укључене у ове послове долазе под утицај овог закона. Као посебно специфичан сегмент треба нагласити дела која су учињена од стране лица које користи свој службени положај за реализацију дела из члана 281, затим помагање у реализацији дела, организовање или руковођење извршењем или финансирањем где препознајемо циљну групу законодавца, а ради се и о свим оним логистичким и другим помоћима приликом реализовања субверзивне активности које до сада нису биле директно обухваћене за све учеснике у кривичним делима са оволико високим казнама – доживотни затвор. Важно је нагласити да је законодавац

[110] Статья 281. Диверсия, Уголовный кодекс Российской Федерации от 13.06.1996 N 63–ФЗ (ред. от 29.12.2022).

предвидео и када се лице може ослободити од кривичне одговорности, а то је благовременом пријавом кривичног дела или спречавањем истог. Овај став је јако битан, јер је службама безбедности, па и полицији, односно надлежним судовима, дао могућност лакшег *приступа* члановима група, приближавању истим, документовања и завршетка, правилног процесуирања судског поступка. Саботажна *пропаганда* у смислу члана 281.3[111] овог законика подразумева „делатност ширења материјала и (или) информација у циљу формирања уверења лица о потреби вршења саботажних радњи". Овде препознајемо изузетно широк спектар могућности подвођења разних пропагандних активности под овај термин „ширење" и „формирање уверења", што овако уопштено може скоро било који облик довести под ово деловање. На крају можемо да закључимо да је државни апарат РФ на изузетно интелигентан начин, под реалним оправдањем огромног повећања броја субверзивних активности на територији РФ у 2022. години, на прикривен начин обухватио, предвидео кроз ове измене и допуне Законика скоро све или већину необавештајних активности које предузимају службе безбедности – политичких, економских, паравојних, пропагандних активности, и прописао страховито велике казне за починиоце ових кривичних дела, чиме ће страним службама безбедности које делују на територији РФ у наредном периоду дефинитивно направити велики проблем у раду, што је онај посредни, невидљиви за већину лица, па чак и аналитичара, крајњи циљ ових допуна и измена Законика, а не само сузбијање субверзивних активности.

У Кривичном законику[112] Републике Србије појмови *диверзија* и *саботажа* су одређени као два посебна дела, на следећи начин. У члану 313. за *диверзију* Законик наводи да „ко у намери угрожавања уставног уређења или безбедности Србије рушењем, паљењем или на други начин уништи или оштети индустријски, пољопривредни или други привредни објекат, саобраћајно средство, уређај или постројење, уређај система везе, уређај јавне употребе за воду, топлоту, гас или енергију, брану, складиште, зграду или какав други објекат који има већи значај за безбедност или снабдевање грађана или за привреду или за функционисање јавних служби, казниће се затвором од пет до петнаест година" (Кривични законик Републике Србије, 2019), док за *саботажу* у истом Законику у члану 314. је констатовано да „ко у намери угрожавања уставног уређења или безбедности Србије на прикривен, подмукао или други сличан начин у вршењу своје службене дужности или радне обавезе проузрокује штету која прелази износ од милион и петсто хиљада динара за државни орган или организацију у којој ради или за други државни орган или другу организацију, казниће се затвором од пет до петнаест година" (Кривични законик Републике Србије, 2019). Овде препознајемо више битних разлика између диверзије и саботаже и законодавац их препознаје као различита дела за исто угрожавање, али уз друге квалификације (да је дело учињено на прикривен, подмукао или други начин, током вршења службене дужности или радне обавезе и да та штета нанета државном органу или организацији мора прелазити одређену материјалну вредност; овде конкретно се ради о износу од 1,5 милион динара – Република Србија и више).

[111] Статья 281.3, Организация диверсионного сообщества и участие в нем, Федеральный Закон N 586–ФЗ.
[112] Члан 313. и 314, Глава двадесет осма, Кривична дела против уставног уређења и безбедности Републике Србије, *Кривични законик Републике Србије* из 2019. године.

С обзиром на вишедимензионалност субверзивних активности, није могуће направити квалификацију или набројати све субверзивне активности или врсте истих, већ се према досадашњим истраживањима наведене активности могу груписати у одређене области. Колико услови, техника, технологије, савремене претње буду диктирали угроженост одређене категорије, наведене активности ће неминовно бити приморане на адаптацију ради правилног и правовременог супротстављања савременим претњама, што ће довести и до нових облика субверзивних активности, па и супротстављања истим.

У политичко – војним круговима врло често је присутно размишљање да остварење циља не треба да бира средство за његову реализацију. Стратешки менаџмент Североатлантског савеза је приликом његовог формирања изнео циљ постојања савеза: да САД доведу у Европу, затим Немачку ставе под контролу и да Савез Совјетских Социјалистичких Република (данас РФ) отерају из Европе (што се тренутно дешава). Овом констатацијом можемо закључити да су сви поступци које су службе безбедности САД, првенствено у сегменту необавештајних активности у оперативном смислу предузимале у претходним деценијама према РФ (као и према другим државама) довели до фантастичних (врло ефикасних) резултата на терену служби безбедности, што дефинитивно службе безбедности РФ нису успеле да сустигну, па је баланс привремено успостављен (или у покушају успостављања) развојем нових информационих технологија и модернизацијом наоружања (Марјановић, 2022). Али исто као што је у Њујорку требало да се догоди 11/09 да би службе безбедности дошле до закључка да је човек основа свега, а не техника, што су САД одмах кориговале након ових пропуста и увеле низ новина и пребациле тежиште у раду на човека (као индивидуе или као корекције у раду на уочене проблеме у координацији рада служби безбедности, које су решене деловањем стратешког државног менаџмента и брзини његовог прилагођавања новонасталим претњама и одвраћању), тако ће вероватно и РФ тренутна збивања у војним операцијама у Украјини сагледати и кроз нови концепт одвраћања прилагодити новим претњама (сагледати да ли само ударна моћ или технологија може сама одговорити задацима стратешког менаџмента у освајању других држава). Државни менаџмент великих сила тренутни концепт одвраћања спроводи комбинованим ангажовањем, и то служби безбедности са тежиштем њиховог рада не на необавештајним активностима као основом рада служби, деловања према држави, већ се необавештајне активности (првенствено политичке, пропагандне, економске, паравојне) користе ради подршке другим активностима и то првенствено војне природе. Начин будуће употребе служби безбедности од стратешког државног менаџмента ће бити умногоме везан за развој нових технологија и то ће првенствено представљати једну од граница, лимита употребе истих (Марјановић, 2022).

6. ПРИМЕРИ НЕОБАВЕШТАЈНИХ АКТИВНОСТИ СЛУЖБИ БЕЗБЕДНОСТИ У ФУНКЦИЈИ ОДВРАЋАЊА

Савремени конфликти се свакодневно припремају од великих сила и то употребом свих инструмената моћи. Циљ је стварање, успостављање несигурности како политичке тако и економске. Наведено се манифестује у облику трговинских ратова, енергетских уцена, пропаганде, политичких превrата, сајбер напада, дипломатских превара и разних других уцена и принуда ради остваривања неких погодности (Јефтић, Мишев, Обрадовић и

Станојевић, 2018). Анализирајући наредних неколико примера необавештајних активности служби безбедности у функцији одвраћања сагледавамо специфичности најфреквентнијих облика одвраћања примењиваних у Естонији, Криму и Украјини.

6.1. СТУДИЈА СЛУЧАЈА: ЕСТОНИЈА

Студија случаја је везана за актуелне догађаје из 2007. године у Естонији. У пролеће 2007. године, Естонија је потпала под кампању сајбер напада која је трајала укупно 22 дана. Политички мотивисана кампања сајбер напада у Естонији је трајала двадесет два дана, а ниједна организација или група није преузела одговорност за сајбер нападе. Поред сајбер напада паралелно су реализовани политички, економски и информациони напади на Естонију, као и неколико изолованих физичких обрачуна (Ottis, 2008).

6.1.1. Корени сукоба између Русије и Естоније

Након распада Савеза Совјетских Социјалистичких Република 1991. године, Естонија се придружила Североатлантском савезу 2004. године. Овај поступак је био предмет спора РФ и њених постсовјетских суседа. Најава да ће статуа Бронзаног војника бити померена изазвала је насилне немире на улицама Естоније, па је тако дана 26. и 27. априла 2007. године велики број етничког руског становништва у Естонији изашао на улице и оптужили су естонску владу да жели да промени историју, односно да промени улогу Савеза Совјетских Социјалистичких Република у Другом светском рату. После насилног сукоба између полиције и демонстраната, естонска влада је преместила Бронзаног војника у касним сатима 27. априла и поставила споменик на војном гробљу у Талину 30. априла (Spiegel, 2017). Овај догађај, као и протести, називани су *бронзана ноћ*.

Етничко руско становништво у Естонији је посматрало Бронзаног војника као сопствени симбол. Статуа обележава совјетско ослобођење Естоније од нациста које се догодило 30. априла. Руска Федерација је става да расељавање статуа нарушава права етничких Руса и да ће Естонија платити последице измештања. У РФ, омладинска група је демонстрирала против естонског амбасадора и напала амбасаду Естоније у Москви. Већина протеста у РФ је била финансирана од Владе РФ, нпр. *Наши су* или *Омладински покрет, наши!*, где су ове групе успостављене 2005. године. Ове антифашистичке студентске групе сада имају више од 100.000 чланова. Демонстрације испред амбасада нису престале све док амбасадор није напустио РФ, а Влада РФ је чак суспендовала железнички саобраћај између Талина и Ст. Петерсбурга (Miniats, 2019)

У студији случаја кризе између РФ и Естоније, као и мера које су уследиле ради исте, изведене су кључне констатације испољавања необавештајних активности служби безбедности и других активности предузиманих од ових држава ради остваривања својих националних циљева (Connable et al., 2020).

6.1.2. Радње и поступци Естоније

Природа и извођење сајбер напада нису били нови на техничком нивоу. Можемо констатовати да се показало да није њихова техничка иновација, него обим и употреба у датом политичком контексту, то што има врло битан утицај на националну политику сајбер безбедности Естоније и упозорења за Североатлантски савез да ревидира своја стратешка документа у областима сајбер одбране. Специфичности које је донео овај сет сајбер напада у

Естонији, једној од најдигитализованијих нација на свету, огледају се у новој политичкој претњи која је захтевала мултинационалне одговоре међународних институција колективне одбране и безбедности по овим питањима. Сајбер напади у пролеће 2007. године су указали на многа нерешена или недовољно дефинисана, одређена питања у оквиру саме алијансе и то категоризације сајбер домена у домену традиционалних међународних односа када сајбер напад представља оружани напад и који се конвенционални међународни закони примењују на неконвенционалну сајбер претњу? Догађаји у Естонији 2007. године су означили значајну промену оперативне стратегије у политици сајбер одбране Североатлантског савеза. Званичне декларације Североатлантског савеза о сајбер претњама откривају нагласак на техничким решењима за сајбер претње, као што је заштита кључних информационих система Североатлантског савеза, док је сајбер безбедност углавном била остављена у рукама појединачних држава чланица. Недостатак за Североатлантски савез је постао очигледан када су истраге о актерима који стоје иза сајбер напада на Естонију открile да не постоји званични протокол за одговор на сајбер напад који би могао осакатити дигиталну инфраструктуру државе чланице. Важно је нагласити да је у извештајима естонског и савезничког тима закључено да се не може доказати било каква умешаност РФ у ове нападе, али без обзира на то, тадашњи министар спољних послова Естоније, Урмас Пает (*Urmas Paet*), није се обазирао на то што нема доказа о умешаности РФ, већ је оптужио Владу РФ да је организовала сајбер нападе на Естонију. Приписивање сајбер напада државном актеру зато што рачунар са којег је напад покренут користи своју националну сајбер инфраструктуру може бити погрешно, а основни је разлог то што рачунари могу бити хаковани и контролисани са даљине, односно из друге државе, што ствара погрешан закључак. Џефри Кар (*Jeffrey Carr*) који је 2008. године створио пројекат енг. *Grey Goose* како би покушао да припише одређене сајбер нападе конкретним појединцима, дошао је до закључка да „није довољно нити правно оправдано једноставно пратити напад до сервера који се налази у страној земљи" (Spiegel, 2017, p. 26).

Одбијањем сарадње РФ да се пронађу наводни починиоци сајбер напада из РФ су овим поступком осујећени. Важно је напоменути да је до 2009. године Естонија процесуирала само једно лице по овом питању, а ради се о Димитрију Галушкевичу (*Dimitri Galushkevich*), студенту и естонском држављанину етничког руског порекла, који је ухапшен и осуђен за незаконито блокирање компјутерских података и кажњен је новчаном казном износа отприлике 1120 евра. Недостатак одговорности државног актера, приликом реализације сајбер напада у Естонији довео је до развоја свеобухватне стратегије сајбер безбедности, која је усвојена у мају 2008. године, годину дана након напада. У Североатлантском савезу је дошло до промена након ових догађаја у Естонији 2007. године. Североатлантски савез је посветио много више сегмената рада сајбер претњама од 2008. године у поређењу са претходним годинама, најављујући креирање политике сајбер одбране која је одобрена јануара 2008. године. Наглашена је потреба за заштитом кључних информационих система држава чланица, али је укључена и реченица о јачању капацитета организације да помогне савезничким нацијама у супротстављању сајбер нападима. Тако је Североатлантски савез 14. маја основао енг. *Cooperative Cyber Defence Centre of Excellence* у Талину (*Tallinn*), главном граду Естоније, након чега је започет рад на успостављању закона, правила и норми које би требало да регулишу међудржавне сукобе у сајбер простору. Сајбер напади спроведени у Естонији су први ове врсте на планети тих размера, а који су усмерени

на дигиталну инфраструктуру једне нације. Наиме, ради се о великим размерама и примио је облик политичког сукоба у источној зони утицаја Северноатлантског савеза. Стварање центра за истраживање и обуку видимо као још један облик, последицу ових напада, а он још увек функционише. Наводно је национална одбрана Естоније од сајбер претњи значајно ојачана. Сајбер напади на Естонију су открили да би држава чланица Северноатлантског савеза могла бити економски, друштвено и политички осакаћена сајбер нападима, што је једним новим видом сајбер напада (годину дана касније руско – грузијски рат у августу 2008. године) представљао пример употребе сајбер ратовања као дела конвенционалног ратовања (Spiegel, 2017).

Сумирајући хронологију догађаја приликом реализованих сајбер напада у Естонији, могу се констатовати следећи закључци:

Први, да је РФ наведено спровела као одмазду за покушај мењања историјске важности руског народа у Другом светском рату и уједно практичну проверу сајбер способности за предстојећи напад на Грузију.

Други, да је контролисани учесник можда био управо онај ко је дириговао Влади Естоније померање споменика. Чињенице које потврђују наведено су следеће. Влади Естоније померање споменика је могао *наредити* само ментор, а то није РФ. Обично тај који направи проблем врло често се појављује и као страна која решава исти тај проблем. Формирање центра Северноатлантског савеза за сајбер одбрану, представља следећи битан моменат са личним присуством стручних лица из Северноатлантског савеза у том центру који се налази у Естонији. Судско процесуирање само једне особе са малим новчаним износом где се оптужује велика сила, РФ, у спровођењу сајбер напада на државу. Сувише јаван наступ са борбом за споменик, руским заставама, заштитом руских интереса и слично.

Након дужег временског периода неслагања између Владе РФ и Естоније, кулминација или врхунац лоших спољно – политичких односа ових држава се догодила када је Влада Естоније донела одлуку којом је свесно извршила провокацију народа РФ када је одлучила да премести статуу изграђену у част Совјетског ослобођења Естоније у Другом светском рату (Бронзаног војника). Руска Федерација је уложила напоре да спречи пресељење споменика и наведени тренутак искористила да оствари и друге циљеве, одржавање и повећање руског утицаја у Естонији, посебно међу њеним руским и руским говорним становништвом, затим одвраћање цивила из Естоније од подршке Западу и Северноатлантском савезу, као и делимична дестабилизација Естоније како би се осигурала њена континуирана рањивост на утицај РФ (Connable et al., 2020).

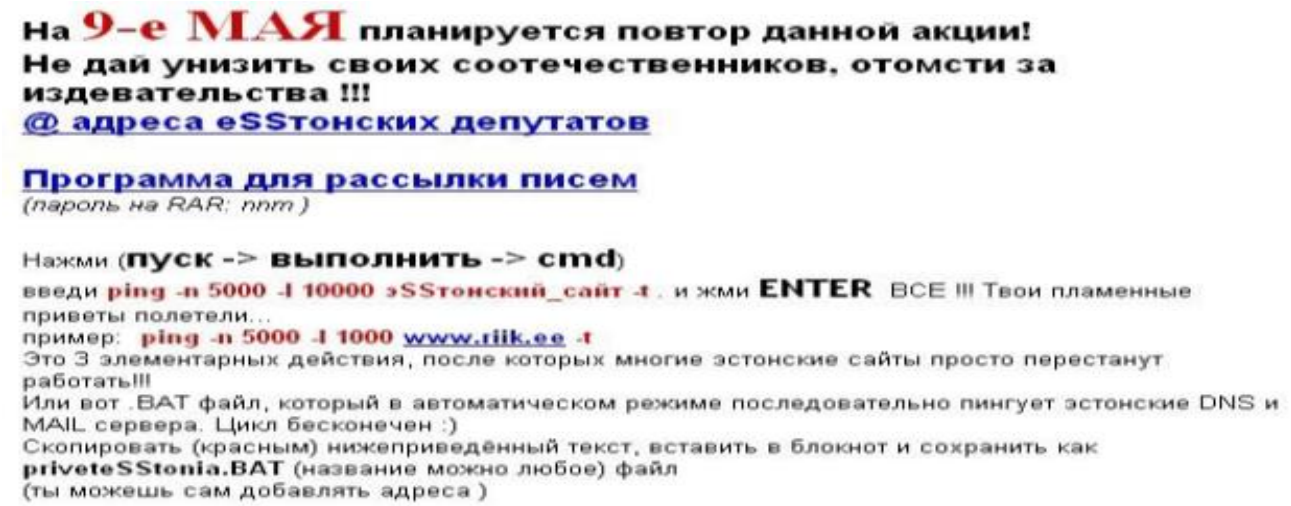
Од првог дана протеста, окупљања руске мањине на улицама Естоније, држава предузима низ репресивних мера и поступака од стране оружане силе, првенствено полиције. Све ово је предузимано с једним разлогом, а то је спровођење донете одлуке (ко зна чије и ко зна где донесене, највероватније не одлуке Владе Естоније, која је била само извршилац, прим. аут.) о премештању споменика Бронзаног војника (Spiegel, 2017).

6.1.3. Необавештајне активности Русије

Дана 27. априла 2007. године (у ноћи када је премештен Бронзани војник), започели су бројни сајбер напади у Естонији. Мете сајбер напада су биле веб – странице естонске Владе, па веб – странице политичких партија, новинских кућа са *нападима ускраћивања услуге* (енг. *Denial of Service – DoS attack*) и *дистрибуираног ускраћивања услуге* (енг.

Distributed Denial of Service – DDoS attack), што доводи до вида блокаде, односно до недоступности веб – страница корисницима. Поступак назван енг. *ping – flooding* је такође коришћен као позив за преплављивање веб – сајтова са *пинг* захтевима који су се појавили на неколико блогова и форума на руском језику. У овом периоду су регистровани и други облици сајбер напада. Наиме, део напада је укључивао уништавање веб – страница, пошто су хакери заменили слику естонског премијера Ансипа са ликом Адолфа Хитлера на званичном владином веб – сајту. Поред овог случаја, и на другим естонским сајтовима су спроведена слична оштећења. Отприлике сви сајбер напади су трајали до 18. маја и циљани су веб – сајтови од владиних институција и естонских интернет провајдера до банака и других услуга које пружа приватни сектор (Spiegel, 2017). Дана 28. априла, регистровани сајбер напади су проглашени за координисане нападе, а не за изоловане догађаје. Џек Авиксо (*Jack Aaviksoo*), био тада естонски министар одбране у време напада, за енг. *WIRED Magazine* је изјавио „да је ово био први пут да је *botnet* угрозио националну безбедност целе нације" (Spiegel, 2017, p. 23).

Ради потребне анализе, коришћене су следеће чињенице из естонског државног тужилаштва. Сајбер напади су се десили у периоду између 27. априла и 18. маја 2007. године. Већина откривених напада може се приписати основном догађају. Наводно, већина злонамерног саобраћаја потиче изван Естоније, а неке банке су привремено прекинуле сав иностран саобраћај. Злонамерни саобраћај је био политички мотивисан и јасна је индикација порекла руског језика. Упити усмерени на владину веб страницу су укључивали фразе попут „АНСИП_ПИДОР=ФАШИСТ" (Ансип је био тадашњи премијер Естоније). Много разних варијанти је коришћено у којима су коришћене и разне вулгарности. Упутства за напад на естонске сајтове су дистрибуирана на многим форумима на руском језику и веб страницама. Пример ових упутстава је приказан у наредном делу рада (види *Слику 7*). Имајте на уму да овај извод укључује информације о томе када, шта и како да се нападне (Ottis, 2008).



Слика 7. Једна од инструкција пронађених на веб локацији током напада.
Извор: Ottis, 2008, p. 3.

Врло често, Естонију називају *еСтонија* због ових догађаја у сајбер простору. До 2007. године, 98% естонске територије је било покривено приступом интернету, док је скоро 50% Естонаца користило интернет. Естонија је такође користила дигиталне потписе и

владине дигиталне базе података. У великој мери, Естонија је зависила од несметаног функционисања својих комуникационих и информационих система, а које су сајбер напади у априлу и мају 2007. године осакатили на националном нивоу. Зависност Естоније од информационих и комуникационих технологија учинила ју је посебно рањивом на сајбер нападе. Када говоримо о сајбер нападима на Естонију који су били везани за употребу дезинформационих кампања, тада говоримо о замени ликова на веб – сајтовима заменом слика шефова државних званичника са Хитлеровом, на пример, дакле о повезивању тадашње Владе Естоније са нацистичком Немачком, алудирајући на то да је Естонија покушала да промени историју уклањањем совјетске статуе са централног трга у Талину. Оваквим и сличним поступцима усмерава се подстицање на перцепцију и мишљење јавности, док у исто време нарушавају информационе и комуникационе системе Естоније. Сајбер напади су укључивали проруску пропаганду од које је само РФ и руска мањина у Естонији имала корист. У периоду сајбер напада, могуће је још увек порицати догађаје. Естонија је као чланица Североатлантског савеза, имала могућност да се позове на члан 5.[113] Северноатлантског уговора из 1949. године, када је била мета сајбер напада 2007. године који представља кључни задатак Североатлантског савеза, колективну одбрану. Међутим, Естонија није разматрала сајбер нападе на њену дигиталну инфраструктуру као оружани напад, па се наводно из тог разлога није позивала на члан 5, па је Североатлантски савез своју подршку ограничио на помоћ Естонији у одбрани њеног информационо – комуникационог система и накнадну истрагу о учесницима одговорним за нападе (Spiegel, 2017).

Сајбер напади су почели у 23 сата по локалном времену у уторак, 8. маја (и ово време почетка је наводно доведено у везу са РФ која је један сат испред временске зоне у Естонији), али су ублажени до 7 часова следећег јутра. Упркос томе, напади су и даље били видљиви у саобраћајним евиденцијама 30 дана након почетног напада. Кулминација сајбер напада је била 9. маја, па је не само време већ и датум доведен у везу са РФ – са *Даном победе* над фашизмом у Другом светском рату. Међу сајтовима погођеним нападима били су и веб – сајтови естонског парламента, министра одбране, као и политичке странке премијера Ансипа и бројних главних универзитета и националних новина. *Hansabank*, највећа банка у Естонији, морала је привремено да престане са онлајн услугама док 97% становништва, које се ослања искључиво на интернет банкарство, није могло да оствари конекцију. Поред већих напада дистрибуираног ускраћивања услуге и ботнет напада, починиоци су такође користили *бомбардовање поште* користећи хаковане е – поруке ради преоптерећења сервера и гашења интернета. *Ратно бирање* је још један метод коришћен у овом сукобу, а обухвата аутоматизоване телефонске позиве који су упућени компанији или институцији, што би остварило ефекат блокада свих канцеларија владе и парламента. Деведесет процената становника Естоније има лак приступ широкопојасном интернету и скоро 100 процената млађе популације је повезано на интернет. После Уједињених Арапских Емирата, Естонија

[113] Члан 5. каже да: „Странке су сагласне да ће се оружани напад на једног или више њих у Европи или Северној Америци сматрати нападом на све њих и сходно томе су сагласне да, ако дође до таквог оружаног напада, свака од њих, у вршењу права на индивидуалну или колективну самоодбрану призната чланом 51. Повеље Уједињених нација, помоћи ће Страни или Странама које су тако нападнуте тако што ће одмах, појединачно и у договору са другим Странама, предузети радње које сматра неопходним, укључујући употребу оружане силе, за обнављање и одржавање безбедности северноатлантског подручја" (Spiegel, 2017, p. 24).

има највећи број претплата за мобилне телефоне. Међународно познати стручњаци су користећи своје вишегодишње знање и стручност, утврдили да су се извршиоци напада вероватно налазили у Естонији. Због чињенице да је већина сајтова са вестима била компромитована, било је немогуће пренети вести о нападу у Естонији како би се друге државе упознале са овим догађајима. Насупрот хваљењу успесима у коришћењу интернета у Естонији и највећим успехом експлоатације истог, ови сајбер напади су показали да е – систем у Естонији има потенцијал да буде и његова пропаст, односно једна од најслабијих и најрањивијих тачака (Miniats, 2019).

Група истраживача је током релизације истраживања дошла до следећих шест метода непријатељских мера које су предузимане током овог периода сагледавања кризне ситуације (студије случаја). Ради се о следећим методама: „подстицање протеста против Владе Естоније коришћењем паравојних снага, притисак на политичке лидере Естоније кроз акције јавне дипломатије осуђујући акције Естоније, примена индиректних економских санкција преко руских компанија, омогућавање грађанске опсаде амбасаде Естоније у Москви, вођење агресивне антиестонске, проруске медијске кампање, наводно спроводи сајбер нападе на владу и цивилну инфраструктуру" (Connable et al., 2020, p. 40–42). Већина догађаја (*Слика 8*) је груписана почетком 2007. године, иако су бојкоти настављени до средине 2008. године.

Слика 8. Непријатељске мере РФ према Естонији – енг. *Estonia Case Timeline.*
Извор: Слика је интерпретација Аутора (In: Connable et al., 2020, p. 41).

Група истраживача долази до следећих констатација истраживањем ове кризе. Ради се о уском, намерном и циљаном, добро координисаном напору који је за већину један део који своје изворе црпи у времену и у географији. Руска Федерација је успешно реализовала већину својих тактичких операција. Важно је констатовати да је дипломатска офанзива била очигледна, међутим, локација тј. извор сајбер напада је квалитетно прикривен. Могу се извући разумни закључци о утицају РФ у протестима и опсади амбасаде. Када анализирамо ове активности, можемо констатовати да је ово била циљана операција која је концентрисала низ непосредних ефеката за постизање конкретног циља. Важно је нагласити да су и након овог периода неке од радњи, активности и мера настављене, али разлика је уочљива у смислу да је ниво интензитета или координације био далеко нижи. Један од закључака је да је РФ успешно спровела своју тактику непријатељских мера, али да део операције није успео (РФ није успела да спречи премештање споменика, статуе). Ова интензивна примена необавештајних активности, непријатељских мера уопште према Естонији од стране РФ, улила је страх у становништво Естоније и поготово у њено руководство. Наведене активности РФ према Естонији су послужиле као чврст аргумент, показатељ Естонији шта би РФ могла да још уради, да се умеша у унутрашње послове Естоније за врло кратко време са минималним ризиком. Ове активности од стране РФ су донекле успеле у подривању перцепције стабилности и моћи Естоније. Међутим, стратешки циљеви РФ у Европи чак и овим успешним застрашивањем су поткопани. Наиме, почев од планиране активности Владе Естоније (премештање Бронзаног војника), лидери у Естонији су тражили одређену сарадњу, заштиту, приближавајући се све ближе Европској унији и Северноатлантском савезу. Примена непријатељских мера са Естонијом је још више одгурнула Естонију од РФ, него што је приближила. Вероватно је управо агресија сиве зоне РФ у Естонији активирала постепено буђење у Северноатлантском савезу, постављајући терен за тренутно отворено противљење агресији РФ (Connable et al., 2020).

Према другим ауторима, анализом реализованих догађаја можемо разматрати неколико вероватних сценарија. *Један* је да се ради о руској информационој операцији против Естоније, *други* да се догодила операција лажне заставе да се РФ постави као нападач, и *трећи* сценарио је да се ради о спонтаном догађају који је био одговор локалног становништва на политику Естоније (Ottis, 2008).

Први сценарио, информациону операцију, овде сагледавамо као коришћење информација и информационе технологије ради утицаја на одлуке и поступке противника. У контексту сајбер напада, обичан грађанин једне државе може бити мотивисан да користи ресурсе под његовом контролом за независни напад на непријатељске системе како би збунио браниоце. Лепота ове врсте сукоба је у томе што пружа скоро савршено порицање за владу или било који други ентитет који стоји иза напада. Можемо рећи да је у нападима вероватно учествовало много људи различитих вештина. Такође је јасно да су напади били политички мотивисани, јер су многи од њих садржали поруку везано за укупни сукоб око статуе. Непријатељска реторика са разних високих рангова политичара у РФ је емитована у медијима и даље дистрибуирана на форумима и веб порталима. Нападачи су добили охрабрење од високих чланова руске политичке елите. Руска Федерација је порицала било какву директну умешаност у сајбер нападе који су погодили Естонију у пролеће 2007. године. Нема доказа о мерама које је Влада РФ предузела да ублажи ситуацију. Под претпоставком да је овај догађај резултат намерне информационе операције, највероватније

је повезан са већим политичким сукобима који су га окруживали. Циљ је могао бити уједињење руског народа против заједничког непријатеља пред изборе. Уколико су сајбер напади били резултат информационе операције, онда би се могло тврдити да је то било делотворно. Напади великих размера изведени су против независне државе, док није било конкретног ентитета који се појављивао као извршилац (Ottis, 2008). *Други* сценарио је да сагледавамо ове активности као операцију *лажне заставе*. Претпоставка да су сајбер напади могли бити операција лажне заставе. Да бисмо схватили, ову вероватноћу узимамо као теоријску претпоставку да онај ко је све организовао и ко је одговоран за све нападе је управо то и желео – да све изгледа као да комплетна организација сајбер напада потиче из РФ (Ottis, 2008). *Трећи* сценарио је да се констатује да се радило о реакцији становништва. Наиме, ова претпоставка говори о томе да су сајбер напади били ништа друго до напади који су попримили масовност, односно постали напади великих размера усмерени против политике Владе Естоније. Као одговор овом сценарију могли бисмо закључити да је ово разлог зашто ниједна организација, агенција или влада није преузела одговорност за нападе (Ottis, 2008).

Билатерални односи РФ и Естоније после 2007. године (сајбер напада) су постали изузетно ретки. Наиме, на интернет презентацији Владе РФ дошли смо до податка да су се четири документа – догађаја догодила у међудржавној сарадњи и то следећи: три су настала 2013. године и један 2018. године. Радило се о следећим догађајима: Споразум између Владе РФ и Владе Републике Естоније о сарадњи у области високог образовања, Споразум између Владе РФ и Естоније о сарадњи и узајамној помоћи у области превенције и ликвидације ванредних ситуација, предлог за потписивање Уговора између РФ и Естоније о руско – естонској државној граници и Уговор између РФ и Естоније о разграничењу поморских простора у Нарва и Фински залив, инструменти за развој територија и инвестициони пројекти од регионалног значаја (Government of the Russian Federation, 2022). Изузетно мали број билатералних контаката између РФ и Естоније након регистрованих сајбер напада говори такође много у вези евентуалних закључака: коме је било у интересу да се догоди наведено?

6.2. СТУДИЈА СЛУЧАЈА: КРИМ

Крим и главни град на полуострву Крима, Севастопољ, 16. марта 2014. године су одржали референдум о независности Крима, односно грађани су се изјаснили о томе да Крим постане саставни део РФ (96,77% грађана Крима изјаснило се да хоће да постане федерални субјект РФ). Руска Федерација је за кримски Устав из 1992. године рекла да је ништаван, а овај устав је прописао да Крим потпада под територијални суверенитет Украјине. Крим је предат Русији под Катарином Великом 1792. године, а Савез Совјетских Социјалистичких Република је 1954. године пренео Кримску област у састав Украјинске Совјетске Социјалистичке Републике. Након што је Украјина 24. августа 1991. године затражила независност од Савеза Совјетских Социјалистичких Република, Крим је остао регион Украјине. Руска Федерација је довела у питање законитост преласка Крима у састав Украјинске Социјалистичке Републике 1954. године, тврдећи да је Крим правно и даље део РФ. Уговор између самопроглашене Републике Крим и РФ потписан је 18. марта 2014. године чиме је Република Крим постала саставни део РФ. Кримски сепаратисти и руске снаге су сутрадан истерали украјинске снаге из спорних региона. Украјина и међународна

заједница нису прихватиле де факто независност Крима и Севастопоља од Крима. Анексија Крима је дочекана протестом од стране међународне заједнице, економским санкцијама уведеним РФ и престанком њеног чланства у Групи осам индустријски најразвијенијих и привредно најмоћнијих држава на планети. Крим је, међутим, остао де факто независан од Украјине (Spiegel, 2017).

Стручњаци и дописници медија стално наводе да је криза у Украјини највећи сајбер рат још од времена сајбер напада на Естонију 2007. године и Грузију 2008. године. Операције којима се долази до снимљених телефонских разговора између званичника САД Викторије Нуланд (*Victoria Nuland*) и амбасадора САД у Украјини, као и шефа дипломатије Европске уније Кетрин Ештон (*Catherine Ashton*) и естонског министра спољних послова Урмаса Паета (*Urmas Paet*) су били приказ моћи *једне стране* да се докаже слаба безбедносна и контраобавештајна заштита западних државних комуникационих линија на највишем – стратешком нивоу и да доведе до дискредитације западних лидера и подели их. Током припрема за преузимање, анексију Крима, РФ је успела да погоди скоро све веб – сајтове украјинске владе и да поремети важну комуникацију система украјинских снага са седиштем на Криму. Део сајбер напада је као мете имао новинске куће и друштвене мреже тј. веб странице. У Украјини је служба безбедности известила да је напад на системе мобилних комуникација и чланова украјинске владе реализован са циљем ометања комуникације између власти и службе безбедности. Украјинска компанија *Ukrtelecom* је објавила да су необележени наоружани људи упали у инфраструктурне објекте изазивајући колапс свих комуникација. У комбинацији са поремећајем емитовања украјинских масовних медија на Криму, ово је створило савршене услове за преузимање дела територије. Такозвани *Сајбер Беркут* (енг. *Cyber Berkut*)[114] је био битан учесник у сајбер рату током кризе у Украјини (Bērziņš et al., 2015). Група је изјавила да ће се борити против актуелне Владе Украјине која глорификује неофашизам и екстремни национализам. Напад на кооперативни сајбер одбрамбени центар Североатлантског савеза (енг. *NATO Cooperative Cyber Defence Centre*) је за *Сајбер Беркут* посебно занимљив, јер је *Сајбер Беркут* изјавио да центар помаже украјинској влади да спроводи пропаганду над становништвом, путем масовних медија и друштвених мрежа, блокира објективне изворе информација и прикрива недозвољене радње власти у Украјини. Релативно је мало међународноправних ограничења која озбиљно могу да угрозе неку државу са прописаним регулативама за информационе операције, односно снагама које могу да докажу (материјализују) такве активности (Bērziņš et al., 2015).

[114] *Cyber Berkut*, енг. – наводно добровољна анонимна група појавила се након распуштања злогласних снага безбедности *Беркут* у Украјини крајем фебруара. Ова група је као мете користила како Украјинску владу тако и стране владе које подржавају Украјину. Наведено је постало познато јавности када је *Сајбер Беркут* објавио телефонску дискусију између госпође Ештон и господина Паета као и приликом напада веб – странице енг. *NATO Cooperative Cyber Defence Centre of Excellence* и самог Североатлантског савеза. *Сајбер Беркут* проруска група има *близанца* у Украјини, са супротстављеним задацима, ради се о енг. *Cyber Hundred* (рус. *Кибер сотня*) који је проукрајинска група чији је главни задатак био да се бори против информационих операција, а за заштиту интереса Евромајдана. Најпознатије активности енг. *Cyber Hundred* биле су хаковање веб – странице *RT TV* канала *Русија Данас* (познатог као енг. *Russia Today*) и владине новине енг. *Russkaya Gazeta – Руска газета* (Bērziņš et al., 2015).

6.2.1. Геостратегијски и геополитички положај Крима

Некада давно, концентрацијом великог броја војника на једном месту је решаван проблем копнене моћи, међутим, већ дужи низ деценија, постоји све већи проблем доласка до војника, па се и евентуална смрт војника тешко може оправдати у својој држави, тако да се прелази на интензивну употребу високопрецизних, изузетно разорних борбених средстава који ће обезбедити толику разорност на копну да се противникова војска једноставно повуче (оно што преживи) као и употребе аутономних борбених средстава без присуства човека (руковалац борбеног средства се може налазити далеко од места сукоба, чак и на другом континенту). Стратегија је још у доба Наполеона дефинисана као нешто што представља уметност у коришћењу времена и простора (Owens, 1999). Геополитика је спона између географије и стратегије и представља њихов ослонац. Географија дефинише ограничења и могућности у међународној политици. Сврха стратегије је да се искористе сопствене географске предности и поготово географске рањивости непријатеља или противника. Геополитика је динамична и представља међународну стварност, представу моћи која се види у утицају географије и технологије, а наравно и економског развоја (Owens, 1999). Напредак технологије и велико нагомилавање одређеног капитала могу утицати на измену, кориговање, модификовање, али не и поништити значај, поготово стратешки, неког географског простора (Owens, 1999). Географски простор представља врло важан стратешки фактор и извор моћи, али морамо констатовати да је географија део укупности глобалних појава (Марјановић и Мићовић, 2023). Геополитика асиметричних претњи у односу на копнену моћ врло лако може испољити утицај који попут брзине муње могу изазвати ефекте још брже промене са једне стране копна, простора, земљишта на другом делу копна који се може наћи и скоро на другом крају планете и да оствари несагледиве тектонске промене у изради стратегија држава на читавој планети (Марјановић и Мићовић, 2023).

У постхладноратовском периоду, однос власти РФ према ширем региону Балтичког мора фокусиран је на одржавање стабилности и континуирани приступ Калињинграду, Санкт Петербургу и другим балтичким лукама као и одржавање приступа балтичком гасоводу Немачкој. Политика РФ према Естонији, Летонији и Литванији се огледа у следећем: балансирање против Североатлантског савеза (односно САД), контрола енергетске и транспортне инфраструктуре, проширење политичких права на руске мањине (посебно у вези са држављанством и језичким правима у образовању) и промовисање историјске улоге Руса у ослобађању Европе у Другом светском рату. Однос тона РФ према балтичким државама директно је пропорционалан тону односа РФ са САД. Важно је констатовати да РФ не гледа на бивше републике Савеза Совјетских Социјалистичких Република као на независне актере, већ их посматра као обично оруђе Запада. Поменуте државе, Естонију, Летонију и Литванију, РФ посматра као оруђе Североатлантског савеза (односно САД) и Европске уније. Када је реч о неким другим државама, попут Украјине, нећемо ни коментарисати о каквом *оруђу* се ради. Чим су спољнополитички односи РФ и САД у добром стању, тада су и односи са државама које РФ сматра за оруђа САД добри, и обрнуто. Страх РФ од ширења Североатлантског савеза, посебно од присуства снага Североатлантског савеза у Немачкој, Пољској, Украјини, балтичким државама, проузроковало је жестоке реакције политичара у РФ. Наведена констатација подстиче званичну реторику која наговештава инвазије РФ са циљем повраћаја својих бивших делова, некада совјетских република. Последица повећаног присуства Североатлантског савеза у некадашњим

републикама Савеза Совјетских Социјалистичких Република и тампон државама за РФ представља директно угрожавање националне безбедности државе што је довело до повећања куповине наоружања оружаних снага РФ и повећаном нуклеарном реториком у одвраћању. Енергетска и транспортна инфраструктура у балтичким државама и РФ је међузависна. Тренутна енергетска политика РФ је да задржи тржиште којим доминира РФ. Поред тога, РФ тражи наставак приступа лукама топле воде у балтичким државама. Етно – језичке тензије стварају поделе које РФ може да искористи. Врло велико иритирање политичара и јавности у РФ је било након погоршавања наратива балтичких држава да је нацизам био оправдан да се супротстави Стаљину и да би балтички регион који су окупирали нацисти био бољи од оног који је окупирао Савез Совјетских Социјалистичких Република, што представља један у низу покушаја меке моћи, утицаја Запада да минимизира учешће Савеза Совјетских Социјалистичких Република у спашавању Европе (Kristek, 2017).

Сагледавајући анексију Крима из угла географије односно географског положаја полуострва, може се одмах констатовати да је Крим било лако затворити копнено. Ради остваривања контроле над овим полуострвом, било је неопходно преузети мали број доминантних тачака и самим тим релативно једноставно одбранити се од евентуалног контранапада. Треба констатовати да је и РФ такође лако могла да спречи копнену комуникацију између Крима и остатка копна. Крим је био административни ентитет, са властитом политиком и историјом, укључујући одређени степен политичке аутономије, што поред географских елемената чини јако битан сегмент у сагледавању геополитичког положаја полуострва. Крим је, географски посматрано, био полуострво физички најближе руском Јужном војном округу (овај војни округ је имао највиши степен приправности оружаних снага РФ, где се наводе подаци попуне од око 90 процената). Констатација је да РФ вероватно не би могла да изведе такву операцију, у истом или сличном временском периоду, против неких делова региона где би се ослањали на Далеки исток или можда чак на централне округе РФ, ради физичке велике удаљености и нивоа приправности оружаних снага РФ који су у овим деловима РФ доста нижи од поменутих. Сплет околности или читав низ брижљиво планираних фаза припрема за реализацију сложених операција, анексије Крима, нису ишле у прилог Украјини. Наиме, Јужни војни округ већ је комплетно био у високој приправности свих снага безбедности РФ, а разлог томе (тада сасвим оправдан) је било спровођење мера пуне безбедносне заштите овог региона ради одржавања Олимпијских игара у Сочију где је РФ била домаћин (говоримо о периоду фебруар и март 2014. године). Географска близина полуострва Крим уз изузетно добру попуњеност са високом концентрацијом спремних оружаних снага РФ омогућила је брзо војно заузимање полуострва, пребацивањем снага РФ (пешадије и специјалних снага) ваздушним и поморским путем, које су преузеле почетну контролу над полуострвом. На основу свих наведених чињеница, реалност је да Украјина ефективно није имала апсолутно никакве изгледе да одбрани ово полуострво или да евентуално реализује било какву од борбених нападних операција када су на терену јединице оружаних снага РФ (уз приватне војне компаније и ангажовање служби безбедности) почеле да се концентришу на полуострву и преузимају све кључне тачке (Kofman et al., 2017). Анализирајући близину РФ и Крима, ту културну близину, што је оружаним снагама РФ и другим ангажованим целинама у операцији анексије Крима олакшало ангажовање које се огледало у дељењу истог језика, културе и етничке припадности већине Кримљана. Ове чињенице су омогућиле велику

предност РФ. Припадницима служби безбедности РФ је било доста лакше да се уклопе међу Кримљане и организују, усмеравају, обавештавају, координирају или предузимају и сами одређене акције у циљу спровођења сада самоодбране. Припадници специјалних снага, падобранци су се могли претварати као да су полицијске или унутрашње снаге и да спроводе контролу евентуалних нереда против демонстраната. Заједнички језик и култура на овим просторима, дозвољавали су оружаним снагама РФ и другим целинама ангажованим на анексији Крима да се брзо инфилтрирају у конкретно окружење и да преузму контролу над полуострвом. Без посебних припрема припадника оружаних снага РФ и других целина ангажованих у операцији су могли тренутно бити спремни за комуницирање са позитивно настројеним становништвом и тиме олакшати преузимање полуострва (Kofman et al., 2017). Када погледамо руско – кримску историју, тада можемо констатовати следеће. Када се планира, а поготово реализује инвазија и анексија, знатно је лакше спровести је у дело уколико се ради о инвазијској сили која се сматра пријатељском и легитимном на простору где долази. Црноморска флота оружаних снага РФ је била историјски базирана на Криму, тако да је велики део становништва гледао ово особље оружаних снага РФ као домаће, односно као пријатељску снагу која је деценијама ту присутна. Никита Хрушчов и Врховни савет Савеза Совјетских Социјалистичких Република препотчинили су Крим под Владу Украјине, Совјетске Социјалистичке Републике 1954. године. С обзиром на то да су обе републике биле део Савеза Совјетских Социјалистичких Република, ово поступање је било углавном симболично и без практичне последице. Кримљани су имали мање економских разлога за страх или протест против анексије, јер приходи, плате и пензије су биле много веће у РФ него у Украјини. Светска банка је за 2014. годину, изнела податке да је бруто домаћи производ по глави становника у Украјини 2014. године износио 3.082,50 америчких долара, док је у РФ он износио 12.735,90 долара. Географски, политички и историјски идентитет и економске везе Крима са РФ били су структурални фактори који су смањили вероватноћу отпора народа и довели до олакшаног руског деловања на полуострву (Kofman et al., 2017). Констатација да ко контролише Крим, тај контролише читаво Црно море је можда једна од констатација са којом би требало завршити овај уводни део геостратегијског и геополитичког положаја Крима.

У данашњим условима ратне технике, величина и облик простора има велики значај у односима заснованим на сили, без обзира на сав напредак технике и претходних неколико деценија. Да данашњи начини сукоба лажним вестима, дезинформацијама, нису никаква новост у сукобима већ само прилагођене методе сада присутним технологијама, потврђује размишљање Сун Цуа који је саветовао генерале да припреме бојно поље користећи обману и маневар. Карл Хаусхофер[115] (*Karl Haushofer*) који је још 1913. године говорио о томе да је Немачкој увећање природе копнене моћи спајање са РФ (енг. *Heartland*) и одвајање од англосаксонаца, што када упоредимо са садашњим догађајима у Немачкој, постављамо питање да ли је и обустава *северног тока* потврда да никада није престала борба англосаксонаца у спречавању обједињавања *Heartlanda* (Марјановић и Мићовић, 2023). Моћ

[115] Карл Хаусхофер (*Karl Haushofer*, 1869–1946) оснивач немачке школе, генерал–мајор, написао је да геополитика мора постати географска савест државе, а већ 1913. године залагао се за трансконтиненталну руту без англосаксонских, која би повезивала Немачку са Русијом и Русију са Јапаном (Марјановић и Мићовић, 2023).

је та која доводи до опстанка, способности да наметнете своју вољу другима (вршите одвраћање), могућност да наређујете онима који имају мање моћи од вас односно да изнудите уступак од слабијих. Крајњи облик сукоба је рат. Борба за моћ постаје борба за ратну моћ, припрема за рат, што се неколико деценија уназад фантастично спроводи од стране офанзивних служби безбедности великих сила које ове облике наметања воље другима највише у „миру" остварују необавештајним активностима или познатије у западном делу планете као субверзивне и несубверзивне активности реализоване у форми *тајних акција*, *треће опције*, *прикривених операција*, *тајних операција, тихе опције, специјалних активности, неконвенционална дејства*, а на истоку под називом *активних мера, мера подршке* (Марјановић и Мићовић, 2023). Све је присутнији овај вид наметања копнене моћи. Двадесетих година XX века Влада Велике Британије није одобрила предлог Макиндер Хелфорда[116] (*Sir Halford John Mackinder*) ангажованог од британске обавештајне службе (енг. *Secret Intelligence Service*), да се формирањем малих држава Западно од Русије уситни геостратешки простор, седамдесет година касније ипак је дошло до територијалног распада Савеза Совјетских Социјалистичких Република управо по том основу, што је чињеница, а да ли је случајност или не остављамо за размишљање (Марјановић и Мићовић, 2023). Ангажовање РФ на Криму 2014. године представља ништа друго него покушај исправљања погрешних геополитичких одлука донесених у прошлости од стране руководства некадашњег Савеза Совјетских Социјалистичких Република на штету данашње РФ.

6.2.2. Активности Крима усмерене према Русији

Да бисмо разумели непосредне поводе за анексију Крима у новембру 2013. године, поменућемо неколико догађаја. Украјински председник Јанукович се није сложио са предлогом да одобри тј. потпише украјинско – европски споразум, споразум о прикључивању Европској унији. Јанукович се у овој ситуацији определио за зајам од РФ. Поред тога, предлагао је ближе везе између Украјине и РФ. Украјинском председнику је РФ тада понудила 15 милијарди долара за украјинску економију и споразум о отплати дуга између Украјине и РФ у вези са испорукама природног гаса, са још 2 милијарде долара које би добила Украјина. Одлуке Јануковича изазвале су низ грађанских немира у Украјини. Увече, 21. новембра 2013. године, Мустафа Најјем, Украјинац, новинар авганистанског

[116] Главни представници класичног учења о копненој моћи, Макиндер Хелфорд и Спајкман Николас кажу да доминација зависи од контроле једног дела Евроазије, односно, Хартленда или Римленда. Гледајући географски вектор националне одбране, чињеница је да је копно, као чинилац војне моћи, врло важно и као геостратешки простор. Колико су битне неке комуникације које прелазе преко неког копна, у неким околностима стратешки положај који условљава и начин приступа морима, карактеристике рељефа и друге карактеристике су изузетно битни сегменти који одређују геостратешки положај копна, државе (Марјановић и Мићовић, 2023). Дефинитивно утичу на *понашање* државе у односима које успоставља са другим земљама као и тих земаља како ће се односити према тој држави. За политичку моћ једне државе, геополитичари су копну увек придавали врло велики значај. Положај копна, величина и облик били су одлучујући у светској политици (Марјановић и Мићовић, 2023). Саму политичку моћ ови елементи не одређују директно, већ када се у одређеним контекстима сагледава утицај копна тада долазимо до пресудног значаја његовог утицаја на распоред ратних оружја и оруђа, затим испољавања утицаја у зависности од копна, какви ће бити планови одређене операције коју воде оружане снаге неке државе или економског утицаја (доступности логистике...) колико ће бити доступна дубина могућег маневра, што условљава копнена моћ. Без обзира на страховито велике технолошке напретке на планети (оружја, оруђа, стратегијских висококофистицираних ракета, стратегијских ваздухоплова, носача авиона, логистике…) који незаустављиво напредују све брже и брже, улога копнене моћи у геостратешким утицајима држава у наредном периоду неће опадати чак ни у ери дигиталних сукоба (Марјановић и Мићовић, 2023).

порекла, отворио је налог на Фејсбуку који је користио за информисање и позивање народа Украјине да се хитно окупе на тргу *Трг независности* (*Мајдан незалежности*) у Кијеву, Украјина, у знак протеста. Прво је било пар стотина окупљених, затим се тај број све више повећавао, а углавном се у почетку радило о студентима и младим људима. Протести су се дешавали углавном током дана, док је део демонстраната спавао на тргу, одбијајући да оде. Протести, који су касније названи *Евромајдан*, врло брзо су попримили политичке конотације и то са захтевима за оставку председника и Владе Украјине. Уверење демонстраната о распрострањености корупције од стране власти у Украјини и наводног кршења људских права је све више расло. Врхунац сукоба се догодио након бруталног растеравања демонстраната 20. новембра 2013. године, када се још више људи појавило на демонстрацијама. Током Евромајдана, протести су постајали све насилнији, и било је много сукоба између демонстраната и полиције. Затим је Парламент Украјине усвојио пакет закона против демонстраната и демонстрација уопште, што је изазвало још веће незадовољство међу демонстрантима. Од овог периода почињу да заузимају зграде Владе Украјине. У периоду од 18. до 20. фебруара настао је брутални сукоб са демонстрантима, када је коришћена бојева и гумена муниција. Снајперисти из Беркута, украјинско специјално обезбеђење, такође су били укључени, пуцајући на неистомишљенике. Овом приликом је убијено 18 полицајаца и 111 демонстраната (које су медији у Украјини називали *Небеска стотина*). С обзиром на велики притисак како са Запада тако и у самој Украјини, Јанукович је заједно са лидерима парламентарне опозиције потписао *Споразум о решавању политичке кризе у Украјини*, који је настао уз посредовање Европске уније и РФ. Врло брзо након потписивања споразума, Јанукович и други чланови Владе Украјине побегли су из државе. Демонстранти убрзо заузимају Јануковичево имање и владине зграде, а парламент Украјине уклања Јануковича са функције председника дана 21. фебруара када Олександар Турчинов, који је раније био шеф Службе безбедности Украјине и посланик Врховне раде, постаје вршилац дужности председника Украјине све док Петро Порошенко није положио заклетву као нови председник Украјине 7. јуна 2014. године (Bouwmeester, 2020). Наравно, илузорно је и помислити да је украјински новинар пореклом из Авганистана самостално дошао на идеју да позове народ преко Фејсбука на протесте и да надлежне службе безбедности нису биле у могућности да спрече такве позиве преко информационо – телекомуникационих система. Овде се јасно препознаје траг служби безбедности, страних служби у организовању и подршци, али не треба искључити ни ангажовање домаћих служби безбедности из Украјине.

Најбољи резултати у примени необавештајних активности се постижу управо комбиновањем већег броја активности доступних у избору необавештајних активности, а не само предузимањем једне активности. Руска Федерација је током 2014. године у Украјини користила прво дипломатско убеђивање како би покушала да оствари утицај на Украјину односно званичан став Кијева, да се не приближава Западу, не усклађује са Западом, где је наведено појачавано поруком, путем информационих активности великих размера. Паралелно са наведеним активностима, службе безбедности предузимају и друге мере, организацијом креирања лажних налога на друштвеним мрежама, наоружавањем сепаратиста и директним ангажовањем у сајбер активностима. Када говоримо о економској компоненти, економским активностима, тада може да се наведе као пример ситуација када је

фирма Гаспром удвостручила цене гаса у Украјини и пошто је Кијев оспорио цену гаса, прекинуто је снабдевање (Radin, Demus & Marcinek, 2020).

Компанија *Ukrtelecom* известила је да су наоружани људи упали у њене објекте на Криму 28. фебруара и да су нешто радили са оптичким кабловима. Прекиди који су тада наступили у информационо – телекомуникационим системима су наводно настали због тих активности. Активност руских националистичких хакера (које су реализоване пре овог догађаја, у Естонији 2007. године, затим и Грузији 2008. године) даље сугерише да су сајбер напади могли бити спроведени, али да до сајбер напада на Украјину наводно није дошло. У том периоду су отворени извори помињали како се *сајбер окршаји* догађају између просепаратистичких и проукрајинских интереса, међутим од јуна 2014. године није било доказа о значајним активностима које су утицале на кључне инфраструктурне или командно – контролне циљеве (Iasiello, 2015).

Сајбер напади на Украјину, ометање комуникационих система између Украјине и региона Крима, инвазија РФ на украјинску територију, била је праћена врстама сајбер напада које је међународна заједница већ приметила у ранијим сукобима и то у Естонији и Грузији. Поред напада дистрибуираног ускраћивања услуге и напада на веб – сајтове украјинске владе и други, хакери су заразили рачунаре кабинета украјинског премијера и неколико амбасада у Украјини злонамерним компјутерским црвом званим енг. *Snake* и хаковали мобилне телефоне дела украјинских званичника и политичара. Упоредо са сукобима оружаних снага РФ и Украјине на Криму, дошло је до размене напада у сајбер простору. Украјинска телекомуникациона компанија *Ukrtelecom* је известила да су непознате особе оштетиле оптички кабл који припада тој компанији, што представља нови елемент. Ова компанија је дала изјаву да је оштећење оптичког кабла директно угрозило комуникационе услуге које је пружала компанија *Ukrtelecom*. Оптички каблови су једна од физичких мета сајбер напада који могу узроковати прекид функционисања комуникационих услуга. Ометање функционисања ових каблова замагљује границу између сајбер напада и оружаних напада у физичком свету. Сајбер напади на Украјину наишли су на отпор у сајбер простору од стране украјинских хакерских група. Хакерска група коју предводи Еуген Докукин (*Eugene Dokukin*) је наводно претила да ће затворити приступ интернету на Криму током сукоба и рутински је одавала осетљиве податке из руског Министарства унутрашњих послова (Spiegel, 2017).

Усред напада на Украјину, група енг. *Lookingglass Cyber Threat Intelligence Group* је предложила истраживање о руском сајбер рату против Украјине под називом операција *Армагедон* – енг. *Operation Armageddon*: сајбер шпијунажа као стратешка компонента руског модерног ратовања. Према *Lookingglass*, напади су почели у тандему са одлуком Украјине да потпише Споразум о придруживању Европској унији 27. јуна 2013. године. Најранија временска ознака регистрованог малвера је била 26. јуна 2013. године. *Lookingglass* примећује да су се напади повећали након што је Јанукович побегао са свог имања 22. фебруара 2014. године и како су почеле најаве *антитерористичких операција* против проруских сепаратиста од стране привремене Владе Украјине. Од тог тренутка, па надаље напади су постали непрекидни. *Lookingglass* је ово наводно утврдио према уступљеним сазнањима Службе безбедности Украјине. Према сазнањима Службе безбедности Украјине, сајбер нападе су водили 16. (ранији назив Федерална агенција за Владине комуникације и информације) и 18. Центар Федералне службе безбедности РФ. Што се тиче тактика коришћених у операцији Армагедон, *Lookingglass* је известио о шаблону у нападима

почевши од распршивања циљаних енг. *spearphishing emails* стратегија које се нису користиле ни у Естонији ни у Грузији, постављајући нову форму напада који је развила РФ. Поред тога, неке корисне поруке током операције биле су у облику тројанца злонамерног софтвера[117], врсте малвера који има могућност контроле система даљински, преко удаљене мрежне везе. У случају Украјине, коришћен је систем манипулатора, а антивирусна индустрија га је класификовала као злонамерног. Ови злонамерни софтвери су коришћени за добијање информација током украјинско – руског сукоба. Сукоб на терену заједно са замахом сајбер напада и злонамерни софтвери можда су били разлог зашто су сајбер напади трајали током много година. То се показало ефикаснијим од напада у Естонији и Грузији. Добијање приступа информацијама о украјинским намерама се показало ефикаснијим од напада у Естонији и Грузији. Војска РФ, односно оружане снаге, могле су да доминирају у Украјини у својим доменима, укључујући копно, море, ваздух, свемир, и да имају највећу контролу над информацијама у простору. У Естонији је коришћен сајбер напад за ометање интернет активности, у Грузији је ова стратегија била коришћена паралелно са војном инвазијом; на крају су све ове стратегије кулминирале употребом сајбер ратовања ради добијања обавештајних података и утицаја на копнене украјинске војне снаге (Miniats, 2019).

Део поступака политичког руководства и других целина ангажованих од стране Украјине који су доприносили успеху РФ у спровођењу операције у Украјини се догодио у свега пар дана. Наиме, након победе Мајданске револуције у Кијеву, *прва грешка* руководства Украјине догодила се када је парламент Украјине наставио са националистичким пројектима, а након свргавања Јануковича. Критичан догађај се десио дана 23. фебруара 2014. године, када је парламент Украјине укинуо закон који је руском језику давао службени статус и заштиту. Колико се радило о погрешном потезу говори и противљење пољског министра спољних послова, Радослава Сикорског, који је интензивно подржавао одржавање протеста током Мајдана. Његов предлог је био да нова власт треба уместо тога да пожели етничким мањинама у Украјини добродошлицу и да ће бити део Украјине, заједно живети, што овим потезом није учинила. Јавност је овај поступак препознала као анти – руски акт. Касније изјаве званичника Украјине, па чак и министара су биле да је већина становника Крима стала на страну РФ управо због доживљаја Владе Украјине као националне владе. *Другу грешку* бисмо могли везати за догађај који се десио 24. фебруара 2014. године. Наиме, поменутог датума, Игор Мосијчук, лидер Десног сектора, крајње десничарске политичке партије и паравојне групе у Украјини, јавно је запретио да ће довести паравојну формацију бораца на Крим. Ову изјаву су једва дочекали медији на руском језику и затим је интензивно користили да би њеним преношењем ширили осећај непосредне опасности од националне Владе Украјине за оне који живе на Криму. Припадници полиције кримског Беркута поставили су контролне пунктове под образложењем одговора на потенцијалну десничарску претњу. Осећај непосредне опасности руског становништва и нејединство украјинске политичке елите су довели до позитивне климе и потврде за потребом за руском помоћи на Криму и давања легитимитета интервенције РФ пред домаћом публиком. *Трећа грешка* руководства Украјине коју можемо регистровати везано за Крим, догодила се 25. фебруара 2014. године. Поменутог дана је

[117] *Remote access Trojan*, енг. – тројанац за даљински приступ је злонамерни софтвер који нападач користи да добије пуне административне привилегије и даљинску контролу циљног рачунара.

министар унутрашњих послова Украјине донео одлуку о распуштању кримске полиције – Беркута, која се вратила у Севастопољ на Криму, након сузбијања протеста у Кијеву. Нагласак у овој одлуци је на томе да је прво јединица враћена назад на Крим, а затим је накнадно распуштена. Ово је било понижење за снаге безбедности, које су веровале да су само извршавале своје дужности по наређењу. Када су се ове снаге вратиле у Севастопољ, народ их је дочекао као хероје и одмах су добили руске пасоше од Москве. Овим пребегом на руску страну и раним обезбеђењем састава, помоћних јединица за реализацију операције од стране РФ, обезбеђен је недостатак људства и рад са лицима који познају терен, становништво и из те су популације. Након анексије Крима, део припадника ове јединице је учествовао и у Донбасу, региону источне Украјине, где су се борили на страни снага РФ, међутим, постоје сазнања да је ово била толико погрешна одлука да је део припадника јединице наставио да се бори са сепаратистима (Kofman et al., 2017). Да закључимо, предузимање исхитрених поступака припадника Владе Украјине и других структура Украјине у име владајуће политичке елите је довело до стварања страха и несигурности међу становништвом, као и до олакшавања реализације предвиђене операције од стране РФ.

Након већег броја терористичких напада изведених према руским грађанима и према цивилној, критичној инфраструктури, поносу председника Владимира Путина, Кримском мосту, 8. октобра 2022. године, служба безбедности РФ – Федерална служба безбедности објавила је да су за експлозију (*Слика 9*) на Кримском мосту одговорни Главни обавештајни директорат украјинског Министарства одбране и њен директор Кирило Буданов. Неколико дана касније, сам Владимир Путин је овај чин окарактерисао као саботажну активност коју је организовала Украјинска служба безбедности, па је 12. октобра 2022. године ухапшено 8 лица осумњичених за ово дело.

Слика 9. Сателитски снимак експлозије на Кримском мосту (познатом и као Керчки мост) 8. октобра 2022. године.
Извор: *slobodnaevropa.org*

6.2.3. Необавештајне активности Русије

Још једно паравојно ангажовање припадника РФ догодило се у марту 2014. године, када су припадници највероватније оружаних снага РФ, у необележеним униформама и борбеној опреми заузели владине и војне зграде на Криму. Наведени поступак паравојних активности РФ је створио могућност анексије дела територије и припајање РФ. Ове паравојне активности су умногоме подсећале на сличне догађаје заузимања главних административних зграда у Прагу, Чехословачка, које су релизовале снаге *Спетсназа* (у

августу 1968. године) како би се створили услови за инвазију Савеза Совјетских Социјалистичких Република ради гушења *Прашког пролећа*. Тајна природа операције је праћена са пропагандним и политичким активностима, где је порицање било основ када су се догађаји дешавали 2014. године (чак је и енг. *British Broadcasting Corporation* известио да су војници били украјински и козаци, док их је Путин називао снагама за самоодбрану), што је помогло РФ да много лакше доврши започету интервенцију, након чега је и сам Путин признао да су те снаге биле од РФ (Riehle, 2022).

Састав војне службе безбедности Главне управе (некада Главне обавештајне управе) који се бави(о) психолошким и дезинформационим операцијама је Јединица 54777. Ова јединица има своје потчињене целине ИнфоРос и Институт руске дијаспоре. ИнфоРос наводно шири лажне наративе завере и дезинформације које промовишу званичници Главне управе против САД. Јединица 54777 је ширила тајне поруке током анексије Крима, а спонзорисана је од стране РФ. У новембру 2018. године, јединица је слала лажне текстуалне поруке украјинским војницима у пограничном региону позивајући их на војну службу, током инцидента у Керчком мореузу. Претпоставља се да су писма упућена члановима Конгреса САД 2015. године од групе *Патриот Украјине*, о корумпираности оружаних снага Украјине, такође дошла из војне службе безбедности Главне управе, Јединице 54777. Врло често су ове и сличне операције тајног утицаја засноване на подацима које су прикупиле службе безбедности од разних извора података, промењених у корист РФ (Riehle, 2022).

Познато је да је генерал – пуковник Федералне службе безбедности Сергеј Бесада посетио Кијев, Украјину у периоду 21. и 22. фебруара 2014. године. Беседа је на челу Пете управе Федералне службе безбедности или тачније *Службе за оперативне информације и међународну комуникацију* која је надлежна за спровођење обавештајне активности усмерене на *блиско иностранство*, бивше совјетске републике. Федерална служба безбедности је себе видела као водећу службу безбедности РФ за суседне земље, међутим број припадника лица ангажованих од стране војне службе безбедности Главне управе (некада Главне обавештајне управе) у Украјини и на Криму временом се стално повећавао. Присуство је било углавном кроз формирање лажних компанија у Украјини, како би стекли дугорочни боравак у Украјини. Ова лица ангажована од стране војне службе безбедности Главне управе су углавном имала следеће задатке: да користе нестабилну ситуацију у Украјини да шире дезинформације, подстичу хаос и конфузију, понекад да изазивају инциденте. Утицај војне службе безбедности РФ Главне управе у Украјини је прогресивно растао. Сајбер нападе који подржавају РФ, када говоримо о активностима у Грузији, спроводили су руски активисти и криминалне организације. У везу са овим активностима доводи се и Руска пословна мрежа. Лица из РФ не само да су поседовала умерено софистицирану технологију, већ и контролу огромних онлајн ресурса. Обавештајне активности служби безбедности РФ у периоду пре анексије Крима ослањале су се на отворене изворе прикупљања података, као и на пресретање телекомуникација Украјине, њене инфраструктуре и циљаних сајбер операција. Већина телекомуникационих мрежа Украјине ослањала се на компаније РФ за производњу технологија и одржавање. Мреже у Украјини које је користила влада направљене су по узору на припреме које је вршио Комитет државне безбедности, односно Федерална служба безбедности као системе пресретања. Телекомуникационе компаније које су у већинском власништву РФ, попут Вимплекома и енг. *Mobile TeleSystems*, поседују значајан део украјинског тржишта мобилне телефоније што наводи на размишљање о сарадњи ових

приватних компанија са службама безбедности РФ. Поседовањем имовинских права у већини телекомуникационе инфраструктуре Украјине, РФ има много лакши начин да приступи телефонским и другим врстама комуникација. Интересантно је и слање кратких порука са текстом украјинским учесницима антируских демонстрација у Кијеву, следеће садржине: „Поштовани претплатниче, регистровани сте као учесник масовних нереда" (Bouwmeester, 2020, p. 318). Једни тумаче да се радило о облику микроциљања, који се не користи за политичке, већ за безбедносне разлоге, док су други проценили да се ради о безбедносним проценама. Службе безбедности РФ, највероватније Јединица 26165, такође су користиле операције сајбер шпијунаже циљајући различите сегменте украјинског друштва. Операција *Армагедон* почела је средином 2013. године, где су мете били украјинске владине институције, јединице за спровођење закона, војни врх, новинари и др. Сам почетак операције се временски подудара са периодом када су Европска унија и Украјина започеле преговоре за Споразум о придруживању Европској унији, што је РФ сматрала претњом за РФ. У новембру 2013. године, по избијању антивладиних протеста у Кијеву, напредни малвер по имену Змија (енг. *Snake*) заразио је канцеларије премијера Украјине и неколико амбасада Украјине у иностранству. Активности ове врсте су указивале на умешаност тајних служби безбедности РФ, као што је Јединица 26165. Малвер је стално ажуриран, а био је прилагођен софистицираним, елитним циљевима за употребу у операцијама енг. *phishing* и *напад китолова*. Идејни творац операције је осмислио исту да би се избегло откривање и приписивање, а напредне технике шпијунаже су пружале властима РФ увид у стратешко размишљање Украјине. РФ је користила циљане новинаре да би боље разумела јавност мишљења, да се идентификују дисиденти и да се створе канали за ширење дезинформација и поруке које су у интересу РФ. Телевизија, посебно прва три канала у РФ, под контролом су државе и често функционишу као гласноговорник највише власти у РФ. Пре анексије Крима, РФ је много улагала у анализирање и утицај на онлајн медијске платформе. Стварну ефикасност руских информационих операција понекад је тешко утврдити, јер су ове операције, укључујући њихове сајбер операције, осмишљене тако да се могу порећи. Хакерске групе, понекад независне, али често повезане са службама безбедности као што су АПТ28 (енг. *Fancy Bear*) и АПТ29 (енг. *Cozy Bear*), пружају властима РФ тајне опције за стицање података и докумената који се могу после користити у кампањама дезинформисања и информативним операцијама (Bouwmeester, 2020).

Руска Федерација има супериорност на локалном нивоу, а она се изражава кроз огромну способност у људству и више врста високо оспособљених оружаних снага. Руска Федерација је у могућности да у кратком временском периоду распореди огромне оружане снаге без упозорења и може да настави са појачањима како би наставила започету мисију. Упркос економским реформама, али и демографском паду, као и оперативним обавезама, ограничили би способност РФ да одржи оружане сукобе у дужем временском периоду, мада би РФ имала могућност примене економских активности према циљаним државама, што би по исте имало несагледиве последице, можда веће и од војних ангажовања. Ове способности осликавају негативну ситуацију, војну ситуацију за Северноатлантски савез. С обзиром на малу вероватноћу да ће РФ употребити конвенционалну силу против Северноатлантског савеза, одлучност и одвраћање Северноатлантског савеза биће додатно појачано ако може да дође до консензуса о томе шта чинити и како да се одговори на нападе у сајбер домену и електромагнетном спектру (Kristek, 2017).

Информациона операција је претходила, пратила и наставила се након војне операције РФ на Криму. Медији РФ су увек одржавали извесно извештавање дешавања на Криму за домаћу јавност, али се то интензивирало како су сукоби између провладиних снага и демонстраната у Кијеву постали насилнији. Протестни покрет на Мајдану, од новембра 2013. године, покренуо је руску манипулацију информацијама усмерених на своје грађане, упозоравајући их на опасности ближих веза са Европском унијом. Постојећа владина гласила, као нпр. *РИА Новости* и *Глас Русије*, обједињени су у *Русија Данас*. Руска Федерација искључила је девет украјинских телевизијских канала дана 9. марта 2014. године, остављајући приступ само руским каналима. Телевизијски канали из Украјине су остали доступни само преко сателитских пријемника. Након пада владе Јануковича почетком 2014. године, руска реторика о догађајима у Украјини постала је оштрија. Руски медији су износили сазнања о привременој Влади Украјине и протесту покрета који га је довео као о *фашистичкој хунти*. Из свега што је предузимано у информационој операцији РФ приликом анексије Крима, могу се извести три циља: дискредитација нове власти у Украјини (*фашистичке снаге*), затим наглашавање тешке опасности за руски народ у Украјини и приказ широке подршке повратку Крима у безбедну средину, својој кући, у РФ. Током истраживања ове проблематике можемо резимирати (види *Табелу 16*) стратешке опште теме, теме о Влади Украјине и о улози западних држава које је користила РФ (Kofman et al., 2017).

Табела 16. Теме руске стратешке комуникације о Криму.

Опште теме	О Влади Украјине	О улози западних држава
• Кримска земља историјски је припадала Русији. • Трансфер Крима Украјини је 1954. године историјска грешка од совјетског периода. • Етнички Руси и сво становништво које говори руски на Криму били су под неминовним ултранационалистичким претњама. • Русија није била укључена у догађаје на Криму. • Референдум од 16. марта о независности био легитиман, демонстрирајући вољу народа Крима. • Украјински војници добровољно одустали, своје оружје и оданост дали су РФ.	• Украјинска влада делује у интересу САД и друге стране силе. • Мајдан покрет је прегажен (насилно) од ултранационалиста. • Председник Украјине је свргнут у нелегитимном државном удару (француски *coup d'état* – противуставно) подржан од Запада. • Проевропско становништво у Украјини су идеолошки потомци присталица нациста и фашиста.	• Западне државе, а посебно САД су језгро оркестра догађајима у Украјини. • Примарна мотивација САД је експанзија Северноатлантског уговора организације и који садржи РФ. • САД су притискајући Европу да уведе санкције против РФ која јесте покретачка снага, а води се политика задржавања против Москве. • РФ својом политиком није одступила од претходне, Западне интервенције, мењају границе и стварају нове политичке ентитете, нпр. као што је Косово и Метохија.

Извор: Kofman et al., 2017, p. 14.

Дана 26. фебруара 2014. године, РФ је почела агресивну промоцију своје поруке за промену режима у Украјини да је била нелегитимна. Ова промоција је реализована један дан пре војног преузимања владиних зграда на Криму од стране РФ. Ову поруку је пренело неколико познатих руских личности и припадника елите, на пример, Сергеј Миронов, лидер руске политичке партије, на каналу вести Русија 24, 25. и Рамзан Кадиров, шеф Чеченске Републике, на каналу *Life News*, тврдећи да су Руси угрожени на Криму и тражећи заштиту РФ од националиста и фашиста из Кијева. Председник РФ Владимир Путин је на

конференцији за новинаре 4. марта рекао да његова земља нема планове за анексију Крима и да на Криму није било војника РФ. Радило се о радњама где се вршило јавно порицање, а ради тајног преузимања. Путин је даље тврдио да РФ не планира инвазију на Украјину, али да би држава могла бити приморана интервенисати уколико се положај Руса у Украјини погорша. С обзиром на велики број оружаних снага РФ распоређених у близини украјинске границе, председник је тврдио да су војне вежбе на Украјинској граници одавно планиране. Кампања на Криму да се супротстави покрету Мајдан је један од примера организовања народа, где су антимајдански активисти под називом *Стоп Мајдан* организовали разне капмање (нпр. слање порука публици преко шатора са натписима *не екстремизам* и *не страној интервенцији*). Поруке приказују протесте на Мајдану као организоване из иностранства и учесника Мајдана као фашистичког екстремисту (Kofman et al., 2017).

Први или међу првим званичнијим сајбер нападима у Украјини су се догодили у октобру 2014. године. Тада су нападима успели да онемогуће електронски систем за састављање резултата избора за парламент Украјине, па је било неопходно ручно пребројавање гласачких листића и одлагање извештавања о резултатима. Хакерска група енг. *CyberBerkut* је преузела заслуге за овај напад, под оправдањем да се радило о бунту, протесту против владајућег режима. Две најпопуларније платформе друштвених медија у Украјини, *VKontakte*[118] и *Odnoklassniki*, биле су хостоване на руским серверима, па су тако власти РФ биле у могућности да блокирају странице које су позивале на протесте на Мајдану и да деле личне податке о онима који су им одговарали. Након ескалације насиља на терену, *VKontakte* и *Odnoklassniki* су пружили алат за прикупљање прилога и регрутовање у РФ за групе као што су *АнтиМаидан*, *Народна милиција Донбаса* и *Фонд за помоћ Новоросији*. Значајан елемент руске информативне кампање било је потенцирање термина *Novorossiya*[119]. Употреба овог термина изазвала је забринутост на Западу, јер је то имплицирало да је РФ намеравала да распарча Украјину. Наставак политике у овом правцу је био и формирање покрета, партије Новоросија[120]. У мају 2014. године самопроглашени Луганск и Доњецке републике су формирале конфедерацију Новоросије и Уједињене оружане снаге Новоросије. За РФ је ово био информативни механизам, али је убрзо напуштен. Москва је настојала да извуче политички ентитет из прошлости са сопственом групом идеолошких бораца и вођа који су настојали да искористе баук Новоросије као полугу за ценкање са Украјинском власти. Украјина је забранила руско емитовање у држави. Сепаратисти које подржава РФ морали су да прибегну употреби силе, јер информациона операција тада није успела да окупи староседеоце на устанак који би могао да захвати Источну Украјину. Далеко од тога да је информациона операција постала главни елемент сукоба, она је све време остала споредни вид сукоба (Kofman et al., 2017).

---

[118] Павел Дуров, оснивач *VKontakte*, продао је свој удео и побегао из РФ у априлу 2014. године (Kofman et al., 2017).

[119] Путин је поменуо овај концепт у медијима када је одржао говор 17. априла 2014. године, подсећајући „да су источна и јужна Украјина, од Донбаса до Одесе, укључујући и регионе који претежно говоре руски, били историјски делови Руског царства" (Kofman et al., 2017, p. 51).

[120] Павел Губарев „крајње десничарски сепаратистички лидер, вођа и један од тзв. гувернера, који су основали партију Новоросија у мају 2014. године. Новоросија се такође залагала за правду и историјску легитимност акција сепаратиста у очима руског народа" (Kofman et al., 2017, p. 52).

Најактивније су биле ангажоване службе безбедности РФ, Федерална служба безбедности и војна служба безбедности Главна управа (раније Главна обавештајна управа) из РФ у Украјини и на Криму. Активност поменутих служби безбедности РФ у Украјини пре анексије Крима се огледала углавном у циљаним убиствима одређених, наводно опасних опозиционих лидера. Током заузимања Крима, следеће структуре су биле ангажоване: *Spetsnaz* – Главна управа, заједно са јединицама 810. независне морнаричке пешадијске бригаде Црноморске флоте заузела је важне тачке инфраструктуре. Отприлике око 50 припадника *Spetsnaz* – Главна управа, обучени до непрепознатљивости и претварајући се да су локална полиција, заузели су и окупирали на Криму зграду парламента дана 27. фебруара 2014. године. Тек након тога су били подржани од ваздушно – десантних трупа РФ. Издато је наређење да ове снаге не отварају ватру осим ако није изазвана и баш неопходна. Један поступак дела официра који су били распоређени на Крим заврђује посебну пажњу (ради спречавања проливања крви, беспотребне), а ради се о официрима оружаних снага РФ који су преговарали са својим колегама из оружаних снага Украјине у блокираним војним базама како би разрешили тензије и понудили повлашћене услове за предају или понуду да се придруже оружаним снагама РФ. Војна служба безбедности РФ, Главна управа (раније Главна обавештајна управа) је такође организовала добровољце за локалну самоодбрану, који су повучени из локалних организованих криминалних група и појединци лојални новом проруском кримском премијеру Сергеју Аксјонову. Овде региструјемо састав који није био толико професионалан у извршавању обавеза, али су били веома видљиви, са уочљивим наоружањем, то су били људи који чувају владине зграде, лица запослена у истим и врло су блиско сарађивали са проруским групама као што су *Ноћни вукови* и приватним војним компанијама као што је *Вагнер* (Bouwmeester, 2020).

Слика 10. Председник РФ Владимир Путин са *Ноћним вуковима*, Крим 2019. године.
Извор: Bouwmeester, 2020, p. 358.

Војна служба безбедности Главна управа (некада Главна обавештајна управа) је такође блиско сарађивала или боље рећи да су одређене групе биле ангажоване од стране војне службе безбедности Главне управе (некада Главне обавештајне управе), а радило се о плаћеницима из приватног војног обезбеђења компаније, као што је *Вагнер* и другим паравојним и насилним групама попут *Ноћних Вукова* (*Слика 10*), мотоциклистичке групе на чијем челу се налази Александр Залдостанов са надимком *Хирург*. Квалитет ових плаћеника

у војном смислу је врло дискутабилан и на ниском нивоу. Ради се о ентузијастима и идеалистима, који су савршено покриће за трупе оружаних снага РФ чије је присуство ускраћено. Оно за шта су изузетно оспособљени, то је изазивање хаоса и конфузије, грађанских немира и непослушности. Припадници оружаних снага Украјине постали су дезоријентисани, изоловани, што је довело до конфузије и неодлучности. Међутим, локална полиција и јединица Беркут на Криму су скоро одмах прешли на страну оружаних снага РФ. За овај период се коментарише да се ради о новом поглављу у раду са агентима од утицаја (Bouwmeester, 2020).

Можемо констатовати да је потреба за допирањем до становништва источне Украјине како би им била приказана потреба за јасном политиком украјинске владе велика. Могућност спровођења одговарајуће анализе становништва одређене државе или територије је основ за планирање информационе операције. Украјинска влада која се плаши инвазије РФ имала је стациониран велики број трупа на граници, дакле вршећи значајан психолошки притисак, али није наређен оружани отпор на Криму. Међутим, неуспех да повуче украјинску војну опрему и издаја трупа дале су трупама оружаних снага РФ на Криму превагу да изврше психолошки притисак и заузму Крим. Неспремној Украјини је било веома тешко да се супротстави добро припремљеној операцији РФ на Криму на ефикасан начин. Дезинформације великих размера које је ширила РФ погоршале су ситуацију и довеле до преоптерећења супротстављених информација за локално становништво и саму Владу Украјине. Све време РФ је доследно приказивала Владу Украјине као „крајње десничарске нацисте" што је као епилог имало одвајање дела становништва од Владе Украјине. Главни успех у овом делу активности РФ препознаје у веровању људи и способности да предвиђање њихових акција буде кључно за успех информационе операције РФ с једне стране, и наравно супротно на другој страни, неуспех Украјине. Дуго је преовлађујући став у многим западним владама био да је цео регион био проруски или барем просепаратистички. У овим сукобима, неформалне структуре моћи, пословне мреже, оцењене су као високо утицајне (Bērziņš et al., 2015).

6.3. СТУДИЈА СЛУЧАЈА: УКРАЈИНА

Студија случаја је везана за догађаје првенствено везане за период 2017. године у Украјини и идентификацији извора неразумевања РФ и Украјине, као и предузиманих необавештајних активности великог броја служби безбедности на овим просторима.

6.3.1. Извор неразумевања Русије и Украјине

Ради схватања историјске позадине и хронологије сукоба у Украјини, важни су догађаји, време и разумевање контекста у коме се сукоб дешавао. Распадом Савеза Совјетских Социјалистичких Република, Украјина је стекла независност, мада је РФ и даље покушавала да задржи одређени утицај над бившим републикама Савеза Совјетских Социјалистичких Република. Интересантно је да односе између РФ и Украјине карактерише велики број спорова, почев од наранџасте револуције током избора 2004. године у Украјини, па око испоруке природног гаса, затим да је Украјина прво започела своје приближавање Европској унији споразумом о придруживању, али се касније ипак окренула поново према РФ. Враћање у „загрљај" РФ, државе Запада нису благонаклоно гледале и врло брзо су видљиви и резултати овог заокрета, убрзава се одлука за Евромајданске протесте што доводи

до одласка председника Украјине Јануковича. Поред протеста који су се догађали у Украјини, у исто време паралелно са протестима су реализовани напади дистрибуираног ускраћивања услуге и оштећење веб страница на украјинским сајтовима. Приликом вршења анексије Крима, највероватније од стране РФ је дошло до још једног повећања сајбер – активности у Украјини и РФ. Регистрована су и два скока у виду два сајбер напада на електроенергетску мрежу Украјине (Baezner, 2018).

Табела 17. Хронологија догађаја који су битни ради разумевања сукоба РФ и Украјине.

Датум	Догађај
05.12.1994	Украјина постаје чланица Споразума о нешириењу нуклеарног оружја враћањем свог нуклеарног оружја РФ. У Будимпештанском меморандуму о безбедносним гаранцијама, Украјина се уверава да њен територијални интегритет и политичку независност неће угрозити РФ.
03.2005 – 01.2006	У марту 2005. РФ оптужује Украјину да преусмерава природни гас за земље Европске уније и да не плаћа порез на снабдевање природним гасом. РФ је 1. јануара 2006. прекинула испоруке природног гаса Украјини, што има ефекта на европске државе које зависе од снабдевања гасом који пролази кроз Украјину.
08.2008	Руска Федерација врши инвазију на Грузију након сукоба између пророских побуњеника и грузијских оружаних снага. Оружане снаге РФ користе комбинацију кинетичких способности и сајбер напада на веб – странице грузијских институција.
12.2011	Након Путинове победе на парламентарним изборима, опозиција организује демонстрације у знак протеста против изборних резултата. Током протеста, руске оружане снаге користе аутоматизоване нападе дистрибуираног ускраћивања услуге да ометају медије и странице друштвених медија како би зауставиле дискусије о изборима.
11.2013	Украјински председник Јанукович одбацује споразум о придруживању са Европском унијом. Проевропски покрет Евромајдан накнадно организује протесте, али је насилно потиснут. У исто време, веб – сајтови украјинских институција су на мети напада дистрибуираног ускраћивања услуге.
18 – 21.02.2014	Насиље над демонстрантима се појачава што је изазвало смрт неколико демонстраната. Напади дистрибуираног ускраћивања услуге се настављају на украјинске веб – странице и на мобилне телефоне украјинских посланика. Украјински парламент пристаје на промену уставног закона и враћање на оквире пре устава из 2004. године.
22.02.2014	Украјински председник Јанукович бежи у РФ. Украјински парламент бира Александра Турчинова за вршиоца дужности председника до планираних председничких избора 25. маја 2014.
27 – 28.02.2014	Пророске групе организују демонстрације у разним градовима Украјине, док неуниформисани војници заузимају аеродроме и друге стратешке локације на Криму. Они су прекинули комуникацију Крима са спољним светом у нападу на украјинску телекомуникациону инфраструктуру и манипулисали њеним оптичким кабловима.
01.03.2014	Парламент РФ одобрава употребу силе против Украјине.
02.03.2014	Руске трупе улазе на Крим.
07 – 14.03.2014	Различите руске веб – странице су на мети напада дистрибуираног ускраћивања услуге у знак одмазде за инвазију.
16.03.2014	Референдум о припајању Крима РФ спроводи становништво Крима.
16 – 18.03.2014	Пријављени су различити напади дистрибуираног ускраћивања услуге на украјинске и руске веб – странице.
17.03.2014	САД и европске државе се договарају о првој рунди санкција РФ.
18.03.2014	Председник Путин потписује нацрт закона о анексији Крима.
04.2014	Почиње у источном украјинском региону Донбаса између пророских сепаратиста и

Датум	Догађај
	украјинских оружаних снага. Истовремено, сајбер напади на руске и украјинске веб – странице се настављају. САД и европске државе се договарају о другој рунди санкција РФ.
24.05.2014	Проруска хакер група по имену енг. *Cyber Berkut* хакује сервере Централне изборне комисије и инфицира изборне мреже малвером. Украјински тим за реаговање на сајбер хитне случајеве успева да уклони малвер са мреже на време пред изборе.
25.05.2014	Петро Порошенко је изабран за новог председника Украјине.
20.06.2014	Председник Порошенко прогласио је седмодневни прекид ватре да би проруски сепаратисти положили оружје. Сајбер напади проруских хакерских група такође престају током овог примирја.
17.07.2014	На лету број 17 Малезијског авиопревозника (енг. *Malaysia Airlines flight 17*) из Амстердама за Куала Лумпур оборили су борци у Украјини, што је резултирало са око 300 мртвих путника.
07.2014	САД и европске државе проширују своје санкције РФ.
06.08.2014	Руска Федерација уводи ембарго на пољопривредна добра из држава које су увеле санкције РФ.
05.09.2014	Зараћене стране договарају се о прекиду ватре у региону Донбаса у Протоколу из Минска. Договор о прекиду ватре пропада у јануару 2015.
25.10.2014	Порошенкова политичка партија осваја већину на украјинским парламентарним изборима. Током кампање примећено је неколико напада дистрибуираног ускраћивања услуге и хаковања на украјинске институције.
11.2014	Руска Федерација ствара нову војну јединицу специфичну за сајбер ратовање на Криму.
12.2014	Објављена је нова руска војна доктрина, која такође детаљно описује концепт информационог ратовања.
12.02.2015	Зараћене стране потписују нови споразум о прекиду ватре, Протокол Минск II. Протокол се крши убрзо након потписивања.
03.2015	Европска унија ствара енг. *StratCom Task Force*, чији је циљ да идентификује и исправи дезинформације које долазе из медија на руском језику.
23.12.2015	Сајбер напад на украјинску електроенергетску мрежу оставља око 250.000 становника без струје на неколико сати.
09.2016	Међународна истрага извештава да је лет број 17 Малезијског авиопревозника оборен ракетом БУК совјетске производње лансираном из региона Донбаса.
25.10.2016	Украјинска хакерска група дошла је до хакованих мејлова кључног саветника Владимира Путина, Владислава Суркова. Његови мејлови откривају да је редовно комуницирао са лидерима проруских сепаратиста у Украјини.
16.11.2016	Руска Федерација се повлачи из Међународног кривичног суда.
01.12.2016	Украјина тестира ракете у Црном мору, западно од Крима, и оптужена је за нарушавање руских територијалних вода.
06 – 14.12.2016	Неколико сајбер напада циља на украјинске банке, државне агенције и министарства.
17.12.2016	У региону Кијева нестаје струје на сат времена након новог сајбер напада на украјинску електроенергетску мрежу.
29.01.2017	У источној Украјини сукоби између украјинских снага и сепаратистичких група се интензивирају након неколико мирнијих месеци.

Извор: Baezner, 2018, p. 7–9.

У студији случаја утицаја који је РФ испољавала према Украјини, као и мера које су предузимане, изведене су кључне констатације (*Табела 17*) испољавања необавештајних активности служби безбедности и других активности предузиманих од ових држава ради остваривања својих националних циљева. Лидери РФ свој утицај у Украјини доживљавају као кључан за опстанак РФ и то кроз одржавање контроле око безбедносне политике у

бившим државама Савеза Совјетских Социјалистичких Република. Крим са својим геостратешким положајем представља важну локацију заједно са лучким градом, Севастопољом, који обезбеђује тампон против продора Запада. Како је проруска украјинска влада пропала, почетком 2014. године и интереси нове владе прешли су тј. окренули се према Западу. Руска Федерација је постала сива зона за предузимање операција као један прикладан и ефикасан метод за постизање спољнополитичких интереса, циљева уз избегавање директне конфронтације са државама чланицама Североатлантског савеза. Следећи су били интереси и циљеви РФ у Украјини, да сачува проруски статус дуж својих граница и спречи револуционарно понашање, затим да поврати позицију РФ као глобалне силе, па да спречи Североатлантски савез и Европску унију да се приближавају границама РФ, стварање одрживе Евроазијске уније која укључује Украјину, и слабљење Североатлантског савеза. Предузимањем непријатељских мера, РФ је омогућила постизање више циљева, али првенствено повећањем глобалног статуса РФ. Почетком 2019. године изгледало је да непријатељско понашање РФ може ненамерно да убрза окретање Украјине све више према Западу (Connable et al., 2020).

6.3.2. Необавештајне активности Русије

Када говоримо о Украјини која је искусила сајбер нападе и покушаје напада у мреже њене владе и електроенергетске инфраструктуре, 2015. године, Служба безбедности Украјине пријавила је напад РФ путем електронске поште на компјутерске системе у Украјини. Исте године поновни упади у мрежу изазвали су непланиране прекиде у три украјинска електродистрибутивна предузећа, што је утицало на приближно 225.000 купаца, а малвер је пронађен и у другим украјинским компанијама у критичним инфраструктурним секторима. Верује се да иза напада стоји тим за компјутерски упад војне службе безбедности РФ, Главне управе, познат на Западу под именом енг. *Voodoo Bear*. Овај тим је реализовао субверзивне активности широм Украјине, уништавајући стотине рачунара у медијским компанијама, бришући или трајно закључавајући терабајте података на државним рачунарима и паралисањем инфраструктуре, укључујући систем за продају карата за железницу у Украјини. Операције *Voodoo Bear* су у складу са ентитетом који подржава руске војне и политичке циљеве путем циљаних операција шпијунаже и саботаже. Само годину дана касније, у децембру 2016. године, напади малвера порекла из РФ, су усмерени на електричне мреже у Украјини, током којих се електрична станица у близини Кијева искључила, остављајући северни део престонице без струје. Један од најозбиљнијих сајбер напада РФ на Украјину догодио се 2017. године, када је вирус *NotPetia* пуштен у компјутерским мрежама Украјине. Дана 27. јуна 2017. године спроведена је серија сајбер напада на веб – странице организација из Украјине, и то: банке, владина министарства, новине, електропривреде и државна предузећа као што су Међународни аеродром Бориспил, Укртелеком, Укрпошта (поштанска служба), Државна штедионица Украјине и Украјинске железнице. Праћење радијације у нуклеарној електрани Чернобил је било искључено сајбер нападом. Малвер је преписао и трајно оштетио датотеке на зараженим рачунарима. Напади *NotPetia* оштетили су више од украјинских циљева, јер вирус је такође изазвао озбиљне поремећаје у раду данске бродске линије *Maersk*, заједно са другим вероватно ненамерним циљевима широм света. У јулу 2018. године, служба безбедности Украјине тврдила је да је осујетила напад на мрежну опрему која припада фабрици хлора *LLC Aulska* у источној

Украјини. Ових неколико примера наводимо као манифестацију економских активности служби безбедности, односно напада *индустријске саботаже*, необавештајних активности (Riehle, 2022).

Девет непријатељских мера РФ примењиваних против Украјине почевши од кризе 2014. године наводимо као најкарактеристичније и битне, а неке од њих су настављене почетком 2019. године. Ради се о „политичком припајању Кримског полуострва, затим пружању директне и индиректне војне подршке сепаратистима на истоку Украјине, па коришћење нерегуларних паравојних снага на Криму и у источној Украјини, као и извођење хитних војних вежби и јачање снага дуж украјинске границе, па искоришћавање сународника, укључивање у медијску манипулацију, пруску јавну дипломатију и сајбер нападе, тражење правног оправдања за непријатељске мере, повећање цена енергената да би се присилила Влада Украјине, и доношење економских мера, ембарга и обустављање слободне трговине" (Connable et al., 2020, p. 43). Утицај РФ на Украјину у овом периоду је спровођен кроз непријатељске мере, али у нејасним фазама, где су врло често мешане тајне, затим тајне и отворене војне и акције служби безбедности са низом информација, дипломатских и економских активности (Connable et al., 2020). Можемо констатовати да су овакве активности у Украјини довеле до губитка историјски важног савезника који је служио за заштиту државе на непосредној граници РФ.

Табела 18. Информациона операција – са прегледом руских порука током кампања у Украјини; селектовани су детаљи о садржају руских порука, алати или механизми који су се користили за пропаганду и друге значајне аспекте компоненти информационог ратовања током ових операција.

I ГЛАВНЕ ТЕМЕ
1. Поруке специфичне за Крим
• Земља је историјски припадала Русији. • Аквизиција Крима од стране Украјине 1954. године била је историјска грешка. • Кампања енг. *Krym Nash* (*Крим је наш* – рус. *Крым Наш*). • Етнички Руси и све становништво Крима које говори руски су под озбиљном ултра – националистичком претњом. • Русија ни на који начин није била умешана у догађаје на Криму; референдум је покренуо и спровео народ Крима. • Кримски војници су добровољно предали оружје и обећали њихову оданост Русији. • Светле слике потлаченог *руског становништва*, *Беркут* хероји, *учтиви зелени људи*.
2. Мајдански устанак
• Запад је оркестрирао устанак. • Већина демонстраната су били насилни антируски ултранационалисти. • Јанукович је побегао као резултат насилног државног удара против његове владе; нова Влада Украјине је нелегитимна. • Потписивање споразума о придруживању издало би односе Украјине са Русијом. • Потписивање споразума о придруживању имало би разорне последице за Украјину. • У страху за своје животе стотине хиљада Руса је побегло из Украјине. • Мајдан револуција је фашистичка, националистичка и антисемитска.
3. Слабљење Украјине као државе
• Украјина је економски пропала држава. • Украјина је вештачка држава која није постојала пре 1991. године. • Украјински језик није ништа друго до комбинација руског и пољског. • Украјина нема одрживу будућност без руских субвенција и покровитељства.
4. Омаловажавање Украјине као државе
• Украјинска влада делује у интересу Уједињених нација и друге државе, стране силе. • Украјинску владу преплављују насилни ултранационалисти. • Проевропско становништво Украјине идеолошки су потомци присталица нациста и фашиста.

5. Величање Русије
• Руска историја и традиција захтевају сопствени Руски пут – јединствен приступ људским правима и развојној путањи. • Пад Совјетског Савеза био је катастрофа глобалних размера. • Русија представља центар словенског/православног света. • Русија је главни борац против фашизма. • Русија се залаже за истину и против светске доминације и хегемоније САД. • Русија сноси одговорност за заштиту руске дијаспоре (*Russkiy Mir*) свуда. • Русија је коначно устала са колена и смогла снаге да се одупре похлепној и себичној политици Запада.
6. Јачање Русије
• Ажурирана војна доктрина (2010). • Најава нове Војне доктрине (јануар 2015).
7. Идентификовање унутрашњих непријатеља
• Опозиција је издаја. • Потражите *петУ колону*.
8. Слабљење Запада
• Морал западног света суштински се разликује од морала руског народа. • Европске земље у великој мери зависе од Русије за гас и увозно – извозне односе. • Време западне цивилизације је декадентно и дошло је до краја: изнутра труле. • Западне државе и САД су једноставно незадовољне и плаше се растуће моћи РФ, па отуда и њихова реакција на њене акције и њихове изолационистичке политике.
9. Омаловажавање Запада
• Западне државе, а посебно САД, су језгро оркестратори догађаја у Украјини. • Ширење Североатлантског савеза и ограничавање способности РФ су главне мотивације за деловање већине држава у Европској унији, САД, Канаде и Аустралије. • САД врше притисак на европске државе да наставе политике санкција против Русије.
II ГЛАВНИ АЛАТИ (МЕХАНИЗМИ)
1. Медијски канали
• Руско контролисани телевизијски канали у РФ, Украјини и на Западу – новински извештаји, – *talk shows*, енг. – разговорне емисије, – документарни филмови и *специјални извештаји*. • Интернет вести са седиштем у РФ, Украјини и на Западу. • Блогови и заједнице друштвених медија. • Штампајте новине са седиштем у РФ, Украјини и на Западу. • Дељење летака и штампаног материјала на догађајима. • Билборди током референдума на Криму.
2. Говорници
• Владимир Путин, Сергеј Лавров и други руски политичари и специјалисти из одређене области. • Украјински политичари и специјалисти из одређених области. • Проруске организације и политичке партије у Украјини. • Западни политичари и стручњаци из Европе и САД. • Локални лидери са протеста. • Редовни грађани и *професионални* учесници протеста. • Познате личности и памет – интелигенција.
3. Општи тон и методе
• Подривање легитимитета Владе Украјине. • Стварање осећаја угрожености и хитног случаја. • Манипулисање историјским чињеницама и памћењем. • Снажан емоционални нагласак, у комбинацији са манипулацијом чињеница, дезинформације и полуистине. • Претерано поједностављивање стварности – *једна велика линија поделе у Украјини*. • Стварање двосмислености.
4. Угњетавање алтернативних погледа
• Готово апсолутна контрола медија у РФ. • Узнемиравање новинара током догађаја у Украјини. • *Троловање* алтернативних медија или мишљења.

Извор: Kofman et al., 2017, p. 79–83.

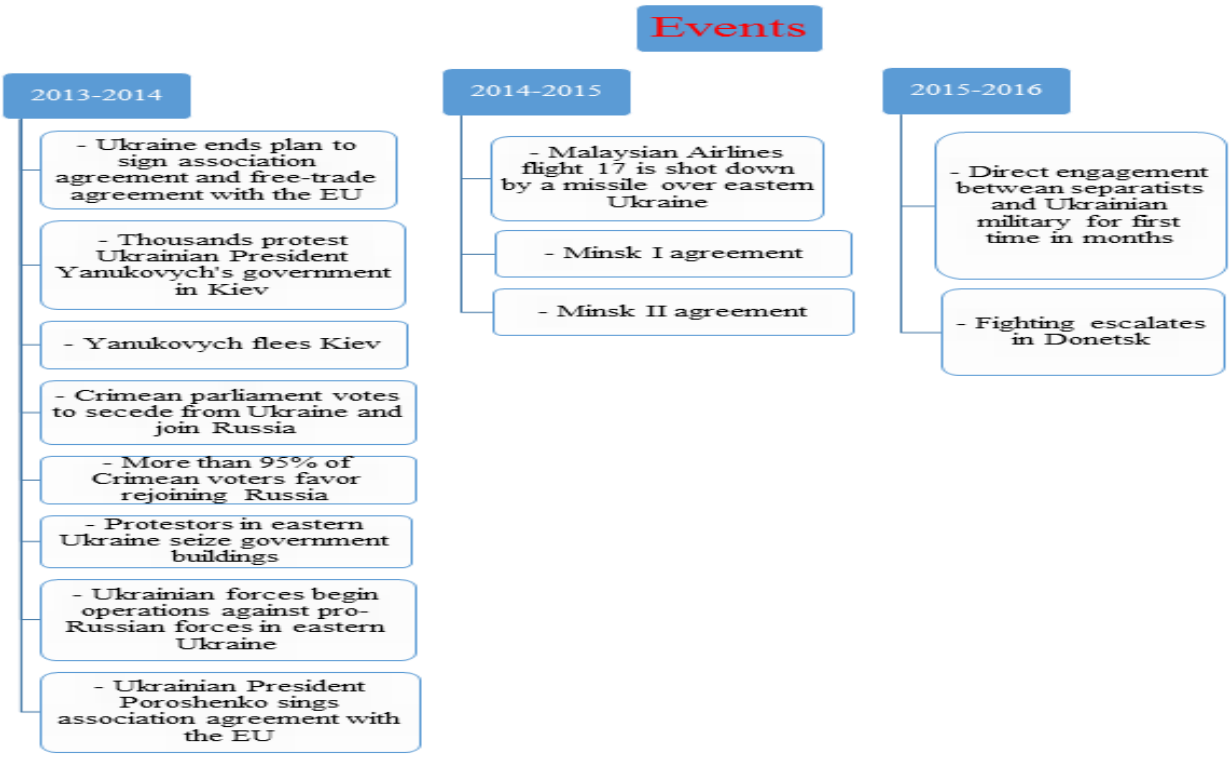
Увидом у ову табелу (*Табела 18*) видимо груписан на једном месту већи део главних тема које су коришћене у информационим операцијама РФ почев од порука специфичних за Крим до омаловажавања Запада, као и главне алате, односно механизме коришћене у тим операцијама.

С обзиром да је у оружаним сукобима циљ стратешка парализа непријатеља, то се постиже циљањем на виталне тачке у држави. Овакав ефекат се постиже на различите начине: оружаним путем, економским активностима, циљањем информационих центара или дипломатским активностима, присилом да се одређени поступци реализују или одвраћањем силом. Информационе операције РФ у Украјини, према констатацијама Запада, користиле су најчешће канале *Русија Данас* и *Спутњик*, као и многе друге руске канале: *LifeNews*, *Россия1*, *Россия 24*, *Первый канал*, *НТВ*, *РЕН ТВ* (Путник и Милосављевић, 2021). Ово су јасно уочљиви елементи, али поред ових, укључене су и оне активности које нису толико видљиве, односно биле су прикривеног карактера. Тако су медији имали другачије приступе, од пласирања једноставних дезинформација, преко полуистина, до софистицираних аргумената, што је довело до стварања информационе доминације руске стране (Путник и Милосављевић, 2021).

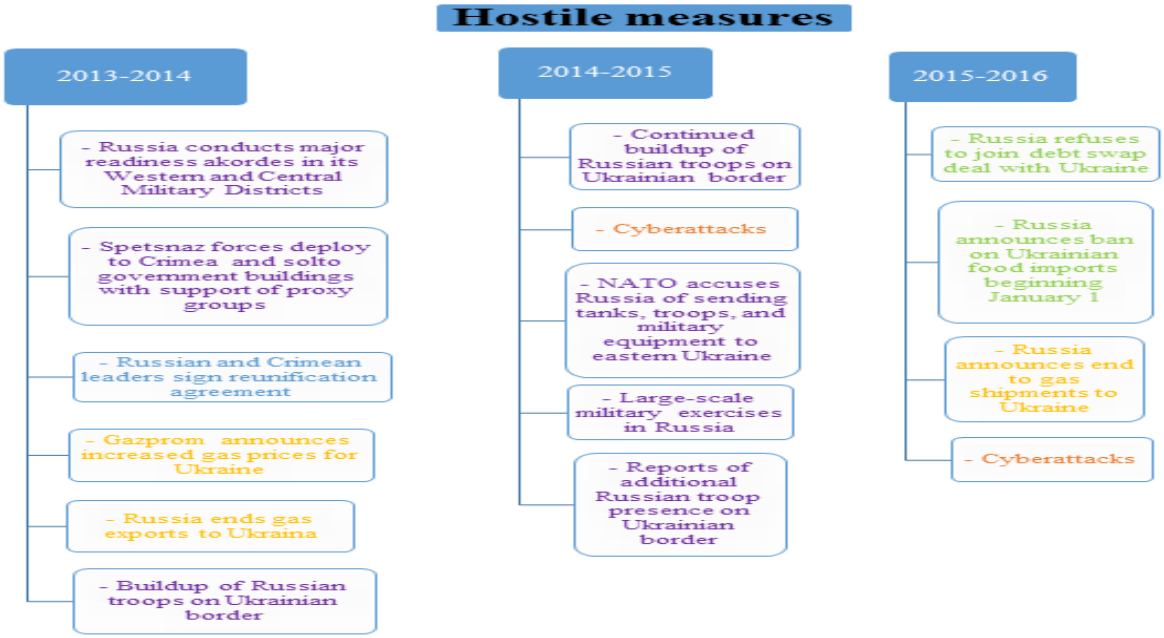
6.3.3. Безуспешно одвраћање и одбрана Украјине

Почетна операција на Криму била је опортунистичка, али строго контролисана, док је наредна операција у источној Украјини била слабије контролисана и можда је наставак сукоба био ван контроле РФ. Руска Федерација је успела да припоји Крим. У периоду до 2014. године нема војног присуства Северноатлантског савеза у Украјини. Након почетка руских непријатељских мера, операција, Северноатлантског савеза, САД су уложиле милијарде долара у подржавање оружаних снага Украјине, владе и економије. Сједињене Америчке Државе су такође успоставиле Заједничку мултинационалну групу за обуку, а Украјина ће помоћи у изградњи до пет батаљона украјинских војника годишње. Руска Федерација је можда настојала да одгурне Северноатлантски савез од својих граница, али је почетком 2018. године Украјина званично била евидентирана на веб – страници Северноатлантског савеза као амбициозни члан.

Руска Федерација је анектирала Крим и створила бескрајно замрзнути конфликт у источној Украјини, али је, ако ништа друго, убрзала политички покрет ка западу Украјине. Руске акције у Украјини скренуле су значајну пажњу на своје утицајне активности у источној Европи и њено економско понашање на међународном плану. Сједињене Америчке Државе, Европска унија и Канада донеле су оштре санкције РФ као одговор на њене операције у Украјини (*Слика 11*). Неки аналитичари тврде да су санкције имале занемарљив утицај на економију РФ, док други сматрају да су постигнути жељени ефекти. Економија РФ била је најмање делимично поткопана, а Украјина се приближила Западу и Северноатлантском савезу (Connable et al., 2020).



Слика 11. Непријатељске мере РФ према Украјини енг. *Ukraine Case Timeline*.
Слика је интерпретација Аутора (Извор: Connable et al., 2020, p. 44).
(Први део *Слике 11*, а други део је на наредној страници).



• Cyber • Economic • Energy • Legal • Military

Слика 11. Непријатељске мере РФ према Украјини енг. *Ukraine Case Timeline*.
Слика је интерпретација Аутора (Извор: Connable et al., 2020, p. 44).
(Други део *Слике 11*).

Анализирајући наведене студије случаја можемо доћи до одређених правила, образаца, везано за активности које су предузимане од стране РФ (*Слика 11*). Ради се о следећем: РФ доследно реагује непријатељским мерама када примети претње; лидери РФ често издају јавно упозорење пре него што примене непријатељске мере; краткорочне и дугорочне мере примењују се у међусобној комбинацији; дипломатска, информациона, војна и економска средства користе се заједнички; РФ истиче информационе, економске и дипломатске мере; сва оруђа која су на располагању влади се користе за примену непријатељских мера, често заједно. Свака врста силе са собом носи јединствени скуп могућности које се могу искористити за одвраћање, спречавање и супротстављање непријатељским мерама РФ. Следећи су примери активности непријатељских мера РФ које би Североатлантски савез могао да реши војним капацитетима, студија случаја сиве зоне[121] и анализе ратних игара РФ као што је Запад 2017. године то и констатовао, на следећи начин: „људско обавештајно извиђање физичких средстава за планирање саботаже, регрутовање људи као извора података служби безбедности, мерење и прикупљање података за службе безбедности, прикупљање података за службе безбедности о локалним информацијама помоћу малих мобилних уређаја, локално циљане информационе операције користећи регионалне медије, пропаганда против Североатлантског савеза, или пропаганда усмерена на одређене војне снаге, сајбер напади на локалне мреже или инфраструктуру (нпр. електричне мреже), сметње сигнала против глобалног позиционог система или других мешовитих војно – цивилних система, намерно погрешно приписани хемијски, биолошки или радиолошки напади, физичка саботажа кључне инфраструктуре, као што су транспортни системи или информационе мреже, тајни атентат на кључно војно или цивилно особље, складиштење оружја или муниције за употребу у будућем рату високог реда, инфилтрација или корупција војних снага партнера, продор или уништавање интернета или инфраструктуре мобилних комуникација, ограничени конвенционални војни напади, као што је копнени или ваздушни напад” (Connable et al., 2020, p. 64, 65).

Табела 19. Нови сајбер напади у Украјини 2017–2018. година.

Датум	Жртва	Врста жртве	Наводни починилац	Техника/ Алат, оруђе
03.2017.	Ukrainian computers	O	Sandworm	Ransomware, an early version of NotPetya
16.05.2017.	Ukrainian president Poroshenko’s official website	G	Unknown	Unknown type of cyberattack that caused the unavailability of the website for a few hours
18.05.2017.	Ukrainian computers	O	Sandworm	Xdata Ransomware, an early version of NotPetya
21.06.2017.	Ukrainian computers	O	Highly likely to be Sandworm	PSCrypt ransomware
26.06.2017.	Ukrainian computers	O	Highly likely to be Sandworm	Ransomware that visually looks like WannaCry

[121] Вишедеценијске интеракције између Запада и Савеза Совјетских Социјалистичких Република или РФ, почев од револуције 1917. године су се налазиле у такозваној *сивој зони* у мерама без рата. Неопходно је констатовати ово као реалност и да *сива зона* представља стални изазов и трајну претњу кохезији и стабилности Запада и њених савеза и вероватни увод и припрему РФ за рат високог реда (и обрнуто).

Датум	Жртва	Врста жртве	Наводни починилац	Техника/ Алат, оруђе
27.06.2017.	Ukrainian infrastructures, primarily computers, before spreading to the rest of the world	G/O	Sandworm	NotPetya malware was disguised as ransomware but was designed to cause damage
10.08.2017.	Ukrainian postal service website	G	Unknown	DDoS attack
24.10.2017.	Ukrainian and Russian computers	O	Allegedly APT28	BadRabbit ransomware
23.05.2018.	Routers worldwide, though primarily affecting Ukrainian targets	O	APT28	VPNFilter malware
G = Владине институције, O = Други учесници.				

Извор: Baezner, 2018, p. 46.

У периоду од почетка и током 2017. године, дошло је до бројних промена у погледу техника, алата (и група – види *Табелу 19*) који се користе у сајбер простору Украјине. Ради се о следећим алатима[122]: веб – странице у Украјини су трпеле повремене нападе дистрибуираног ускраћивања услуге (енг. *Distributed Denial of Service – DDoS*), оштећења на веб страницама, злонамерне програме, нови малвер који је заразио велики број рутера и повезаних уређаја као и рад на другим тајним активностима у сајбер простору – енг. *malware* (енг. *BlackEnergy, Snake, Operation Armageddon, X–Agent, CrashOverride, NotPetya, BadRabbit, VPNFilter, Python/Telebot*), пропаганда и дезинформације. Овим алатима су постизани следећи резултати: тешка доступност или недоступност конкретних веб – сајтова, украдене су одређене информације са заражених мрежа, вишесатни нестанак струје у Украјини због напада на неколико електрана, пропагандне и дезинформационе кампање оштећених рачунара и уређаја и сл. Напади дистрибуираног ускраћивања услуге су наставили да утичу на украјинске веб странице, напади не захтевају софистициране вештине и нису посебно штетни по мету. Проруски или антивладини хактивисти и патриотски хакери често стоје иза таквих напада који су обично служили за објављивање протеста хактивиста против украјинске владе. *Malware*, енг. – злонамерни програми; пет нових малвера је идентификовано од јануара 2017. године, и то: енг. *CrashOverride, NotPetya, BadRabbit, VPNFilter, Python/TeleBot. CrashOverride* је био малвер који је коришћен за напад на

[122] *Малвер* – злонамерни софтвер који може имати облик вируса, црва или тројанског коња. *Worm*, енг. – *црв,* самостални, самореплицирајући програм који инфицира и шири се на друге рачунаре путем мрежа. *Тројански коњ* – злонамерни софтвер скривен у легитимном програму да би заразио и „преузео" систем (Baezner, 2018). *Ransomware*, енг. – злонамерни софтвер који закључава рачунарски систем корисника и откључава га само када се плати откупнина и сл. *Напади дистрибуираног ускраћивања услуге (*енг. *DDoS)* – чин преоптерећења система великим бројем пакета кроз истовремену употребу заражених рачунара (Baezner, 2018). *False – flag*, енг. – лажна застава, чин обмањивања противника да мисли да је сајбер напад извршио неко други. *Хактивизам* – употреба техника хаковања за политички или друштвени активизам. *Firmware*, енг. – софтверски програм програмиран на хардверском уређају који даје упутства за комуникацију између уређаја и другог хардвера, фирмвер се чува у флеш меморији уређаја само за читање (Baezner, 2018). *Spear phishing*, енг. – „софистицирана техника пецања, која не само да имитира легитимне веб – странице, већ и бира потенцијалне мете и прилагођава им злонамерне е – поруке. Е – поруке често изгледају као да долазе од колеге или легитимне компаније" (Baezner, 2018, p. 47). *Sandworm*, енг. – пешчани црв, такође је познат и као енг. *Quedagh, Voodoo Bear, TeleBots, BlackEnergy group.* Сандворм је спроводила наводно значајне кампање у Украјини, сматра се подјединицом АПТ28 и тако је повезана са војном службом безбедности РФ, Главном управом (раније Главном обавештајном управом). *Gamaredon Group*, енг. је проруска хакерска група највероватније инструисана од стране 16. и 18. центра Федералне службе безбедности у РФ. *Gamaredon Group*, енг. обично користи *phishing*, енг. мејлове са приложеним злонамерним документима како би заразила своје мете. Познато је да група користи јавно доступне сајбер алате, али развија и сопствени малвер (Baezner, 2018).

украјинску електричну мрежу у децембру 2016. године, али са могућношћу прилагођавања окружењу. Дизајниран је за приступ индустријској контроли свог циља на даљину. Његов циљ није сајбер шпијунажа, већ да изазове штету. Вероватно је напад на електричну мрежу у децембру 2016. године био тестирање малвера. Компанија за сајбер безбедност *Dragos Inc.* приписала је енг. *CrashOverride* сандворму – пешчаном црву. *NotPetya*, енг. је црв који изгледа као рансомвер, а стручњаци за сајбер безбедност приписали су *NotPetya* сандворму. *BadRabbit*, енг. је рансомвер који је почео да се шири РФ и Украјином у 2017. години и првој половини 2018. године. Заразио је своје жртве путем лажног ажурирања енг. *Adobe Flash*. *BadRabbit*, енг. је дешифровао податке када је откупнина плаћена. Служба безбедности Украјине је оптужила АПТ28 за вршење напада *BadRabbit* и коришћење рансомвера као диверзије приликом покретања енг. *phishing* кампање. Компанија за сајбер безбедност *ESET* приписала је енг. *BadRabbit* сандворму. *VPNFilter*, енг. је злонамерни софтвер који инфицира рутере и друге повезане уређаје као што је мрежно складиште (енг. *Network – Attached Storage*). Инфилтрирано је више од 500.000 рутера у 54 земље (до 2018. године). Малвер дели неке низове кода са енг. *BlackEnergy* малвером. *VPNFilter*, енг. такође има функцију која га чини постојаним до поновног покретања (други малвери углавном не преживе поновно покретање). Министарство правде САД приписало је *VPNFilter*, енг. АПТ28, а стручњаци за сајбер безбедност сузили су починиоца на сандворм. *Python/TeleBot*, енг. је тројанац који је 2016. године циљао финансијске институције Украјине. Малвер се ширио путем е – порука за крађу идентитета са зараженим ексел документима. *Python/TeleBot*, енг. је послат у е – порукама за крађу идентитета са истих сервера као *BlackEnergy*, енг. малвер који је коришћен у нападу на електричну мрежу Украјине у децембру 2015. године енг. *Python/TeleBot*, посебно, има могућност да комуницира са нападачима и да прима команде, а може и да украде датотеке, прикупи информације на рачунару, направи снимке екрана и отпреми додатни малвер (Baezner, 2018).

Како бисмо сумирали све најбитније констатације о информационим операцијама РФ и Украјине у наведеним периодима, можемо констатовати следеће. Информације су моћно оруђе утицаја, а информативна кампања је била пресудна за операције РФ у Украјини. Наратив представника РФ се огледа у кључним документима политике, затим наратив РФ је у великој мери заснован на историјској основи. Криза у Украјини је резултат дуготрајности стратегије РФ, а улога сународника у иностранству је критична и треба је пажљиво размотрити за неке будуће сукобе. Безбедносне импликације за суседне државе РФ су посебно озбиљне. Анализом публике долази се до кључних елемената за рад и успех мада треба да је присутно и то да постоји „друга страна медаље", руске информационе операције. Државе користе превару као тактику за одвлачење пажње и одлагање неких догађаја. Операције дезинформисања протоком времена слабе, нестају (Bērziņš et al., 2015).

Да су активности служби безбедности Украјине биле укључене у битне криминалне активности и да су се њени припадници бавили коруптивним радњама доказује и поступак хапшења Андрије Наумова 7. јуна 2022. године и то у Републици Србији, на граничном прелазу на југу Србије, који се сумњичи за прање новца. Ради се о бившем високо позицинираном припаднику украјинске службе безбедности (генерал у Служби безбедности Украјине) који је код себе имао више стотина хиљада евра и дијаманте, о чему је известила Радио Слободна Европа наводно на основу информација добијених у Вишем јавном тужилаштву у Нишу, Република Србија, надлежном за овај случај. Индикативно је и то што

је са њим у возилу био држављанин Немачке, извесни господин Акст (*Aleksander /Alexander/ Akst*).

У проучавању сајбер напада на Естонију, може се констатовати да Грузија и Украјина деле слична искуства. Може се закључити да је извршена концентрација на офанзивну употребу сајбера од стране РФ у сврху одржавања своје надмоћи у сфери будућности – сајбер простору, а географски првенствено испољавање утицаја на простору бившег совјетског блока. Велики број теоретичара се бави изучавањем паравојних активности РФ, ангажовањем наводних приватних војних компанија као прокси снаге, међутим, сајбер напади, сукоби и поступање РФ у овој врсти сукоба је за сваки респект и поштовање. РФ је кроз војну стратегију и друга документа успела имплементирати сајбер нападе у најбитнији сегмент – информационо ратовање. Када се погледа уназад, анализом војних стратегија још од Савеза Совјетских Социјалистичких Република, па до РФ, могу се констатовати три најбитније целине ове стратегије: *мобилизација државе, одбрана равнотежом* (или неравнотежом), и улога *партизанског начина ратовања* као основе за будуће сукобе, односно *асиметрично, хибридно ратовање* и друге сукобе у *сивој зони* и слично. Када говоримо о периоду Савеза Совјетских Социјалистичких Република, *мобилизација државе* је имала за циљ да заштити унутрашњу револуцију у границама савеза, а затим да припреми државу за рат. Када посматрамо данас, део ове мобилизације посматрамо и кроз информациони простор. Манипулисањем сајбер простором заузима се контролна функција и преузима улога мобилизације. Потврда важности улоге информационог простора је евидентна у три случаја (случај Естоније, Грузије и Украјине), када су сајбер напади утицали на комуникације у три државе у време напада. *Одбрана равнотежом* је пре почетка Другог светског рата имала проблем. Као резултат, оно што је требало да буде баланс, постало је неравнотежа која фаворизује напад у односу на одбрану. Тако је и са укључивањем сајбера у укупну доктрину. Руска Федерација је прихватила скоро потпуно офанзивно војну стратегију све до XXI века. *Партизански рат* еволуирао је у данашње *асиметричне* и *хибридне* облике сукоба и друге сукобе у сивој зони. Овај метод вођења рата и сукоба је наставио да се развија, делимично због чињенице да асиметрично и хибридно ратовање добро функционишу са сајбером, што фаворизује офанзивне делатности. Сукоби у наведеним државама се могу сврстати као асиметрични или као хибридни, мада у суштини могу и као једна и друга врста. Важно је при томе нагласити да је руска употреба сајбер сукоба представљала проширење асиметричних и хибридних метода. Улога Владе РФ као актера у међународној сајбер агресији врло је нејасна, односно недоказана, недефинисана. Употреба сајбер ратовања је врло важна, не зато што су најчешћи актери ових сукоба Руси, већ зато што је руска употреба сајбер ратовања тако непрозирна, неоткривена, тајновита и данас. Може се констатовати да одобравање метода, алата од Владе РФ да се примењују у сивој зони, *испод радара*, при чему је добро познато да се наведеном применом алата може зарадити осуда мало или нимало, можда неко од испитивања, провера од стране међународне заједнице и то је то, чиме се ствара изузетно ефикасан облик агресије што је дефинитивно опасно по непријатељске државе (Miniats, 2019).

У *Белој књизи* постоје информације о кршењу људских права и владавине права у Украјини (обухвата период од јула до новембра 2014. године), масовним и намерним кршењима међународног хуманитарног права, људских права и владавине права од стране украјинских оружаних снага, и радикалних националистичких оружаних група (Ministry of

Foreign Affairs of the Russian Federation, 2022a). Према подацима Федералне миграционе службе РФ, укупан број држављана Украјине који су уточиште од крвавог сукоба нашли на територији РФ прелази 830.000 (само руска домаћинства имају примљено и дато уточиште за око 444.000 избеглица из Украјине). У паду авиона на лету број 17 малезијског авиопревозника погинуло је 298 људи у Доњецкој области у јулу 2014. године (други извор наводи 300 путника, прим. аут.). Ефикасна и непристрасна истрага ове трагедије још није спроведена и очигледно се лагано разводњава, од стране оних који нису заинтересовани у откривању истине. Третман према штићеницима и затвореницима са југоистока од стране Украјине, представљао је често такве методе мучења као што је спаљивање са усијаним предметима, слање на минско поље, лажне стрељачке водове и бацање у јаме са лешевима; постоје записи о укрцавању у воду – техника мучења која је некада била популарна код америчких тајних служби када су у питању њихове специјалне методе рада у затворима у иностранству, укључујући и један у заливу Гвантанамо. Међународни институт за заштиту репортера и безбедност је оценио Украјину као најопаснију земљу на свету по безбедност новинара. Почетком августа 2014. године А. Стенин, фоторепортер Интернационалне информативне агенције *Русија Данас*, убијен је у близини Доњецка. У наведеном периоду настављено је застрашивање пуцњевима, физичким нападима и отмицама. Постоје докази о хапшењима и неоснованом затварању грађанина који је поделио информације о стварном стању ствари на југоистоку Украјине на интернету. Методе које примењује Украјина укључују атентате на политичке противнике, намештање кривичних предмета, незаконите претресе, одузимање имовине, обично хулиганство, као и друге противправне методе застрашивања које се противе принципима владавине права и демократским стандардима (Ministry of Foreign Affairs of the Russian Federation, 2022a). Репресије над руским медијима у иностранству и руским новинарима, у Естонији је у 2022. години од почетка специјалне војне операције у Украјини за заштиту Донбаса, емитовање руске телевизије и радија – Планета, телевизије *нова, независна, невладина, наша*, Мир и телевизијског канала Русија 24 обустављено на годину дана (25. фебруара), због систематског ометања рада информативног портала *Спутњик медија* од разних структура и претњи његовим новинарима, медији су објавили престанак рада (8. марта), Телеком оператер (*Telia Eesti*) проактивно је обуставио емитовање руског телевизијског пословног канала (8. марта), блокиран је приступ руским сајтовима вести *нтв.ру; рен.тв; 5–тв.ру; 78.ру; 1тв.цом; лента.ру; тасс.ру* (15. марта), а главном и одговорном уреднику Спутњика Литванију М. Касему и главном и одговорном уреднику новинске агенције Балтневсу А. Старикову забрањен је улазак на период од пет година (11. и 12. јула), привремено су задржани запослени у Известији К. Солдатов и Д. Тимофејев, новинарима су укинуте визе, стављени су на црну листу и забрањен им је улазак у Европску унију на три године, 12. августа (Ministry of Foreign Affairs of the Russian Federation, 2022b). Увидом у Календар међународних политичких активности у 2015. години дошли смо до сазнања да није било билатералних састанака између РФ и Украјине, нити РФ и Естоније.

У 2014. години у Украјини је убијено шест новинара и једно лице запослено у медијима, а у Естонији није убијено нити једно лице (Reporters Without Borders, 2022). На званичном сајту Владе РФ нема регистрованих догађаја у вези са реализованим билатералним односима Владе РФ и Владе Украјине.

Одвраћање у РФ представља интегрисани низ нуклеарних, ненуклеарних, невојних и информационих мера утицаја које су обједињене у једну целину. Стратешко одвраћање поред нуклеарне способности примењује и друге начине присиле (Миљковић и Марјановић, 2023). Када говоримо о актуелним сукобима, РФ је у примени одвраћања према Украјини (посредно Североатлантском савезу) током 2022. године примењивала војне нуклеарне и ненуклеарне и део невојних мера у више домена утицаја (Миљковић и Марјановић, 2023). Мере које је РФ примењивала током 2022. године, а које региструјемо као активности одвраћања су: одвраћање нуклеарним оружјем, ненуклеарним хиперсоничним оружјем, економским активностима (првенствено енергетским) и информационим активностима. Током сукоба у Украјини у 2022. години, одвраћање РФ кроз информационо ратовање је било посредно, док је тежишно примењиван кинетички сукоб оружаних снага. Можемо констатовати да информациону супериорност РФ није успела да оствари у Украјини током 2022. године што је довело до негативног утицаја у примени одвраћања путем информација (Миљковић и Марјановић, 2023). Неопходно је констатовати да се овде није радило о сукобу РФ са Украјином већ посредно са скоро читавим Североатлантским савезом, па и шире. Поред подршке у војним капацитетима, у свим невојним, односно необавештајним активностима биле су активно укључене и службе безбедности и други капацитети ових држава, што представља огроман потенцијал којем се РФ супротстављала перспективним развојним концептима одвраћања.

7. ПЕРСПЕКТИВЕ РАЗВОЈА КОНЦЕПТА И АКТИВНОСТИ ОДВРАЋАЊА ВЕЛИКИХ СИЛА

Развој нових технологија, затим система оружја, довео је до појаве нових концепата одвраћања условљених појавом хиперсоничног оружја, што је довело до нове ескалације нестабилности између две велике силе, САД и РФ, и овако нестабилног концепта конвенционалног и нуклеарног одвраћања. Поред хиперсоничног оружја, појава дронова као феномена који су направили страховите промене у начину употребе оружаних снага, као и супротстављања истим, и вртоглави напредак у информационој и сајбер сфери довеле су до потребе за новим коцептима одвраћања.

7.1. ОЧЕКИВАНИ ПРАВЦИ РЕВИДИРАЊА СТРАТЕШКО – ДОКТРИНАРНИХ ДОКУМЕНАТА САД И РФ

Не треба прецењивати шта се од одвраћања може очекивати тј. постићи, али нови инструменти и домени одвраћања се мењају развојем нових технологија, што нуди нове могућности. Санкције и одвраћање су примењиве, оне претходе и прате напоре одвраћања. Међутим, генерално су несхваћене у смислу циљева, сем принуде. Повећање отпорности – одвраћањем, порицањем, појављује се у политичким документима Западних влада и Европске уније од 2014. године као одговор на све већу појаву хибридних претњи. Сајбер – способности се могу ефикасно користити као инструмент одвраћања, а и вештачка интелигенција. Синтеза увида из когнитивних наука, укључујући теорију перспективе, поткрепљује размишљање да стратези одвраћања никада не би требало да претпоставе да ће мете одвраћања реаговати у складу са правилима рационалног модела учесника у сукобу. Такође, присутан је и ефекат емоција у процесима доношења одлука, а поготово се код

ауторитарних лидера чини да емоције као што су част, престиж или страх од губитка образа могу заправо довести до побољшања преузимања ризика. Чак и када се учесници у кризи понашају рационално, веће организације се можда неће тако понашати, или може доћи до забуне који одвраћајући одговор је оправдан. Поставља се питање у тој оправданости, ко поступа и по којем правном оквиру у одвраћању. Када Северноатлантски савез и разне европске владе (њихове агенције, службе) расправљају о приступу читавог друштва у супротстављању нежељеним активностима екстерног хибридног утицаја, могу и хоће да сарађују у стварању кохезивних одговора, али неопходно је да буде увек присутан тај моменат сваке чланице у одвраћању, да ће пресудна одлука сваке чланице посебно ипак бити донешена у складу са личним, а не колективним интересом (Osinga & Sweijs, 2021).

Уколико је Северноатлантски савез озбиљан у томе да испуни своје обавезе из члана 5, онда ће морати да одговори РФ, односно њеним непријатељским мерама. Овде је велики проблем како препознати сиву зону, непријатељске мере. Употреба непријатељских мера је дуготрајна, али сајбер, информационе операције и друге акције су нове технологије и то може бити тешко за Северноатлантски савез да правовремено идентификује одговарајућу меру и одговор на њу. Запад мора да буде свестан да су непријатељске мере одрживо оруђе у сваком сукобу и да ће их РФ примењивати са значајном тактичком стручношћу (Connable et al., 2020).

Циљеви критичне инфраструктуре укључују нуклеарну енергију, електрична предузећа, воду, авијацију, телекомуникације, критичне производне секторе, и комерцијалне објекте. У 2015. години је објављен чланак *Њујорк Тајмса*, где се наводи да су САД те године пратиле океански истраживачки брод РФ под именом *Јантар*, који је опремљен са два самоходна дубокоморска подводна брода, док је крстарио од источне обале САД према Куби, где је један кабл у близини поморске базе оружаних снага САД у заливу Гвантанамо. Званичници тврде да постоји могућност да су брод и подводна летелица способни да пресеку каблове миљама дубоко испод површине мора. У 2017. години британски званичници су упозорили да морнарица РФ представља *катастрофалну* претњу за подводне каблове. Тако је у фебруару 2020. године Министарство одбране САД објавило свој буџетски захтев за 2021. годину у који је укључило мапу која прекрива поморске активности РФ и Народне Републике Кине, преко међународних подморских комуникационих каблова. Јасно је да наведено показује да стране поморске снаге потенцијално угрожавају глобалну економију доводећи у опасност подморске каблове (Riehle, 2022). Поред наведених каблова, безбедносно је интересантан и догађај везан за наводну хаварију 2022. године на Северном току 1 и на Североном току 2 у Балтичком мору када је РФ у медијима оптужила Велику Британију као државу одговорну за ову саботажу.

Ђумели (*Francesco Giumelli*) се бавио питањима санкција у XXI веку. Оне имају велики значај за стратегију одвраћања, где режими санкција често претходе наредним корацима за јачање одвраћања војним претњама. Санкције би требало да наносе штету противнику (мада су у најновијим дешавањима санкција према РФ много већи посредни ефекти санкција на друге државе и народе него на земљу којој се уводе), а да таква штета нанесе економски вид проблема који би се врло лако могао превести у политичку или неку другу добит. Санкције морају бити циљане, а не опште и према свим свеобухватне. Разлог је то што различити типови режима, демократски или ауторитарни, имају различите рањивости. Циљане санкције укључују ограничења слобода за појединце и одређене

недржавне субјекте као и замрзавање имовине, финансијска ограничења, с тим што је јако битно да се пре него што се донесе оваква одлука прво провери да ли по законима своје државе циљна група уопште има право на поседовање имовине у иностранству и слично, односно да ли смо уопште погодили меру присиле. Циљане санкције често за мету имају појединце, а они одређена људска права (наравно када говоримо о средњим и малим државама, док овај постулат није употребљив за велике силе). Циљане санкције су осмишљене тако да не наносе смртоносне последице, штету на својим циљевима. Циљане санкције се могу повећати што може обесхрабрити мету, а ту се јавља и проблем оправдавања таквог чина, морална димензија. Санкције се користе у разним областима, почев од разних криза, па међународног тероризма, затим неширења и управљања сукобима, постконфликтна реконструкција, организована борба против криминала и трговине људима (Giumelli, 2021). Веома је битан спектар санкција који се намерава применити (да ли испољава утицај или не), а посебно треба бити присутна процена коме (економски моменат утицаја на такву државу или друге ентитете, односно моћ, да буде испољена присила на другог, нпр. уколико је држава енергетски независна – промашај је и помињати енергетски вид санкција и сл.) се санкције уводе. Врло често, што можемо видети и на дневном нивоу (сукоба великих сила у 2022. години), увођење санкција може бити само фиктиван чин у одвраћању, а да је стварна намера прикривена, тотално на другом правцу деловања. Мада, може бити и циљ да наведене санкције буду само оправдање за народ и обичан свет, док је други циљ продужетак сукоба или нечијег исцрпљивања, изнуривања снага, средстава, моћи, док је крајњи циљ ко зна шта. На сличан начин посматрано, у реализацији војних операција врло често није познато које су стварне намере односно који је коначни циљ спровођења неке операције. Тај коначни циљ се настоји постићи применом одређених техника, тактика, радњи, поступака и мера, тако да први, други или ко зна који нижи циљ, чак и када се не оствари, не значи да тај коначни циљ није остварен или неће тек бити остварен; чак не мора бити уопште у тој области која се сагледава, што одвраћању даје временски зазор и пуни смисао као мери која се предузима у некој области.

Ослањање на приватне компаније у развоју, изградњи, одржавању и управљању својим инфраструктурама информационим и комуникационим технологијама је постало честа појава, јер не може више само државни сектор да подржи активности у овом домену. Укључивањем приватног сектора као равноправног актера може се надокнадити овај недостатак (Klaus, 2021). Раније је укључивање приватних компанија у реализацију одређених задатака служби безбедности у одвраћању била строго чувана тајна, али већ деценијама уназад употреба *наводно* приватних компанија (само у регистру) за потребе држава или других ентитета, структура у будућности, може постати јавна активност.

7.2. ПРОМЕНЕ У ДЕЛОКРУГУ И НАЧИНУ РАДА СЛУЖБИ БЕЗБЕДНОСТИ

Као и у свакој организацији, и у службама безбедности уколико руководство, менаџмент службе безбедности не врши управљање службом у складу са важећим нормативима, за очекивати је настанак проблема озбиљне природе по функционисање националне безбедности државе. Наиме, у наредних неколико констатација истичемо део проблема до којих може довести принцип лошег управљања службом безбедности (Harder,

2017); недовољан надзор и контрола рада службе безбедности подрива поверење у пружање услуга припадника службе, прекомерна тајност рада ствара могућност за злоупотребе које могу довести до угрожавања безбедности државе и људи (усклађивање се може контролисати, надзирати од спољашњих надзорних тела што треба искључивати само информације о изворима података служби безбедности, текућим операцијама служби, методе рада службе као и процедуре, идентитет припадника службе и њихово знање, способности, порекло и детаљи достављених података страним службама поготово ако се ради о тајним међународним сарадњама служби), свака илегална радња коју служба предузме угрожава државу и човека, политизовање служби безбедности доводи до неефикасне заштите националне безбедности, зато што служба безбедности уместо да се бави тренутним и будућим претњама сходно стратегијама донешеним у држави и новим претњама усмереним ка урушавању државе, она служи политичкој партији (у екстремном случају може довести и до стварања политичке полиције употребљене за политичку репресију), неефикасне сужбе безбедности немају рационалан приступ у коришћењу ресурса на употреби (Harder, 2017). Веома је битно да постоји сегмент јавности који је довољан за контролу и надзор служби безбедности како би се спречило да службе безбедности, односно првенствено менаџмент истих, створи убеђење о некажњивости о учињеним поступцима.

Промене у Западним службама безбедности (у Италији): реформе су настављене Законом број 410 од 30. децембра 1991. године, где је у раду, координацији служби безбедности извршена промена. Наиме, службама безбедности наложен је координисан рад обавештајних и истражних активности на супротстављању организованом криминалу (тако су службе безбедности овлашћене за спровођење обавештајних и безбедносних активности, како у земљи тако и у иностранству, обавезане да координирају када се ради о субверзивном деловању; истиче се комплексност субверзивног – необавештајног деловања) против „свих облика угрожавајућег или *субверзивног деловања* од стране организованих криминалних група, који представљају претњу институцијама државе и развоју друштва" (Милошевић, 2008, стр. 269). Закон број 124 од 3. августа 2007. године је чак формирао нове целине (и објединио део већ постојећих) у обавештајно – безбедносном систему Италије. У закону из 1991. године видимо да је још пре више деценија Италија констатовала *субверзивну активност* (*необавештајну активност*) као веома битну претњу по институције државе и уопште развој друштва, која преко организованог криминала као секундарне функције спроводи активности примарног карактера из домена необавештајних активности, док 2007. године констатујемо нормативно уређење, прилагођавање читавог система у организационом смислу новим претњама безбедности. Овај пример Италије наводимо као један од претеча у нормативном и практичном смислу констатовања пропуста у раду служби безбедности, првенствено координације рада и организационог уређења обавештајно – безбедносног система државе и исправљања тих грешака, где је чак и великој сили попут САД било потребно да се догоде озбиљни немили догађаји (попут терористичких аката 11/09) да би се констатовали овакви и њима слични закључци за унапређење рада служби безбедности, односно квалитетније безбедносне превентивне заштите националних интереса (Милошевић, 2008).

Наиме, терористички напади 11. септембра у САД открили су како су баријере између служби безбедности и других органа за спровођење закона и институција, створене да заштите грађанске слободе, постале превише ригидне, спречавајући тако ефикасност рада

надлежних служби. Ефективност координације против претњи је била битно смањена и довела је до идентификације ове баријере које су допринеле угрожавању националне безбедности САД. Мере које је држава спровела услед уочених пропуста у координацији и раду служби безбедности су решене имплементацијом нових закона и подзаконских аката ради побољшања размене информација широм САД. Закон о националној безбедности из 2002. године (енг. *Homeland Security Act of 2002, P.L. 107–296*) дао је Одељењу за унутрашњу безбедност (енг. *Department of Homeland Security*) одговорност за интеграцију информација за спровођење закона и обавештајних служби у вези са терористичким претњама држави. Одредбе Закона о реформи служби безбедности и превенцији тероризма из 2004. године (енг. *Intelligence Reform and Terrorist Prevention Act of 2004, P.L. 108–458*) успоставиле су Национални центар за борбу против тероризма (енг. *National Counterterrorism Center*) као координатора на савезном нивоу за информације и процену тероризма и створиле позицију директора Националне обавештајне заједнице да обезбеди стратешко управљање у 17 организационих елемената међународне заједнице. Поред регулисања мера за побољшање координације између служби, предузете су и мере у организационим променама служби безбедности ради побољшања сарадње у целој савезној влади; тако су исте укључиле формирање Заједничке оперативне групе за борбу против тероризма (енг. *Joint Terrorism Task Forces*) предвођене Федералним истражним бироом и однедавно, као део Одељења за унутрашњу безбедност, Националну мрежу центара за фузију. Канцеларија директора Националне обавештајне заједнице (енг. *Office of the Director of National Intelligence*) укључује и Центар за интеграцију обавештајних података о сајбер претњама (енг. *Cyber Threat Intelligence Integration Center*) где је и овај сегмент обједињен једним центром (DeVine, 2019a).

Федерација америчких научника у САД је након препознавања претње коју носи лажна информација, дезинформација, формирала Групу за истраживање дезинформација која је састављена од научника, стручњака за комуникације, научника за податке и технолога, са сврхом откривања, разумевања и ефикасног разоткривања дезинформација и лажних наратива у вези са конкретном темом, а актуелни су били догађаји у вези са пандемијом *COVID–19* (Federation of American Scientists, 2022b). Није искључено да наведене целине могу бити пример за сличне реорганизације по овом питању у целинама служби безбедности.

Велики је број дронова који достављају огроман број података у одређене базе података које је неопходно прегледати и извршити селекцију битних од небитних података. Када се у неком тренутку помене број од више хиљада дронова, поставља се питање колико је аналитичара, оператера који су потребни да би ови подаци добијени снимањем дронова постали употребљиви и корисни за спровођење операција. Већ годинама уназад, проблем генерисања све већег броја података представља озбиљан проблем, како за службе безбедности тако и за друге актере у сукобу. Вештачка интелигенција може бити решење за сортирање, тријажу и проналазак у што краћем времену податка који су битни за реализацију одређеног задатка, операције. Овим поступцима би била унапређена анализа доступних података па самим тим и повећана брзина у доласку до тачних података. Ово је изузетно битно у времену када енг. *fake news* и друге дезинформације утичу на доношење одређених одлука, оцена, процена и сл. Поред наведеног, вештачка интелигенција би могла вршити трансформацију податка из једног у други вид записа (аудио запис у писани извештај; видео запис у писани; писани у аудио запис; проналазак податка на основу аудио звука и друго),

све ово са циљем побољшања квалитета, као и брзине доступних података који након анализе од стране службе безбедности постају информације за доносиоце одлука (Hoadley & Sayler, 2020).

Служба безбедности, као и активности које предузимају, чини/е саставни елемент сваке информационе операције. У САД постоји неколико десетина различитих служби безбедности. Регистроване су организационе промене служби безбедности великих размера у САД, а све ради побољшања коришћења савремених ресурса у обезбеђивању што квалитетније националне безбедности САД. Директор Централне обавештајне агенције у САД објавио је да спроводе промене у одељењу које су предвиђене за 2015. годину, а измене су усмерене на унапређење рада у информационом простору и везане су за супротстављање изазовима у сајбер простору. Америчке војне службе безбедности посвећују много пажње добијању и анализи информација из отворених извора о страним земљама. Руководилац војне службе безбедности у САД, Винсент Стјуарт, на саслушању Сенатског комитета за оружане снаге САД о претњама националној безбедности САД, саопштио је да током одвијања руско – украјинског сукоба власти РФ користе „комплекс различитих војних и невојних инструмената притиска на Кијев, укључујући пропаганду, информационе операције, операције у сајбер простору, тајне агенте, редовне трупе, скривање иза *добровољаца* и плаћеника, пребацивање војних опрема сепаратистима и претње војном интервенцијом" (Шариков, 2020, p. 8). Службе безбедности су регистровале да се квантитет и квалитет претњи у свемиру и сајбер простору повећава и представља озбиљну претњу по националну безбедност САД. Директор Националне обавештајне заједнице САД, Џејмс Клапер током свог излагања (пред истим комитетом) изнео је да „руске власти спроводе широку и интензивну пропагандну кампању усмерену на руску публику да оправдају придруживање Крима и створе снажно уверење да западни свет представља претњу Руској безбедности. Пропагандна кампања руских власти је усмерена не само на становништво Русије, већ и на страног корисника" (Шариков, 2020, p. 8). Очигледно је да задатак супротстављања руској пропагандној кампањи постаје приоритет политике служби безбедности САД као и Министарства одбране, али и других ресора америчке владе.

Обмањујући део анексије Крима опчинио је многе и импресионирао како обмана може, али не самостално, већ потпомогнута и другим организованим активностима, да буде коришћена у операцији преузимања одређене територије. Када говоримо о другим организованим активностима, тада мислимо првенствено на руске специјалне јединице – снаге, хакере, тролове РФ, наоружане цивиле и паравојне организације. Интересантан је податак да су украјински војни команданти на Криму праћени, да им је прећено, попут јавних окупљања руље и сл. Уколико оваква и слична присила није уродила плодом, да убеди украјинског команданта да дезертира, пребегне или да се преда, паравојне активности су довршавале ове послове и то групе попут *Ноћних вукова* које су завршиле посао застрашујући украјинске војнике (Bouwmeester, 2020). Овде препознајемо један нови моменат активности; те активности су управо довеле до одређених промена у извођењу руских безбедносних операција. Наиме, када се изврши компарација сукоба из 2008. и 2014. године, уочавамо јасну разлику између руско – грузијског оружаног сукоба када су информационе операције подржавале операције копнене војске и ратног ваздухопловства и противваздухопловне одбране, док је већ 2014. године, током анексије Крима, улога промењена тотално, јер су сада информационе операције, укључујући активне мере и

одвраћање, биле главне операције које су опет биле подржане физичким активностима, радњама где је то било потребно (Bouwmeester, 2020). Интензиван – посредан рад служби безбедности са приватним војним и другим компанијама, организацијама, ради остваривања присиле, врло често и директних физичких обрачуна, па и ликвидација, доводи до грубог враћања у прошлост, што се тиче употребе ових институција у примени метода рада у заштити националних интереса држава где постоји велики број двоструких или вишеструких правила (аршина), како за велике силе (којима је дозвољено све), тако и за мале државе (које морају да поштују законе, правила, прописе под образложењем увођења *демократије* и сличним образложењима – присилама).

Услед повећане друштвене зависности од нових технологија, регистрованих нових претњи по безбедност држава, условило је трансформације служби безбедности (као и других целина система безбедности) и нове начине примене различитих концепата одвраћања у САД. У саставу службе безбедности Централне обавештајне агенције, постоји формацијска целина која се назива Дирекција за операције (енг. *Directorate of operations*) и ради се о дирекцији оперативног карактера која се бави прикупљањем обавештајних података добијених из људских извора. Када је потребно и под јединственим околностима, они спроводе *тајне акције* према упутствима председника. Интересантно је да је једно од радних места за које је расписан стални конкурс (укључујући 13. децембар 2022. године када је преузет материјал), радно место за Официра за паравојне операције, где припадници паравојних операција воде и управљају програмима *тајних акција* и прикупљају стране обавештајне податке од виталног значаја за креаторе политике националне безбедности и да ће, уколико се ради о пуном радном времену, овакво лице имати почетну плату $70,491, па до $116,788 с тим што почетна плата може бити и далеко већа уколико се ради о лицу са већим искуством (Central Intelligence Agency, 2022). Од формалних услова неопходно је имати диплому о завршеној вишој школи и подобно је познавати неки страни језик. Важно је поменути и да је услед прилагођавања актуелним претњама формирана нова, најмлађа дирекција у саставу Централне обавештајне агенције, а ради се о Дирекцији за дигиталне иновације, која убрзава иновације широм Централне обавештајне агенције. Дирекција се стара да тимови имају алате и технике који су им потребни за рад у модерном, повезаном свету и да и даље буду тајни. Од сајбер безбедности до инфраструктуре за информационе технологије, ови службеници држе Централну обавештајну агенцију. Једно од радних места за које је расписан стални конкурс (укључујући 13. децембар 2022. године када је преузет материјал) је и Службеник за сајбер операције, коме је посао прикупљање обавештајних података од противничких система и мрежа користећи напредне алате, технике и друго. Уколико се ради о пуном радном времену, овакво лице ће имати почетну плату $66,077 до $138,868, а посебно интересантно је то што се већ у конкурсу наговештава да је могуће да ће радити у САД или у иностранству, тако да се дефинитивно ради о оперативцима, не само о специјалистима за информационе технологије (Central Intelligence Agency, 2022).

Анализирајући структуру Федералне службе безбедности, представљену на званичној интернет презентацији ове службе, долазимо до констатације да главну структуру чине четири дела: Федерална служба безбедности Русије (у чијем саставу су службе, одељења, дирекције и други пододсеци које непосредно спроводе области деловања савезне службе безбедности, као и одељења која обављају руководеће функције), Службе територијалне безбедности (Одељења Федералне службе безбедности Русије за поједине регионе и

конститутивне ентитете РФ), Снаге безбедности у трупама (Одељења Федералне службе безбедности Русије у Оружаним снагама РФ, другим трупама и војним формацијама, као и у њиховим органима управљања) и Граничне власти (Одељења Федералне службе безбедности Русије за граничну службу). Поред ове четири целине у односу на специјалности, Федерална служба безбедности садржи: јединице авијације, образовне организације – центре, јединице специјалних снага, научна одељења, експерте – форензичка одељења, војносанитетске јединице (Federal Security Service of the Russian Federation, 2022). Када констатујемо да једна служба безбедности као што је Федерална служба безбедности, поседује Снаге безбедности у трупама где поред своје припадности у оружаним снагама РФ (због чега у суштини служба безбедности и постоји када је у питању сегмент оружаних снага) предвиђа постојање својих припадника у *другим трупама и војним формацијама као и њиховим органима управљања*, тада јасно препознајемо припадност њених припадника и у невојним и војним формацијама са посебним нагласком припадности и у њиховим органима управљања. Овде препознајемо сегмент могућности деловања у паравојним активностима служби безбедности и с обзиром да у својој формацији поседује јединице специјалних снага и авијацијске јединице, а сувишно је било шта коментарисати о аутономности у ангажовању на необавештајним активностима са оваквим капацитетима једне службе и када се на све то придодају Граничне власти, тада стварно имамо једну изузетно моћну организацију која све има под својом структуром за деловање како у држави тако и у иностранству.

У складу са Законом *О спољној обавештајној служби* усвојеним у децембру 1995. године, формирана је садашња организациона структура руске Спољне обавештајне службе која садржи: оперативни део, аналитички део, функционална одељења – одељења, службе, самостална одељења (Служба Внешней Разведки Российской Федерации, 2022). Овлашћења Спољне обавештајне службе РФ дефинисана су чланом 6. Федералног закона *О спољној обавештајној служби* где између осталих потенцирамо следеће: закључивање са савезним органима извршне власти, предузећима, установама и организацијама РФ споразума неопходних за спровођење обавештајних активности; организовање и обезбеђивање заштите државних тајни у институцијама РФ које се налазе ван територије РФ укључујући утврђивање поступка за спровођење физичке и техничке заштите ових институција као и мере за спречавање цурења путем техничких средстава; омогућавање безбедности држављана РФ послатих ван територије РФ, који по природи својих делатности имају приступ информацијама које представљају државну тајну, и чланова њихових породица који су са њима; за обављање својих делатности, Спољнообавештајна служба РФ може, по сопственој лиценци и сертификацији, да набавља, развија (са изузетком криптографских средстава заштите), креира, управља информационим системима, системима за комуникацију и пренос података, као и средства заштите информација од цурења података техничким каналима (Служба Внешней Разведки Российской Федерации, 2022). Важно је констатовати да давање овлашћења служби безбедности Спољној обавештајној служби (између осталих) да закључује споразум са савезним органима, установама, предузећима и организацијама даје могућност њеног директног ангажовања у више врста необавештајних активности само кроз ово овлашћење. Омогућавање безбедности држављана РФ послатих ван територије РФ као и физичку и техничку заштиту државних тајни које се налазе ван РФ захтева поседовање специјализованих структура, јединица, целина које ће се бавити овим

пословима и наравно да се исти ти састави могу користити за необавештајне активности у иностранству што уопште није приказао на званичном интернет сајту службе безбедности.

Овом приликом треба напоменути да велики проблем у организовању и раду служби безбедности у безбедносној заштити критичне инфраструктуре државе представљају сложеност инфраструктурних система и идентификовање специфичних ризика и претњи којима су изложени (Мићовић и Марјановић, 2022). Утврђивање редоследа спровођења радњи у заштити критичне инфраструктуре сходно рањивости којима се одређени системи излажу може бити једно од питања за службе безбедности сходно расположивим подацима и насталим проценама на основу истих (Мићовић и Марјановић, 2022). Како је неопходно инвестирати у застареле инфраструктурне објекте, што представља велику инвестицију и финансијски расход ради довођења у што функционалније стање критичне инфраструктуре државе, тако је неопходно прилагођавати службе безбедности да постану што опремљеније, обученије, функционалније, брже, способније, делимично прилагођене, организационо – структурно, између посталих потреба и потребама критичне инфраструктуре, које ће превентивно реаговати и учествовати у одвраћању током угрожавања националне безбедности државе (Мићовић и Марјановић, 2022).

7.3. САЈБЕР ОДВРАЋАЊЕ У БУДУЋНОСТИ

Страни обавештајни субјекти спроводе „сајбер операције са циљем продирања у нашу јавност и приватни сектор у потрази за политичким и војним схватањима, осетљивим истраживањима, интелектуалне имовине, пословне тајне, и лично идентификоване информације. Страни обавештајни субјекти представљају и контраобавештајне и безбедносне претње" (Strategic Plan 2018–2022, 2017, p. 2).

Поред напред наведених активности у постхладноратовском периоду – сајбер активности – оно што бисмо могли навести да је званично саопштавано као скоријег датума од представника служби безбедности САД или других извора, наводимо у даљем делу истраживања. У септембру 2020. године, директор Федералног истражног бироа, Кристофер Реј (*Christopher Wray*), изјавио је да је РФ имала *веома активне напоре* (мислећи на војну службу безбедности РФ, Главну управу) да се умеша у изборе 2020. године и да је спроводила операције утицаја и дезинформација, али да „за разлику од 2016. године, нису видели упорне сајбер напоре РФ да се приступи изборној инфраструктури" (Bowen, 2021, p. 19). Наводно је у извештају приватног сектора за сајбер безбедност компанија у иностранству наведено да је војна служба безбедности РФ, Главна управа, хаковала компјутерске мреже украјинске компаније за природни гас *Burisma*, где је син председника САД Џоа Бајдена (*Joe Biden*), Хантер Бајден (*Hunter Biden*), раније био члан одбора. Поред САД, и Француска и Немачка су јавно оптужиле војну службу безбедности РФ, Главну управу, односно њене сајбер јединице, да спроводе опсежну и интензивну сајбер шпијунску кампању против владиних циљева и уочи избора. Једна фирма за сајбер безбедност је повезала Главну управу са покушајем пробоја критичне инфраструктуре САД. У јулу 2021. године, службе безбедности САД и Уједињеног Краљевства идентификовале су Јединицу 26165 као широко распрострањену, која анонимно врши приступе, грубом силом против стотина циљева владиног и приватног сектора широм света (Bowen, 2021).

На пример, поред Националног центра за борбу против тероризма, Канцеларија директора Националне обавештајне заједнице (енг. *Office of the Director of National*

Intelligence) укључује и Центар за интеграцију обавештајних података о сајбер претњама (DeVine, 2019a). Овај центар је основан 2015. године и одговоран је на савезном нивоу за пружање анализе свих извора података добијених ангажовањем служби безбедности у вези са сајбер претњама САД. Слично као Национални центар за борбу против тероризма који обједињава све битне податке о могућем угрожавању САД од тероризма, Центар за интеграцију обавештајних података о сајбер претњама, остварује комуникацију са другим службама безбедности и другим институцијама широм савезне владе и на државном и локалном нивоу како би била олакшана размена података служби безбедности и пружио јединствен, координиран напор за израду адекватне, пре свега правовремене процене о угрожености и пружање превентивног упозорења о сајбер претњама држави (DeVine, 2019a).

Успостављање сајбер команде у САД (енг. *United States Cyber Command*) већ је било разматрано средином 2000–их као перспектива за општи руски наступ. У РФ наводно је формално замишљено и успостављено негде 2014.–2015. године, постојање руске сајбер – јединице под војном командом, одвојене и различите од обавештајних служби по структури и фокусу мисије, што јавно није било признато све до 2017. године. Превласт у РФ била је наводно фокусирана на домаћу Федералну службу безбедности, која је, поред Генералштаба, Главне управе и Министарства унутрашњих послова, пружила жесток отпор идејама о повећаној војној улози у сајбер простору до 2014. године (Wilde, 2022).

Ради стварања повољног информационог окружења за САД формирана је Сајбер команда САД (енг. *U.S. Cyber Command*) која координира и руководи трансрегионалним операцијама и сарађује са другим одељењима Владе САД и припадницима војно – индустријског комплекса. Када помињемо војни комплекс САД, тада говоримо о терминологији коју употребљавају припадници оружаних снага, везану за *сајбер простор* који тумаче као једну од сфера оружане борбе (поред већ познатих сфера оружане борбе ваздуха, мора, копна и свемира). У већини великих система, па и у службама безбедности, тек када се догоде нежељене делатности или неки скандал, озбиљније се приступи овој области. Тако је и након бројних скандала везаних за откриће Едварда Сноудена, бившег припадника америчке службе безбедности Агенције за националну безбедност и критика америчких власти, дошло до великог опреза у развоју било које офанзивне операције у сајбер простору, првенствено у вези са поштовањем законодавства у области приступа поверљивим информацијама (информације о офанзивним сајбер операцијама – енг. *Cyberspace operations,* увек су степена тајности – државна тајна). Министарство одбране САД у својој надлежности за једну од области коју штити (у безбедносном смислу) има сајбер простор јавних и приватних информационих мрежа у САД. Као кључне претње националној безбедности САД, Командант Сајбер команде САД Мајкл Роџерс, истиче следеће: повећање случајева продора у јавне и приватне рачунарске мреже у циљу крађе информација; затим нови тип сајбер напада у последње време узима маха (развијањем војних информација као средстава прерушених у злочиначке групе); док у другом обраћању, директор Агенције за националну безбедност и Командант сајбер команде напомињу да је тренутно главни посао усмерен на супротстављање активностима Исламске државе у Ираку и Сирији. Сходно нормативима у САД, ради супротстављања сајбер и сличним нападима спремне су да употребе било које средство као одговор на сајбер нападе, а ту се мисли на дипломатске, економске и војне одговоре. У последњем говору, директор Агенције за националну безбедност је изјавио да је концепт *сајбер одвраћања* још увек прилично незрео. „У великој мери концепт сајбер

одвраћања је у веома раној фази развоја и тек треба да се развије и усвоје кодекси понашања у сајбер простору који ће бити у складу са идејом одвраћања и подржавати је" (Шариков, 2020, p. 6).

Озбиљне импликације по националну безбедност САД, сенатор Тед Круз види у препуштању вођства у развоју вештачке интелигенције Народној Републици Кини, РФ или другим земљама. Директор Националне обавештајне заједнице Даниел Коатс (енг. *Director of National Intelligence – Daniel Coates*) 2017. године је тврдио да способности наших противника да користе вештачку интелигенцију укључују повећану рањивост САД на сајбер нападе, потешкоће у утврђивању извршиоца напада, омогућавање напретка у страним системима за развој оружја и страних служби безбедности, чиме се повећава ризик по националну безбедност САД. Ривалитет у развоју вештачке интелигенције је озбиљан проблем за сваку државу, јер увек остаје као могућност да онај други има мање моралних, правних или етичких недоумица око развоја, па затим и употребе војних система (оружја) вештачке интелигенције (Hoadley & Sayler, 2020).

Да би функционисала као сопствени систем одвраћања, изградња сајбер одвраћања захтева велики број различитог сајбер оружја, метода напада, јер су за једнократну употребу против истог противника. Функционисање сајбер одвраћања захтева да противник нема на располагању значајно конвенционално оружје или да нема воље (нпр. политичке или правне или технолошке баријере) да га користи. Израелски концепт кумулативног одвраћања наглашава потребу за тренутним и кредибилним одговором. Стратешко одвраћање Израела може се описати као одвраћање одмаздом, док је стратешко одвраћање РФ, посебно њено сајбер одвраћање, више одвраћање порицањем, иако су средства која користе често увредљива. Укупна стратегија одвраћања РФ и Израела заснива се на њиховој стратешкој култури и њиховој перцепцији претњи које се међусобно разликују. Кључна разлика у стратегијама одвраћања ових држава је у томе што Израел користи кумулативне методе како би јасно ставио до знања куда иду црвене линије, док је стратешки циљ РФ да их замагли и створи сукоб, рат у магли. У оквирима будућности, очигледно је да и Израел и РФ улажу у развој вештачке интелигенције, роботике и аутономних система наоружања. Ко буде напреднији у овим областима ће вероватно имати квалитетније одвраћање, али с друге стране, ово такође наглашава важност сајбер одбране, јер и напредни системи наоружања или других технологија могу бити непредвидиви и рањиви (Turunen & Kari, 2022).

Одвраћање порицањем мора предвидети, односно узети у обзир, различите интензитете и врсте претњи са којима се свака држава суочава. Потребно је установити који напори САД могу бити најкориснији, уз процену већ познате рањивости и размотрити где помоћ САД може бити најефикаснија. У државама које нису у Северноатлантском савезу, а ради се о бившим совјетским републикама, као што је Украјина, РФ је у стању да употребљава најшири спектар својих субверзивних способности, укључујући коришћење како војних, тако и политичких пуномоћника. Напори да се побољша законска уређеност у одређеним областима и ојача алтернатива извозу енергије РФ и јачање сајбер безбедности могу бити драгоцени тамо где постоји могућност за то (Radin, Demus & Marcinek, 2020).

У свом извештају Уједињених нација (енг. *UN symbol A/77/296*, од 17. августа 2022. године), специјални известилац за негативан утицај једностраних принудних мера на уживање људских права, Ален Доухан, даје преглед и процену развоја сајбер технологија и њиховог утицаја на употребу једностраних санкција, оцењује законитост и хуманитарни

утицај мера које предузимају државе и регионалне организације у вези са злонамерним активностима у сајбер простору, а посебну пажњу поклања блокирању приступа веб – страницама и софтверу (Douhan, 2022). Тако се као прироритет намеће констатација питања одвраћања, заштите сајбер простора сагледавајући га ради успостављања сајбер мира између држава (Путник, 2022).

7.4. НОВЕ ТЕХНОЛОГИЈЕ И ОДВРАЋАЊЕ

Корени стратегије одвраћања вероватно су стари колико и настанак друштва. Прва осмишљавања заштите друштва, па државе једне од друге, углавном су била базирана на могућем избегавању сукоба, рата са другима. Тај вид избегавања – одвраћања је обухватао неке мере, планове који су предузимани, а како би се друга страна натерала да одустане од своје намере према матичној држави. Врло често, та стратегија одвраћања је подразумевала куповину и набавку најсавременијег наоружања и опреме, па када је дипломатија заказала и исцрпила све изворе, тада је по развијању служби безбедности ступила примена присиле, првенствено када говоримо о великим силама на планети, најчешће у облику необавештајних активности. Врхунац стратегије одвраћања између великих сила региструјемо током Хладног рата и гомилањем стратешког нуклеарног оружја како би она друга страна била у могућности да одговори други пут, да се обезбеди уништење оне друге велике силе. То обезбеђење другог удара или одговора на евентуални напад велике силе нуклеарним оружјем, првенствено се односи на чувену тријаду где би морали имати стратешке балистичке ракете које се лансирају са копна или из подморница, као и тешке бомбардере од којих је један број константно у ваздуху чекајући команду за активирање ракета према циљу. Када помињемо хиперсоничне ракете у лепези избора начина одвраћања, тада можемо рећи да стратегија одвраћања сужава простор за реаговање, односно за одбрану на евентуални напад и самим тим време које је нападнутој држави на располагању да се одбрани или евентуално да одговори према тој држави (да је нападне). Уколико држава не поседује сателитске радаре, према проценама стручних лица из ове области, ако је хиперсонично оружје лансирано према непријатељу, тада ће имати на располагању тек око шест минута до момента пре удара ракете. Уколико се хипотетички размишља о другом удару на државу која је прва реализовала напад, спровођење таквог наређења (процедурално) уз поштовање прописаних норми за такве ситуације, а ради недостатка времена, неће омогућити спровођење овакве процедуре. Једино што државама које немају сателитска рана упозорења остаје као опција је да пропусте неки од корака у процедурама одлучивања за употребу ракета где би било дозвољено реаговање, на нижим нивоима командовања, руковођења, на нивоу јединица. Време од уочавања претње до лансирања ракете је први дефинисао Џон Бојд (*John Boyd*, стратег у САД) и назвао је енг. *OODA* петља (енг. *Observe, Orient, Decide, Act Loop*), која обухвата низ догађаја од регистровања претње, преко оријентисања и доношења одлуке до реаговања, лансирања ракете. Хиперсонично оружје уводи још једну нову димензију нове нестабилности и овако нестабилног концепта нуклеарног одвраћања (Стојановић, 2020).

У транскрипту Извештаја војних званичника за буџет Министарства одбране оружаних снага САД за 2023. фискалну годину (енг. *Army Officials Brief FY23 Department of Defense Budget Request*) 28. марта 2022. године, потпуковник Кели (*Brandon Kelley*), у вези са одвраћањем наводи следеће, подржавајући мисију одвраћања Североатлантског савеза у Европи са преко 45.000 војника распоређених у Немачкој и Пољској: стратешке циљеве

остварити кроз интегрисано одвраћање, активну кампању и изградњу трајне предности; израдити прототип хиперсоничне ракете, затим ракете средњег домета и др. Трансформација структуре оружаних снага укључује постављање, на пример, трећег војног домена који би интегрисао ватру, сајбер и електронско ратовање као и информационо ратовање, познат као Пројект Конвергенс '22 (енг. *Project Convergence '22*), што представља стални напор комбиновања експериментисања и вежби са партнерима и савезницима. Постоји 185,4 милиона долара за подршку напорима Европске иницијативе за одвраћање, укључујући за два комплекса за обуку батаљона за операције и одржавање возила у Графенверу у Немачкој (Army Officials Brief FY23 Department of Defense Budget Request, 2022).

Годишњи извештај Федерације америчких научника за 2022. годину (енг. *Federation Of American Scientists*) пружа потпуни преглед Пентагоновог стратешког одвраћања, што обухвата 264 милијарде долара предвиђених за копно, поред основне улоге интерконтиненталних балистичких ракета у нуклеарној стратегији САД (Federation of American Scientists, 2022a).

Некада давно, долазак до нових сазнања о непријатељу је био попут поступка припадника оружаних снага на следећој слици (*Слика 12*). Уочавамо да један део извора података покушава да нешто чује, други део или сегмент чине извори података који у том периоду покушавају да виде нешто, а официри те сакупљене податке грубо анализирају док доласком нових технологија долази до озбиљних промена у овим активностима.

Слика 12. *Scouts at Sevastopol*[123] енг. (рус. *Пластуны под Севастополем*) *Vasily Grigorievich Perov, 1874, Kiev*.
Извор: *arthive.com*.

Службе безбедности РФ у великој мери се ослањају на људске методе рада, као што су регрутовање агената, формирање лажних (или коришћење постојећих) компанија (фирми) и људски продор у конкурентске компаније (фирме) за задатком економских активности службе безбедности и доласка до података о економској и научно – технолошкој области. Службе безбедности РФ такође користе страно корпоративно окружење које је спремно да сарађује са компанијама из РФ, користећи корпоративне споразуме и инвестиције као платформе за рад служби безбедности у економским активностима. Део ових сарадничких споразума је постао мета активности дезинформисања служби безбедности РФ, у случајевима када постоји претња да се планиране економске активности неће реализовати како је то планирала служба безбедности РФ или само руководство РФ. Поред наведених

[123] Примена метода прикупљања и анализе сазнања страна у сукобу, пре доступности нових технологија.

метода, припадници служби безбедности РФ такође тајно прикупљају податке отвореног карактера или дају задатке изворима података да прикупљају податке за њих. Основно обележје сада поменутог начина доласка до података од економског интереса је тајност, али се ради о подацима који су отвореног карактера. Компјутерске операције за унутрашње економске контраобавештајне сврхе у РФ се користе интензивно, док када се актер компјутерски[124] циља на индустријско предузеће или другу организацију тј. институцију, чини се да су те акције пре саботажног карактера, необавештајног облика деловања, него прикупљање обавештајних података мада су честе појаве и једне и друге активности служби безбедности (Riehle, 2022). Нуклеарно оружје РФ чине снаге које се састоје од стратешких система дугог домета (интерконтиненталне балистичке ракете), балистичких ракета на подморницама, тешких бомбардера и система за дејства краћег и средњег домета. Модернизацијом нуклеарних снага, новим ракетама, подморницама и авионима, РФ развија нове системе за дејство где је без обзира на смањење бројчаног стања ракета, према проценама САД, РФ задржала више од 1500 бојевих глава које објективно могу угрозити територију САД. У марту 2018. године председник Владимир Путин је објавио да РФ развија нове типове нуклеарних система. Ови нови системи укључују, интерконтиненталне ракете са способношћу да носе више бојевих глава, хиперсонично клизно возило, аутономно подводно возило и крстарећу ракету на нуклеарни погон. Хиперсонично клизно возило, ношено на постојећој балистичкој ракети дугог домета која се одваја у једном моменту, ушло је у употребу крајем 2019. године. Хиперсонично оружје није новина у технологијама, али повећана маневарска способност (што га чини неухватљивим) на тако великим брзинама (преко 5 маха), повећана прецизност, управљање летом ракете и друге техничке и маневарске карактеристике су велика новост у новим технологијама и развоју и модернизацији ракета ове врсте (Стојановић, 2020). Можемо да констатујемо да се овде поставља питање капацитета противракетне одбране САД. Победник у овој трци, трци за новим технологијама, дефинитивно је онај који поседује квалитет, то видимо из напред наведеног, јер су се деценијама трке између великих сила одвијале у квантитету поседовања наоружања и друге војне опреме.

Вештачка интелигенција пружа могућност вишеструког увећавања силе кроз повећање броја јефтиних војних система где једна таква летелица, возило, дрон нема шансу у супротстављању системима противракетне одбране и противваздухопловне одбране као и против високософистицираних летелица, ваздухоплова, али велики број таквих дронова има могућност множења силе, па би *рој* таквих дронова потенцијално могао да преплави високотехнолошке системе, стварајући део тренутних платформи превазиђеним и застарелим. Приступачност дронова (мала финансијска вредност, јефтини за куповину), оних који поседују вештачку интелигенцију, може у будућности тотално променити односе војне

[124] У 2016. години, Савезни уред за заштиту устава у Немачкој известио је да је регистрована хакерска кампања повезана са војном службом безбедности РФ, Главном управом (некада Главна обавештајна управа), у немачким истраживачким институцијама и компанијама, а посебно у области ласерске технологије и оптике. Поред наведеног, хакерске кампање су биле везане и за прикупљање података из фармацеутских компанија у трци за проналажењем вакцина за *COVID–19*. У извештају Националног центра за безбедносну и контраобавештајну службу САД 2018. године, о Спољно – економској шпијунажи у сајбер простору, тврди се да је у последње време РФ драматично повећала своју потражњу за прегледима изворног кода за страну технологију која се продаје у земљи (Riehle, 2022).

моћи. Наиме, овим начином размишљања, сагледавања војне моћи из угла који је управо описан, могле би сиромашне земље или чак и недржавни актери, без огромне популације становништва и војних јединица, снага, средстава и опреме, да постану несразмерно величини изузетно утицајни на бојном пољу или да те ефекте искористе у неку другу сврху за спровођење одређеног одвраћања, присиле и остварења циљева (Hoadley & Sayler, 2020).

Ограничена база знања из области вештачке интелигенције је сасвим довољан разлог за можда превелика очекивања у вези са очекивањима из домена вештачке интелигенције и апликација везаних за системе наоружања. Утицај на националну безбедност вештачка интелигенција испољава кроз будући начин употребе оружаних снага државе, затим начин прикупљања, а поготово коришћења безбедносно и обавештајно интересантних података. Вилнер и Баб (*Alex Wilner and Casey Babb*) презентују на који начин вештачка интелигенција може да утиче на принуду. Изменом калкулације трошкова, површним наметањем рационалних политичких одлука и смањењем потребе за ангажовањем људи у саставу војске или других организација у активностима које предузимају. Вештачка интелигенција може делимично или потпуно уклонити људске емоције и одлуке о примени принуде у реалности. Када говоримо о овом сегменту, тада мислимо на прикупљање, анализу, синтезу и деловање у односу на податке до којих долазе службе безбедности, с тим што је применом вештачке интелигенције све проверено више пута из великог броја извора, у јако кратком временском периоду, што читава армија аналитичара и оперативаца не би могла месецима да установи, провери, предузме. Оваквим радњама, поступцима се поспешује стратегија кажњавања, принуде, па тиме и смањује удаљеност између података служби безбедности (безбедносно и обавештајно интересантних), политичких одлука и принудне акције. Када се говори о дроновима као тренутном феномену који је и даље изузетно актуелан, ако би били модернизовани са вештачком интелигенцијом, њихово коришћење и употреба тако да се користи велики број дронова у исто време, тзв. ројеви, где би својом масовношћу, бројношћу и другим особинама надјачали одбрану противника, представљали би офанзивни моменат употребе дронова, док када размишљамо о дефанзивном моменту употребе оваквих средстава, тада једну од варијанти видимо у безбедној опцији аутоматског одговора током регистровања напада. Вештачка интелигенција може убрзати деловање у свим доменима принуде, па и када дође до сукоба, у кризним ситуацијама и на крају ратном стању (Wilner & Babb, 2021). Можемо констатовати да је вештачка интелигенција у домену одвраћања и принуде у развоју и да се може очекивати да ће њен утицај на одвраћање бити значајан. Војне, као и апликације вештачке интелигенције за потребе служби безбедности, ће се материјализовати и бити интегрисане од стране војних организација, служби безбедности и других организација чиме ће се остварити велики напредак у раду истих, мада никада не треба заборавити, искључити сегмент ризика који носи примена оваквих и евентуално у потпуности ослањање на овакве и њима сличне апликације.

Као један од одговора на стратешке бриге у вези са вештачком интелигенцијом и за даљи напредни развој вештачке интелигенције, Поморска постдипломска школа (енг. *Naval Postgraduate School*) у САД види у интегрисању сталних напора истраживача и студената укључених у преко 100 актуелних пројеката (децембра 2022.) са јединственим конзорцијумом фокусираним искључиво на апликације везане за вештачку интелигенцију. Капацитети ове високошколске установе у САД између осталог обухватају и интегрисање најсавременије технологије у поморску ратну борбу кроз употребу и развој вештачке

интелигенције, 5Г мреже, квантне науке и технологије, аутономних система, хиперсоничне системе, сајбер простора, способности засноване на свемиру, адитивна производња – штампа у три димензије и др. (Naval Postgraduate School, 2022).

Аутономни смртоносни оружани системи (енг. *Lethal Autonomous Weapon Systems*) представљају самосталне системе који нису још увек у масовној употреби, али представљају перспективно оружје у развоју намењено да смањи претњу по губитак живота приликом реализације операција док се сама употреба предвиђа на терену где се очекују проблеми са комуникацијама, ометања, и надмоћ непријатеља у ваздушном простору, што би досадашње системе избацило из употребе и/или довело до нежељених губитака. Аутономни смртоносни оружани системи представљају посебну врсту система наоружања који за потребе рада и употребе у реалним условима користи читав низ сензора, програма – алгоритама компјутерских са циљем аутономног извршења одређених задатака, оштећења, избацивања из употребе, уништења објеката, наоружања, средстава и људи. Оружане снаге САД немају закон из ове области који би их ограничавао у развоју оваквих и сличних система. Министарство одбране САД прописало је Директиву 21. новембра 2012. године, ажурирану све до данас, са називом *Аутономија у системима оружја* (енг. *Department of Defense Directive 3000.09, Autonomy in Weapon Systems*), која регулише рад са полуаутономним и аутономним системима оружја. На основу ове директиве дата је обавеза да сви системи који се стварају, развијају и употребљавају, без обзира на класификацију, буду направљени на такав начин да омогуће командантима – руководиоцима и оператерима да доносе у реализацији задатака одговарајуће нивое људских одлука. Пре развоја и стављања у употребу оваквог оружја, неопходно је одобрење четири нивоа руководиоца. Оружје које примењује несмртоносну, некинетичку силу, као што су неки облици електронског напада, на материјалне циљеве су изузети из ових услова. Произвођачи аутономног оружја у Народној Републици Кини рекламирају беспилотне летелице за продају које су наводно способне за потпуно аутономан рад, па и за извођење смртоносних удара, што према изјавама званичника САД, Секретара одбране, представља претњу за САД (Hoadley & Sayler, 2020).

Када говоримо о развоју нових средстава и опреме, система у наоружању и војној опреми, вредно је поменути између осталих, енг. *B–52H Stratofortress*, тешки бомбардер великог домета који може да обавља различите мисије. Бомбардер је способан да лети великом подзвучном брзином на висинама до 50.000 стопа (15.166,6 метара). Може да носи нуклеарна или прецизно вођена конвенционална убојна средства са могућношћу прецизне навигације широм света (Science & Technology, 2022); затим Војну радионицу људских перформанси где испитује катализаторе за спремност војника (наведено можемо да препознамо као озбиљан проблем у одвраћању данас и у будућности, поготово у државама где су људи осетили квалитетнији живот, те ову радионицу можемо схватити као једну од предузетих мера од стране државе, односно оружаних снага САД према регистрованој претњи), затим активности у свемиру (Science & Technology, 2022).

Амерички аналитичари констатују да је РФ почела да примењује стратегију одвраћања, где би могла да запрети употребом нуклеарног оружја, ако изгуби сукоб са чланицом Североатлантског савеза како би присилила САД или чланице Североатлантског савеза да се повуку из борбе. Поставља се питање о томе да ли су амерички програми модернизације (трке за новим информационим и другим технологијама) потребни да би се

одржало америчко нуклеарно одвраћање, или би такви програми могли да подстакну трку у наоружању са РФ. Неопходно је сагледати закључке експертских заједница о руској нуклеарној доктрини када се одлучује да ли САД треба да развију нове способности за одвраћање руске употребе нуклеарног оружја и да ли би то могле бити необавештајне активности служби безбедности. Стратегија националне одбране САД из 2018. године идентификовала је као главни изазов за безбедност САД стратешку конкуренцију са РФ и НР Кином. Тренутну структуру руских снага, укључујући њене интерконтиненталне балистичке ракете дугог домета (енг. *intercontinental ballistic missiles*), балистичке ракете које се лансирају са подморница (енг. *submarine – launched ballistic missiles*) и тешки бомбардери што чини тријаду нуклеарних снага као и нестратешко нуклеарно оружје мањег домета. Овај део такође наглашава кључне елементе релевантне инфраструктуре, укључујући рано упозоравање, команду и контролу, производњу, тестирање и складиштење бојевих глава. Такође описује кључне програме модернизације (*Табела 20*) које РФ спроводи да би одржала и, у неким случајевима, проширила свој нуклеарни арсенал.

Табела 20. Кључни програми модернизације ракетних система у РФ – Нуклеарни програм оружаних снага РФ.

System	Warheads	Notes
Avangard HGV	One per vehicle, nuclear	Can be delivered by SS – 19 and potentially the Sarmat ICBMs; intended to overcome missile defense
RS – 28 (Sarmat) silo ICBM	10+, nuclear	Deployment expected around 2022; intended to overcome missile defense
Poseidon Autonomous Underwater Vehicle	Conventional or nuclear	Carried by special – purpose submarines; intended as a second – strike, retaliatory weapon
Burevestnik Nuclear Powered Cruise Missile	Nuclear	*Unlimited* range, owing to its nuclear reactor; intended to overcome missile defense
Kinzhal Air – Launched Ballistic Missile	Conventional or nuclear	Intended to target naval vessels
Tsirkon Hypersonic Cruise Missile	Conventional or nuclear	Intended to attack ships and ground targets
Barguzin Rail – Mobile ICBM	Up to 4? Nuclear	Program reportedly postponed in 2017
RS–26 Rubezh ICBM	Up to 4? Nuclear	Program reportedly postponed in 2018

Извор: Woolf, 2021, p. 20.

Руска Федерација распоређује своје стратешке нуклеарне снаге у више од десет база (*Слика 13*) широм своје територије. Руска Федерација тренутно модернизује (спроводи у више сегмената развој како информационих тако и других технологија неопходних за спровођење војних програма у развоју наменске индустрије РФ) већину компоненти своје нуклеарне тријаде, која је почела 1998. године. Савез Совјетских Социјалистичких Република је често мењао своје копнене ракете, са новим системима, а модификације су се појављивале сваких неколико година. Руска Федерација није одржала овај темпо, већ се посветила повећању прецизности, ефикасности и можемо слободно рећи ексклузивитету модернизованог или новоразвијеног пројекта који би умањио или потпуно поништио све постојеће системе заштите у тој области (Woolf, 2021).

Слика 13. Базе стратегијских снага РФ.
Извор: Woolf, 2021, p. 14.

САД још увек нису успеле да развију, самим тим ни да инсталирају, системе одбране од балистичких ракета које би биле у могућности да изврше пресретање стратешких балистичких пројектила, ракета оружаних снага РФ. Министарство одбране САД је 2019. године у свом извештају навело да се првенствено ослања на одвраћање по питањима заштите од интерконтиненталних балистичких ракета (како руских тако и кинеских). Руска Федерација није ово прихватила као коначно решење САД према овом питању и сматра да ће САД развити и распоредити пресретаче противракетне одбране са способностима потребним да се супротставе пројектилима РФ. Тако, РФ сматра да ракета *Авангард* представља нови изазов за САД, јер противракетна одбрана не може да пресретне ову ракету. Поред ових ракета, систем који је можда највише узбуркао јавност у 2019. години поставља питање где су границе развоја нових технологија и њиховог коришћења у војне сврхе, односно у одвраћању великих сила од нежељених намера. Руска Федерација је развојем *Посејдона*, подводног дрона или подморнице без посаде или система који се креће попут торпеда са невероватним техничким карактеристикама огромне брзине кретања, велике дубине кретања, великог домета, а поготово ефекта на циљу где би активирањем *Посејдона* са нуклеарном бојевом главом у приобаљу САД довео до стварања цунамија са високим таласом од ког би били уништени читави градови и шире. Не треба заборавити ни учинак радиоактивности као ни других ефеката. Међутим, ово средство није ништа мање опасно ни са конвенционалним бојевим главама, за које би могло да пронађе употребу за мање ефекте (уколико можемо да кажемо да је пар хиљада припадника оружаних снага и невероватно висока цена наоружања и друге војне опреме мањи ефекат), нпр. за супротстављање носачима авиона који, као што нам је добро познато, плове увек у пратњи великог броја бродова ратне морнарице који се користе за његову заштиту и уједно подршку у извршењу задатака, што би значило њихово тренутно уништење (Telegraf.rs, 2019).

Развој и модернизација система наоружања и друге војне опреме доводе до врло брзих промена у концептима одвраћања, али и до заустављања (избацивања из употребе) читавих серија система за одбрану, за напад, услед превазиђености, појавом нових технологија, које су често из *субјективних* разлога (једноумља које влада у свим великим системима и самим тим тромости која је у њима присутна) и *објективних* разлога (огромна финасијска средства неопходна за улагање у развој) довеле до неопходности ангажовања државног стратешког менаџмента у изналажењу решења (што најчешће као обавезу добијају службе безбедности). Све ово се предузима од стране стратешког менаџмента како би се премостио јаз до сустизања других у развоју нових технологија. Подсетићемо само на неколико случајева где може да се постави питање сврсисходности улагања огромних новчаних средстава у набавку одређених средстава и опреме наоружања, система: обарање невидљивог бомбардера авиона стелт технологије *Ф117* (током агресије Североатлантског савеза 1999. године на Савезну Републику Југославију); употреба дронова у ликвидацијама високих државника (Ирак); затим улазак у оперативну употребу са високим маневарским могућностима хиперсоничних ракета (РФ); да ли је и потапање крстарице „Москва" био епилог дејства ракете Нептун која је од 2021. године у оперативној употреби њена модернизована варијанта или не, и други низ примера, а што би само један квалитетан развојни пројекат нове технологије могао да доведе до немогућности да се неко оружје, систем уопште, више користи у употреби. Након догађаја у Украјини 2022. године, неизбежно је да ће се стратешки државни менаџмент великог броја држава укључити у трку за поседовањем најновијих технологија или развоју већ постојећих, ради одвраћања других држава и већим финансијским улагањима у наоружање и војну опрему (Немачка – политичари најављују једнократно 100 милијарди евра улагања одмах – 2022. године, а да не вршимо даљу анализу и Република Србија – стратешки државни менаџмент најављује куповину првенствено средстава најновије технологије). Већа количина новца може утицати на брзину напретка одређених технологија, али није могуће све решити толико брзо (најаве Немачке и Србије се у делу предвиђених набавки могу реализовати ако све буде како треба тек до краја 2030. године), односно реализовати у временски кратком року, поготово послове у сфери развоја наоружања и опреме (или куповине) где су процедуре испитивања и развоја јако дуге, али зато се тај недостатак надокнађује ефикасним реаговањем стратешког државног менаџмента, ангажовањем служби безбедности, првенствено у домену примене необавештајних активности (Марјановић, 2022).

У водећој компанији задуженој за израду наоружања и војне опреме у РФ, *Rosoboronexport*, можемо констатовати читав низ нових система, где бисмо између осталих за одвраћање у ваздушним снагама посебно истакли следеће: ваздушно – извиђачки комплекс са беспилотним летелицама великог домета – *Orion–E*, мултифункционални комплекс са беспилотним летелицама – *Orlan–10E*, комплекс са беспилотним летелицама – *Tachyon*, исправљена ваздушна бомба са ласерском главом за навођење и високоексплозивном фрагментационом бојевом главом – *KAB–250LG–E*, вођена ваздушна бомба – *KAB–500Kr, KAB–500–OD* и др. У копненим снагама: противтенковски ракетни систем – *Kornet–E, Kornet–EM*, противтенковски ракетни систем *9K115M1–Metis–M1*, самоходна хаубица калибра 152 мм са аутоматским системом навођења и управљања ватром *ASUNO – Msta – S*, модернизована самоходна хаубица за калибар 155 мм–*Msta–S* и читав низ других средстава наоружања и војне опреме (Rosoboronexport, 2022). Све ове системе је

неопходно усклађивати не само са најновијим достигнућима, већ са могућим начином употребе – екстремних средстава која и нису толико скупоцена, високософистицирана, борбена, масивна, где се поново човек и његове визије употребе средстава враћају у центар збивања као кључни елемент одвраћања.

8. ЗАКЉУЧНА РАЗМАТРАЊА

Спроведено истраживање на тему одвраћања као стратешког концепта у постхладноратовском периоду, након уводног разматрања и методолошког оквира истраживања реализовано је кроз *пет поглавља* у којима су дати одговори на постављена истраживачка питања. Ради прегледности и лакшег праћења, у наставку рада ћемо у систематизованој и сублимираној форми дати преглед закључака до којих смо дошли.

Прво поглавље је посвећено концепту одвраћања великих сила у периоду након Хладног рата. У овом делу рада су обухваћене две велике силе, САД и РФ. У овом поглављу су дати одговори на прво и друго истраживачко питање – који су концепти одвраћања присутни код великих сила у периоду након завршетка Хладног рата и како су они артикулисани кроз стратегијско – доктринарне оквире и на који начин је убрзани техничко – технолошки, а посебно развој информационих и телекомуникационих технологија, утицао на промене у стратегијама одвраћања великих сила након завршетка Хладног рата. Прегледом научне и стручне литературе и анализом садржаја утврђено је да су у дефинисаном периоду присутна два различита концепта одвраћања – један у САД, а други у РФ. Ови концепти утврђени су стратешко – доктринарним документима који су, услед брзог развоја информационих и телекомуникационих технологија, врло често доводили до промена у садржају и обиму овог појма. Развој информационо – комуникационих технологија захтевао је измену стратешких и доктринарних докумената, њихово ажурирање, у циљу прилагођавања новонасталим околностима.

Истраживањем су биле обухваћене две групе индикатора. *Прву групу индикатора* (који обухватају, између осталог, прво и друго истраживачко питање) су чинили одвраћање у постхладноратовском периоду, које је истраживано кроз идентификацију стратегијских докумената који регулишу одвраћање и промене које доводе до нових концепата у одвраћању, као и поступци, па и промене делова система безбедности услед развоја нових технологија и билатералних односа држава након интервенција служби безбедности. Тако су САД од краја Хладног рата па до данас донеле велики број стратегијских докумената који се на посредан и директан начин односе на одвраћање. Ради се о следећим документима: доктрине председника (1992, 2001, 2009, 2017, 2021), стратегије националне безбедности (1999, 2006, 2017), национална одбрамбена стратегија (2018), националне војне стратегије (1989, 1992, 1995, 2004, 2011, 2015, 2018). У истом периоду, РФ је усвојила следећа документа: стратегију националне безбедности (2009, 2015, 2021), војну доктрину (2010, 2014), Закон РФ о безбедности (1992, 1993, 2002, 2005, 2006, 2007, 2008). Конфронтација ове две силе уз избегавање директног оружаног сукоба изискује редефинисање постојећих стратегија, доктрина и других докумената који треба да пруже одговор о новом начину одвраћања. Повећана друштвена зависност од нових технологија доводи до увећања претњи по безбедност држава новим облицима угрожавања и изворима претњи. Истраживањем теорије у САД идентификована су посебна обележја одвраћања која карактеришу овог

актера. Извештај сопствених војних служби безбедности о противнику је најважнији вид информисања дипломатске комуникације. То наводи и на питања изненађења и непостојања ваљаних података или лоше координације служби безбедности везано за нападе у САД које су покренули *недржавни* актери 11/09, што је довело до стратешког изненађења и неуспеха у одвраћању. Несигурност у погледу одвраћања се надокнађује што реалнијим вежбама (увежбавањима што већег броја учесника) на свим нивоима. На одвраћање су утицали и други развоји, како технолошки тако и идеолошки. С једне стране, то је повећана прецизност у стратешком оружју и размештање интерконтиненталних балистичких ракета са конвенционалним бојевим главама, а са друге, развој стратешких способности сајбер напада је представљао значајан основ за редефинисање актуелног концепта одвраћања. Промене у овом концепту приметне су у односу на тероризам, затим сферу сајбер безбедности (уопште нових технологија), принуду, истраживачке центре, као и одвраћање у контексту хибридног сукоба и конкуренције сивој зони. Време спровођења одвраћања често је суштинска спутавајућа категорија, од момента издавања задатка за употребу одређене врсте оружја/оруђа/ средстава до његовог дејства на циљ. Велике силе користе широку лепезу војних и невојних активности у сврху принуде (економски притисак, кампању дезинформисања, подстицање политичке корупције, шпијунажу, обезбеђивање оружја опозиционим групама, поларизовање домаћих дебата у циљним земљама, сајбер напади и др.). Тако су аналитичари на *Западу* изнедрили још један нови појам и то *Одвраћање од више домена* (енг. *Cross – domain deterrence,* чиме се увеличавају фактори успешности одвраћања који укључују и комуникацију – *информациони домен*, веродостојних претњи наметањем трошкова – *економски домен*, као и снажне политичке воље – *политички домен* и др.). Можемо да закључимо да је Џорџ Ф. Кенан (*George F. Kennan*), који је назвао акције попут саботаже, дезинформација и мере политичке дестабилизације *мере без рата* (енг. *measures short of war – MSW*), најсвеобухватније одредио мере и активности које се предузимају у „сивој зони" осим конвенционалног или нуклеарног рата високог реда. *Непријатељске мере* (енг. *hostile measures*) је најадекватнији термин, будући да обухвата категорије *тајних или прикривених активних мера* (енг. *clandestine or covert active measures* – што би било најприближније делатностима које је Кенан настојао да опише), односно *активних мера* (енг. *active measures* – термин коришћен у хладноратовском периоду на Истоку, Савез Совјетских Социјалистичких Република) или *мере подршке*[125] (термин коришћен у постхладноратовском периоду у РФ), односно *необавештајних активности* (термин коришћен у Републици Србији). Ради се о државним активностима осим конвенционалног или нуклеарног напада високог реда примењене против других држава (ентитета) у било ком тренутку и у било ком контексту, са непријатељском намером да стекну своју предност и смање способности, стабилности или предности друге државе (ентитета). Мере које нису ратне се генерално схватају као акције једне државе против друге државе (или више држава или савеза), које се обично спроводе у *сивој зони*. Термини *сива зона* и *хибридни рат* су популаризовани након интервенције РФ на Крим 2014. године. *Сива зона* је простор између потпуног неангажовања и избијања рата високог реда, а термин *хибридни рат* (енг. *hybrid warfare*) се генерално приписује Франку Г. Хофману (*Frank G. Hoffman*) и можемо закључити да оно што САД

[125] Према изјави Јевгенија Примакова (старијег), директора службе безбедности – СВР, 1991–1996. године, РФ.

назива хибридним ратом то обухвата концепт стратешког одвраћања у РФ, односно руском способношћу за принудом.

Истраживање је показало да је једна од битних карактеристика на стратегијском нивоу препознавање облика одвраћања, па затим активности које би уследиле у поступању надлежних лица, целина, компанија, институција, према стратешким документима САД у одвраћању. Клинтонова доктрина потенцира да тамо где су вредности и интереси САД у питању, и где могу, ту се мора бити спреман за деловање. Буш је наступао са доктрином „ја одлучујем и одлучујем шта је најбоље". Стратегија *превентивних удара* као одбрана од непосредне или претпостављене будуће претње безбедности САД имала је два циља – амерички примат и превентивни рат. Евидентно је да се Обама залагао за избегавање међународних заплета осим ако нису били апсолутно витални за америчке националне интересе. Мајк Помпео (*Majk Pompeo*) је изјавио да је Касем Солејмани (*Kasem Solejmani*) убијен у склопу шире стратегије одвраћања претње коју представљају непријатељи САД, која се односи и на Кину и Русију, ублажавајући тиме тврдње да је највиши ирански генерал убијен, јер је планирао нападе на америчка дипломатска представништва (Lamarque, 2020). Председник Доналд Трамп је рекао да су међу потенцијалним циљевима тих напада четири америчке амбасаде, а министар одбране Марк Еспер (*Mark Esper*) је изјавио да није видео никакве обавештајне податке који би упућивали на могуће нападе на дипломатска представништва. Трамп је поново *долио уље на ватру* рекавши да „заправо и није битно" да ли је Солејмани представљао претњу (Lamarque, 2020). Помпео је рекао да се иза убиства иранског генерала крије „шира стратегија" (део те стратегије, на основу ових закључака можемо слободно констатовати, представља и *обмана* на стратегијском нивоу ради изазивања одређене интервенције, *убиства, бомбардовања*, да би после одређеног времена, било демантовано или не, а тада то више никога и неинтересује). *Национална стратегија одбране САД* из 2022. године је увођењем *интегрисаног одвраћања* и давањем приоритета у одбрамбеној политици велике силе као што су САД на одвраћању у два приоритета (од само четри која је поставила стратегија одбране САД из 2022.) истакла значај одвраћања. Поред тога, за ову стратегију је интересантно нагласити представљање *сиве зоне* односно како се у стратегији наводи *активности у сивој зони* где наступа углавном присила ради остварења циљева постављених од руководства државе, где већи део ових и сличних активности предузимају или у њима учествују службе безбедности државе углавном предузимајући необавештајне активности. Поред примене силе као крајње одреднице *Националне војне стратегије* у САД, други део који одређује поменуту стратегију чини претња силом, односно терање, приморавање непријатеља, противника или његовог савезника на одвраћање. У мају 2002. године ставља се већи нагласак на нови стратешки концепт, *напред одвраћање* са обележјима глобалне способности у додатном ангажовању на прекоморском прикупљању обавештајних података, прикривеним специјалним операцијама, беспилотним ваздушним возилима, сајбер ратовањем, хиперсоничним ракетама и способношћу спречавања противника од ометања америчке комуникационе и обавештајне имовине у свемиру и удара у подземне циљеве. Национална војна стратегија из 2004. године у САД је предвидела побољшање не – нуклеарних способности напада, информационе операције, командовање и управљање, обавештајне и свемирске снаге где ће све побројано допринети да способност одвраћања буде робуснија и ефикаснија. Национална војна стратегија из 2011. године у САД је предвидела *недржавне актере*, где поред државних и недржавни актери

додатно усложњавају одвраћање и одговорност ширењем њиховог досега кроз напредне технологије које су некада биле искључиво домен држава. Национална војна стратегија из 2015. године је специфична по званичној намери наношења економских трошкова непријатељу где своју *супериорност у економији* САД поставља као један од доминантних, чак и војних задатака у одвраћању непријатеља од нежељених намера САД. Интересантан је још један пример одвраћања. Израелска Стратегија одбрамбених снага (највероватније по узору на САД) наглашава да ће акције које треба да одврате непријатеља бити спроведене у оквиру *Кампање између ратова* (енг. *Campaign between wars – CBW*).

Истраживањем је утврђено да актуелна теоретска разматрања везана за концепт одвраћања у РФ и стратешких докумената који прописују одвраћање имају следећа обележја.

У вези са потврђивањем одговора датих на истраживачко питање, истраживање је указало да је важно напоменути да је у некадашњем Савезу Совјетских Социјалистичких Република постојао концепт који је називан *маскировка* и подразумевао је концепт и активност маскирања (прерушавања, обмане) у којем учествује цели народ. Веома је тешко уопште превести ову реч – маскировка, јер у енглеском језику би обухватила најмање десет речи (на пример, камуфлажа, прикривање, обману, дезинформације...). Инструменти који су коришћени у овом концепту маскировке су дипломатија, информисање, распоређивање оружаних снага и економске мере. *Стратешко одвраћање* према мишљењу Министарства одбране РФ представља координирани систем војних и невојних (политичких, дипломатских, правних, економских, идеолошких, научно – техничких и других) мера предузетих узастопно или истовремено, све са циљем одвраћања војних акција које повлачи за собом штету стратешког карактера. Компоненте концепта, односно његове делове, чине: нуклеарно одвраћање, ненуклеарно одвраћање и невојно одвраћање. Анализом најбитнијих сегмената *Стратегије националне безбедности РФ* из 2009. године, можемо констатовати да се *стратешко одвраћање* у РФ поред развоја и опремања нуклеарним и офанзивним наоружањем као тежишним мерама одвраћања, спроводи и најбитнијим сегментом стратешког одвраћања које обухвата политичке, војне, војно – техничке, дипломатске, економске, информационе и друге мере. Стратегија националне безбедности РФ из 2009. године, зановљена 2015. године је изузетно квалитетно предвидела тренутно актуелне догађаје на планети, почев од проблема са Украјином, затим сајбер и војне претње, економске кризе и друге претње. *Стратегија националне безбедности РФ* из 2021. године препознаје одвраћање кроз спровођење војне политике стратешким одвраћањем где ће поред оружаних снага РФ бити ангажоване и друге трупе, војне формације и органи (овде препознајемо приватне војне компаније као и све остале потребне државне и недржавне институције, организације, фирме и слично). Наглашена је потреба одржавања довољног нивоа способности (између осталих) и нуклеарног одвраћања. *Војна доктрина РФ* прописује војне мере заштите националних интереса земље и интереса својих савезника тек након исцрпљивања могућности коришћења *политичких, дипломатских, правних, економских, информативних и других инструмената ненасилне природе*. Суштина одвраћања према војној доктрини се у делу сегмената доста подудара са Стратегијом националне безбедности РФ, али и наглашава ненуклеарно одвраћање као и друге инструменте ненасилне природе. Многи западни аналитичари заокупљени су тиме да РФ планира операције *хибридног ратовања* против чланица Северноатлантског савеза, међутим, у Војној доктрини РФ сам термин *хибридни рат* није део руске војне доктрине. Када се изјашњавају руски аналитичари,

за њих је *хибридни рат* западна конструкција док је у Стратегији националне безбедности и у академској расправи у употреби шири концепт *стратешко одвраћање*. Овај концепт је део званичне стратегије и битан је за анализу садашње и будуће безбедности и одбрамбене политике РФ. Можемо закључити да је *стратешко одвраћање* концепт који обухвата оно што други називају доктрином *хибридног ратовања* РФ, руску способност за принуду. Руска Федерација препознаје амерички војно – технолошки напредак и балистичко – ракетну одбрану као кључне претње, па се наведено доживљава као поткопавање руских стратешких нуклеарних снага. Невојне претње руској безбедности су све распрострањеније, опасније, невидљивије и делотворније по угрожавање националне безбедности државе. Претње се јављају у информативној и културној сфери (супротстављање дезинформацијама, *фалсификовање историја*, подривање историјске, духовне и патриотске традиције на пољу одбране државе и др.), као и информационо – телекомуникационој сфери (сајбер напади и др.). Савремени рат све више бира невојна средства за сукобе између држава.

Из такозване доктрине Валерија Герасимова, Начелника Генералштаба оружаних снага РФ закључујемо да отворена употреба оружаних снага, неретко под плаштом очувања мира и регулисања кризе јесте примена само у одређеној фази, ради постизања крајњег тријумфа у сукобу. Анализом ове изјаве изводимо закључак да све оне фазе (да ли их назвали непријатељске мере, тајне акције, активне мере, необавештајне активности) до момента отпочињања оружаног сукоба високог реда, представљају најбитнији моменат у предузимању спољнополитичких мера за долазак до реализације државних циљева и припреме за коначну реализацију циљева, најчешће оружаним снагама државе.

Постхладноратовски период је обележио један велики *земљотрес* на светској сцени, а реч је о *нестанку једне суперсиле* – Савеза Совјетских Социјалистичких Република 1990. године и опстајања само једне суперсиле на планети – САД. Овај период, после 1990. године, карактерише хегемонија САД – предузимање низа *једностраних одлука, поступака, интервенција, агресија* према другим државама, без одобрења Уједињених нација. Ти поступци САД у постхладноратовском периоду су представљани углавном као део одвраћања од недозвољених делатности, а у ствари су врло често представљали *комбиновану примену обмана, дезинформација, информационих операција* и других необавештајних активности, правно неодобрених од стране Уједињених нација, а које су САД предузимале према другим државама, све са циљем правдања нелегитимних поступака. Доласком Владимира Путина на власт, *РФ се враћа у категорију велике силе* (део теоретичара сиријски сукоб види као моменат завршетка овог процеса), што је постигнуто првенствено смањењем корупције, затим наглим развојем економије РФ, успостављањем јединства са исламским светом, након чега се епицентар светске моћи из САД помера према РФ, односно према Истоку. Свака прерасподела, односно *померање центра моћи великих сила доводи до нестабилности*, несигурности у спољнополитичким односима због чега је повећана вероватноћа доласка до извесних сукоба. Неслагање које се јављало између ове две велике силе је друга страна покушала увек да надомести паметнијом и квалитетнијом употребом служби безбедности са посебним освртом на њихову примену необавештајних активности.

Од *другог до петог поглавља* спроведеног истраживања дати су одговори на *треће, четврто и пето истраживачко питање* (која су општа, посебна и специфична обележја необавештајних активности у савременим околностима обликованим развојем информационим и телекомуникационим технологијама, затим како су се трансформисале

службе безбедности зарад реализације савременог концепта одвраћања и на који ће начин концепт одвраћања утицати на креирање безбедносних политика националних држава у блиској будућности). На основу истраживања промена које су настале од периода Хладног рата до данас, у погледу развоја информационо – телекомуникационих технологија, дипломатије, људског друштва, анализирано је како су ове промене утицале на начин одвраћања држава, организација, појединаца, и описане су опште карактеристике савремених начина употребе служби безбедности. Службе безбедности су сагледане кроз необавештајне активности у зонама где су се догађале информационе операције и друге необавештајне активности, о чему сведочи велики број научних истраживања насталих на овим темама. Сагледана су општа, посебна и специфична обележја необавештајних активности и константна присутност (број, интензитет присутности) служби безбедности у спровођењу стратегија одвраћања, студија случаја информационих операција у Естонији, Криму и Украјини. Наведено нам даје одговор на питање каква је била улога служби безбедности у реализацији савременог концепта одвраћања, а каква је улога служби безбедности данас. Велика активност офанзивних служби безбедности кроз пропагандне, политичке, економске и паравојне активности условила је промене у стратешко – доктринарним документима националних држава и дала је нови правац у одвраћању. Сајбер напад, сајбер простор, диктира и диригује промене у стратегијама и доводи до израде нових стратегија. Истраживање је спроведено кроз *другу групу индикатора* коришћених у овом истраживању, а коју су чиниле активности служби безбедности у одвраћању, посматране кроз политичке, пропагандне, паравојне, економске, као и информационе активности (операције).

Друго поглавље се бави основним појмовним одређењима служби безбедности, као и активностима којима се баве службе безбедности с фокусом на значају обавештајне, контраобавештајне и необавештајне активности. С тим у вези, начин прикупљања података и оперативни рад служби безбедности су сагледани од појмовних, теоретских одређења, до практичних делатности у реализацији одвраћања. Спроведено истраживање је дало одговоре на истраживачко питање и потврдило полазну претпоставку да је однос политике, дипломатије и служби безбедности у спрези приликом планирања, организовања и спровођења активности одвраћања. Имајући у виду значај националних интереса, посебно је анализирана спрега дипломатије и обавештајних активности, као и специфичности које овакве активности носе у активности одвраћања.

Спроведено истраживање је дало одговоре на постављено истраживачко питање о улози служби безбедности у реализацији активности одвраћања великих сила. На основу обављеног теоријског истраживања установљено је да *терминологија* која се користи на Западу *није усаглашена* са оном која се употребљава на Истоку, и то за велики број истих појмова/тема/области, као и за сегмент рада служби безбедности односно активности које предузимају, где је на Западу једна врста одређења, док је на Истоку друга врста поимања исте или сличне појаве/сличних појава. У Републици Србији је у употреби посебна терминологија. Превођење, некада само једне речи, коришћене на истоку (рус.) у западну (енг.; односно англосаксонску) терминологију, представља немогућу мисију (нпр. руска реч *маскировка* се у енглеском језику описује са десет одредница које и поред тога не обухватају у потпуности садржај дефиниендума) и обрнуто (нпр. енглеску реч *intelligence* у другим језицима није могуће превести без великог броја других речи, сложеница). Изводимо констатацију о комплексности изучаване материје са терминолошког и језичког аспекта.

На основу обављеног теоријског истраживања о ангажовању служби безбедности РФ, радне групе формиране у Великој Британији, па и у САД *нису успеле да дођу до заједничког појмовног одређења активних мера, па нема ни коначне класификације* већ само оквирне. Тако за службе безбедности у САД постоје само најфреквентније области ангажовања (политичке, пропагандне, економске, паравојне, сајбер и друге) у којима се најчешће примењују ове активности служби безбедности и/или других структура ангажованих у реализацији задатака добијених од политичког врха државе.

Наиме, поред тога што се дугорочним планирањем у циљу остваривања одређених циљева предвиђају одређена нежељена дејства, део истих које нису предвиђене се најчешће појављују као претње створене од непријатељске службе безбедности. Тако је једна од претњи била и она коју је у свом обраћању медијима навео председник Републике Србије, дана 10. октобра 2022. године, када је обелоданио сазнања да је више пута извршен покушај саботаже турског тока – гасовода и да би његовим евентуалним оштећењем Република Србија била одсечена од допремања ове врсте енергента, па је служби безбедности Републике Србије – Безбедносно – информативној агенцији, дат задатак спровођења безбедносне заштите ове врсте, инфраструктурног објекта од посебног значаја за државу. Ова изјава говори о озбиљности сагледавања необавештајних активности страних служби безбедности не само између великих сила, већ и према малим државама и да је једино исправно супротстављање тајним делатностима ангажовањем службе безбедности угрожене државе. Ово није прва претња за коју је председник Републике Србије јавно објавио да је ангажована служба безбедности у супростављању „невидљивим" непријатељима (између осталог и током борбе са *COVID–19* и другим).

Необавештајне активности могу се спроводити у склопу обавештајних (или паралелно са њима), или контраобавештајних активности, односно служби безбедности обавештајног или контраобавештајног карактера. Углавном се разлика у деловању своди на то да ли се предузимају активности офанзивног карактера или дефанзивног, као и да ли се ради о тежишно иностраном деловању или деловању у земљи.

У трећем поглављу је направљен посебан осврт на необавештајне активности и информационе операције као врсте активности у којима учествују или које предузимају службе безбедности. Спроведено истраживање је дало одговор на постављена истраживачка питања са садржајем детаљног објашњења појмовног одређења необавештајне активности у научној и стручној литератури у САД и РФ. Поред бављења овим двема великим силама, истраживање даје одговор о садржајима које обухватају необавештајне активности у Републици Србији, са нагласком на проблему различитих појмовних одређења истих или сличних активности у наведеним државама. Објашњена је веза између необавештајне активности и информационих операција. Такође, описане су и класификоване и друге сфере необавештајне активности: *пропагандне активности, политичке активности, економске активности и паравојне активности*. У свакој од наведених сфера необавештајне активности данас значајно место заузима сајбер простор у коме се спроводе информационе операције. У том смислу, сагледано је традиционално схватање необавештајне активности и, насупрот њему, савремено схватање које посебан нагласак ставља на информационе операције као на средство за спровођење необавештајних активности. У овом поглављу су представљене и нове теорије које се баве односом информационих операција и необавештајних активности. Оно што је неизбежно у сагледавању ових појава јесу и етичка

питања употребе необавештајне активности, како у традиционалном облику, тако и путем информационих операција.

Спроведеним истраживањем су највећим делом дати одговори на постављена истраживачка питања где је у сукобу РФ и Украјине, односно можемо слободно констатовати РФ и Североатлантског савеза, посредно, сукоб *информационим операцијама доживео врхунац* – од сиријског праћења сукоба, информациона операција доведена је до водеће или главне активности у сукобу, а кинетичке снаге су биле помоћне снаге у реализацији операције (случај Крим). *Употреба дезнинформација* на свим нивоима, на дневном нивоу је толико била присутна приликом оружаног сукоба РФ и Украјине, да је крајем 2022. године један догађај могао изазвати директни сукоб између РФ и Североатлантског савеза. Радило се о дејству ракетама оружаних снага Украјине на територију Пољске, када су страдала два пољопривредника, а овај догађај је председник Украјине (Зеленски) представио као деловање оружаних снага РФ. Овај догађај је у потпуности подсетио на сличне догађаје примене дезинформација на простору Ирака, Ирана, затим Балкана, почев од догађаја на пијаци Маркале у Сарајеву, БиХ, Сребренице у БиХ, етничког чишћења српског народа из Републике Хрватске, Крајине – операција „Олуја", догађаја у селу Рачак, КиМ, Република Србија и других догађаја. Често су овакви догађаји искоришћени као повод за незаконито и неправедено бомбардовање, интервенцију, учествовање у *паравојним активностима, пропагандним, политичким и коначно економским активностима*. Овај догађај је наведен само као један пример у Украјини, а било је низ покушаја обмана.

С тим у вези, истраживање је показало да је једно од најбитнијих обележја, уназад пар деценија, у раду служби безбедности, ангажовање *агената од утицаја.* Уз високу корупцију, агенти од утицаја представљају једну од највећих претњи државама, данас и у будућности. Претња достиже врхунац постављањем таквих агената на руководећа места у систему безбедности, на стратегијском нивоу, односно у држави уопште. Разлог је једноставан, тада институције које се требају супротстављати недозвољеним делатностима долазе под руководство агената од утицаја и тиме уместо да се боре против агената од утицаја, почињу радити за њих. Карактеристичан је пример из 1991. године, када је председник државе, тада СССР, издао налог директору КГБ за уништењем КГБ.

Поред тога, евидентно је да су *дезинформације* које експлоатишу друштвени медији врло битна техника, инструмент одвраћања. Када говоримо о отпорности једног друштва, никако не можемо да не сагледамо све технике које су примењиване у реализацији неког догађаја и то да не проверавамо тако што ћемо потврђивати један исти податак, преко различитих медија/извора (мислећи да смо тако проверили податак) који су на једном платном списку, једне организације, службе безбедности – државе као неког крајњег невидљивог корисника. То су честе замке које се могу врло лако подвести под добро припремљену дезинформацију. Главна одлика сваког друштва у повећању отпорности (енг. *resilience*) би требало да буде повећање знања и способности свих грађана, поготово лица на руководећим дужностима у државним и приватним институцијама, у препознавању и супротстављању претњама националној безбедности.

Истраживање је показало да је агенција под називом *УСИА* (енг. *United States Information Agency – USIA*), основана од стране САД 1953. године и наводно укинута 1998. године (бар под овим називом и у овом облику), била стратешка комуникацијска агенција

која је укључивала средства емитовања и јавну дипломатију. *УСИА* је давала правац стратешке комуникацијске политике, а све наводно ради стварања боље слике о САД, првенствено у иностранству. С тим у вези, ова агенција се бавила остваривањем интереса САД и њених савезника, између осталог и за окупљање заинтересованих страна из извршне власти за супротстављање *активним мерама* усмереним према САД, што је био сукоб, необавештајним активностима вођен од стране РФ путем информационих операција[126].

Најзад, спроведено истраживање је потврдило да након препознавања важности коју носи претња коју одређујемо као лажна информација, дезинформација, као једна од мера супротстављања САД овом феномену је формирање целине која је састављена од научника и стручњака из области комуникација великих података и других експерата са сврхом откривања, разумевања и ефикасног разоткривања дезинформација и лажних наратива, што може бити један од модела одвраћања, лажним информацијама.

Имајући у виду значај националних интереса, постхладноратовски период одвраћања је обележио и интензивну појаву *мултинационалних операција* – МнОп од стране Североатлантског савеза (колективног одвраћања), где је под покровитељством принудне дипломатије вршено убеђивање, присила над сукобљеним странама, односно да будемо прецизнији – *према непослушној страни*.

С тим у вези, истраживање указује на честу појаву немогућности поштовања закона и других норматива у ангажовању служби безбедности ове природе где су ангажовања углавном недозвољеног, незаконитог карактера за лице, организацију, државу (ентитет) према којој (коме) се предузима, док за државу која предузима ове активности спада у низ одобрених мера одвраћања од матичне државе.

Четврто поглавље је представило резултате истраживања о месту и улози служби безбедности у конкретним случајевима сајбер напада, посматраних у парадигми необавештајних активности служби безбедности. Анализирани су сајбер напади на Естонију (2007. година), обмана приликом анексије Крима 2014. и сајбер напад на Украјину 2017. године. У наведеним студијама случаја су анализиране карактеристике и посебности примене сајбер напада у оквиру извођења акција служби безбедности. У овом поглављу су представљена искуства у примени сајбер напада од стране служби безбедности и анализиране неопходне нове мере безбедносне заштите критичних информационо – телекомуникационих система држава и савеза.

Сумирајући хронологију догађаја приликом реализованих *сајбер напада у Естонији* могу се констатовати следећи закључци. *Први*, да је РФ наведену операцију спровела као одмазду због покушаја мењања историјске улоге руског народа у Другом светском рату и уједно практичну проверу сајбер способности за предстојећи напад на Грузију. *Други* закључак, да је контролисани учесник можда био управо онај ко је дириговао Влади Естоније померање споменика. Чињенице које потврђују овај закључак су следеће. Влади Естоније померање споменика је могао *наредити* само ментор, а то није РФ. Најчешће се онај који направи проблем појављује и као страна која решава исти тај проблем. Формирање центра за сајбер одбрану од стране Североатлантског савеза представља битан моменат са личним присуством стручних лица из Североатлантског савеза у центру у Естонији. Затим имамо

[126] Служба безбедности Савеза Совјетских Социјалистичких Република – КГБ је водила део кампање, операције дезинформација чији је циљ био дискредитовање САД на међународној сцени под називом *Инфекција*.

судско процесуирање само једне особе са казном која је представљала мали новчани износ, где се оптужује велика сила, РФ, за спровођење сајбер напада на државу. Следи и сувише јаван наступ са борбом за споменик, руским заставама, заштитом руских интереса.

Спроведено истраживање је највећим делом потврдило специфичности избора Крима за анализу, јер представља комбинацију физичких и сајбер напада на структуру информационо – телекомуникационих структура у Украјини (сајбер простор), посебно (физички и сајбер простор) на Криму. Специфичност чини и формирање групе енг. *Cyber Berkut* – наводно добровољна анонимна група појавила се након распуштања снага безбедности *Беркут* у Украјини крајем фебруара 2014. године и она је проруска, док њеног *близанца* непријатеља у Украјини представља група енг. *Cyber Hundred* која је вршила циљане сајбер нападе, мада су регистроване и друге наводно недржавне групе. Одржавање Олимпијских игара у Сочију је искоришћено за концентрацију великих оружаних снага РФ у близини Крима без *аларма* на Западу и географска и културна близина Крима је погодовала РФ за заузимање полуострва.

Истраживање је указало на тактике коришћене у операцији *Армагедон*, где је *Lookingglass* известио о шаблону у нападима почевши од распршивања циљаних енг. *spearphishing emails* стратегија које се нису користиле ни у Естонији ни у Грузији, постављајући нову форму напада који је развила РФ. Поред тога, неке корисне поруке током операције биле су облици малвера за даљински приступ (енг. *RAT – Remote Access Trojan*), врсте малвера који има могућност даљинске контроле система, преко удаљене мрежне везе. У случају Украјине, коришћен је систем манипулатора, а антивирусна индустрија га је класификовала као злонамерног. Ови малвери за даљински приступ су коришћени за добијање информација током украјинско – руског сукоба. Сукоб на терену заједно са замахом сајбер напада и малвера за даљински приступ можда је био разлог зашто сајбер напади трају много година. Показало се ефикаснијим од напада у Естонији и Грузији. Преговарање колега из оружаних снага РФ са колегама из оружаних снага Украјине на Криму, ради предаје својих целина оружаним снагама РФ и избегавања проливања крви представља једно од битних обележја ове анексије. Грешка Владе Украјине о распуштању јединице Беркут је помогла РФ да на терену регулише све спорове са становништвом ангажовањем управо њених припадника.

Поред тога, евидентан је један од најозбиљнијих сајбер напада РФ на Украјину који се догодио 2017. године, када је вирус *NotPetia* пуштен у компјутерске мреже Украјине. Спроведена је серија сајбер напада на веб странице организација из Украјине на: банке, владина министарства, новине, електропривреду и државна предузећа као што су Међународни аеродром Бориспил, Укртелеком, Укрпошта (поштанска служба), Државна штедионица Украјине и Украјинске железнице. Праћење радијације у нуклеарној електрани Чернобил је било искључено овим сајбер нападом.

С обзиром да је у оружаним сукобима циљ стратешка парализа непријатеља, то се постиже циљањем на виталне тачке у држави што је постигнуто оружаним путем, економским активностима, циљањем информационих центара или дипломатским активностима, присила да се одређени поступци реализују или одвраћање силом чиме се ствара доминација једне стране у сукобу.

Спроведено истраживање је потврдило да сукоби у сајбер домену између Естоније и РФ 2007. године, затим сукоб Грузије и РФ 2008. године и интервенција РФ на Украјину

2014. године, имају значајну улогу и да су подстакли САД и Северноатлантски савез да прошире своју политику сајбер одбране развојем централизованије стратегије сајбер безбедности и оснивањем информационо – телекомуникационих центара за одбрану од ових и сличних напада.

Нестанак правих вредности, морала и части у XXI веку је довео до тога да је светом завладала лаж, превара, обмана као основни постулат у раду и односу са познаницима, колегама, потчињенима на послу, као и између фирми, тела и држава, што се најбоље показало појавом вируса *COVID–19.* Лажи, обмане и преваре су се преселиле и у дневни живот широм планете у компаније, организације где ће руководиоци са оваквим односом према запосленима сигурно довести те организације до гашења, односно нестанка.

Руска Федерација несумњиво је показала шта је могуће да се догоди једној земљи попут Естоније, Грузије, па и великој држави попут Украјине, уколико се понаша супротно интересима РФ.

У *Петом поглављу* су сумирани резултати истраживања и дата закључна разматрања о перспективама утицаја стратегија одвраћања великих сила на делатност служби безбедности као и о угрожености националне безбедности држава према којима се примењују необавештајне активности и информационе операције. Анализирањем утицаја нових технологија на концепте одвраћања великих сила истражено је условљавање промена до којих тај утицај доводи. У овом поглављу су дати одговори, смернице за ревидирање стратешко – доктринарних докумената Републике Србије, као и предикција очекиваних промена у делокругу и начину рада служби безбедности у будућности.

Истраживањем је потврђена промена у структурама обавештајно – безбедносног карактера у Северноатлантском савезу, где је основан Заједнички одсек за обавештајно – безбедносне активности 2014. године, који представља један од механизама раног упозорења о намерама РФ о угрожавању њених чланица. Трансформацијом Северноатлантског савеза као одговор на анексију Крима од стране РФ у 2014. години, уводи се комбиновање одвраћања *порицањем* (конфликт сиве зоне, отпорност друштва, реакција и напредовање распоређених снага да се супротставе ограниченом отимању земље) и одвраћање *казнама* (пун ланац реакција и снага које се могу распоредити, од конвенционалних до нуклеарних). Још једна битна одлика одвраћања из 2021. године је то да је поред четврте димензије сукоба (сајбер простора) Северноатлантски савез додао и пету димензију сукоба (у свемиру).

Одговарајући на постављена истраживачка питања, закључујемо да се успон приватних војних компанија (енг. *Private Military Companies – PMCs)* из РФ подударио са развојем војне доктрине и стратегије у РФ у вези са употребом и улогом недржавних актера у сукобу. Интензиван је рад служби безбедности са приватним војним и другим компанијама и организацијама, ради остваривања присиле, врло често и директно физичких обрачуна, па чак и извршења ликвидација, где постоји велики број двоструких или вишеструких правила (аршина) како за велике силе (којима је дозвољено све укључујући и кршење закона), тако и за мале државе (које морају да поштују законе, правила и прописе, под образложењем увођења *демократије*, поштовања људских права и сл.). Употребу приватних компанија за државне потребе војне, полицијске, па чак и послове служби безбедности, проналазимо у САД још давне 1850. године приликом ангажовања чувеног Алена Пинкертона који је спречио атентат на Линколна преко своје приватне агенције, па до уназад пар деценија и низа ангажовања приватних војних компанија из САД, како на простору бивше

Социјалистичке Федеративне Републике Југославије тако и у великом броју држава широм планете, где год су САД пронашле своје *државне интересе*.

Једно од сазнања до којих смо дошли истраживањем је и проблем који се јавља у раду већег броја служби безбедности, а то је спровођење *координације* између служби безбедности и међусобни ривалитет истих, односно ко ће први доћи до неког податка и да ли ће тај податак уступити другој служби безбедности, што може довести до озбиљног угрожавања националне безбедности државе. Сједињене Америчке Државе су покушале да 1. децембра 2014. године побољшају своју безбедносну и контраобавештајну заштиту тако што су одредиле свој Национални контраобавештајни и безбедносни центар (енг. *National Counterintelligence and Security Center – NCSC*) ради постизања што ефикасније интеграције и усклађивања контраобавештајне активности и области безбедносних активности у оквиру једне организације. У истраживању као један од најбитнијих закључака можемо констатовати следеће: једна тако велика сила као што су САД региструје на основу пропуста у својој заштити националних интереса да је обједињавање безбедносне и контраобавештајне компоненте кључно решење у побољшању првенствено безбедносне заштите, па и контраобавештајне заштите једне организационе целине, пре свега ради правовременог начина доласка до безбедносно интересантног податка и моменталног предузимања мера у превентивном деловању које треба да буду правовремене. Интересантно је и то да тамо где се испољава негативан утицај САД на друге државе, у тим државама службе безбедности раздвајају безбедносну и контраобавештајну компоненту вероватно ради стварања неефикасних служби безбедности, система безбедности, а самим тим и држава уопште, док у исто време САД обједињују у својој држави ове две компоненте, што представља нераскидиво ткиво превентивног деловања сваке озбиљне службе безбедности, државе.

Истраживање је истакло и низ решења које је Израел предложио у својој одбрамбеној стратегији (енг. *Israel Defense Forces Strategy* 2016). Израђивачи овог документа били су најодговорнија лица из система безбедности и одбране, што би требало да послужи као пример и другим државама. Предвиђа конкретно решење регистрованог проблема, одговора на конкретну претњу. Одговор треба спровести кроз изградњу снага за кампању између ратова (енг. *Campaign Between The Wars – CBW*), што обухвата стварање координационог центра за операције кампања између ратова. Наведени центар треба да поседује међуорганизацијске и међуминистарске елементе, као и да развија способности за тајне и прикривене операције за кампању између ратова. У ових пар речи је предвиђен суштински концепт одвраћања ове државе где једна стратегија не представља само теоретско писање о неким проблемима, већ и конкретно, темељно давање системских решења у држави, што неће представљати апсолутно никакав проблем у реализацији с обзиром да су учесници израде овог документа најодговорнија лица из система безбедности и одбране Израела лично.

Један од резултата истраживања представља и потврда важности улоге образовања у повећању квалитета националне безбедности државе која је несагледива у области одвраћања, што смо доказали кроз велики број примера наведених у овом истраживању. Пример овладавања научно – технолошком надмоћи у освајању нових технологија у употреби хиперсоничних ракета, односно побољшања маневарских способности хиперсоничних високопрецизних ракета, видимо у примеру РФ над остатком планете или дронова произведених у Турској, Ирану и другим државама и сличне екстремне предности у

сајбер домену, домену економије (Кина) и слично. Важно је истаћи да једно од ових обележја представља и то да је РФ активна у развоју војне вештачке интелигенције, првенствено роботике. Вештачка интелигенција има потенцијал да пружи бројне предности[127] у војном контексту, али она може и да доведе до појаве нових различитих претњи. Све одговоре који су дати у овом истраживању на постављена истраживачка питања везано за промене у раду служби безбедности потврђује и изјава коју је Песков Димитрије, државни саветник РФ, дао медијима априла 2023. године, о појави нових претњи које ће довести до великих промена у безбедносним структурама у будућности.

Превентивно коришћење нуклеарног оружја у доктринама САД, а у доктринама РФ само услед опстанка државе РФ, говори нам да САД и даље сматрају да су једина суперсила на планети, што је у колизији са геополитичким и чињеничним стањем.

Потребе за променама у структурној организацији безбедносно – обавештајних система држава су све чешће, а изазване су учесталим променама тежишта стратешких праваца деловања ових структура услед регистровања нових врста претњи. Спровођење ових и сличних промена је потребно, међутим врло често представља и потенцијалну претњу, када не стигне да се заврши потребан циклус формирања и функционисања организације и већ се улази у нове структурне или друге врсте промена организација ове врсте. Овакви и слични поступци у једној организацији могу бити контрапродуктивни и водити ка урушавању или чак и уништењу те организације.

На основу регистрованих савремених претњи, које су углавном тајне природе, једино исправно супротстављање је ангажовањем служби безбедности, што доводи до закључка о потреби *интензивирања рада на јачању службе безбедности Републике Србије*. Узор могућег начина јачања службе безбедности и активности одвраћања се може препознати у већ познатим и примењиваним решењима у САД, Израелу, као и РФ, па би ради унапређења одвраћања у Републици Србији требало размислити о следећим предлозима:

– *Упростити и редуковати број стратешких прописа* у Републици Србији. Неопходно је у будућности упростити израду важних докумената стратешког нивоа, како је то урађено у Израелу где ова документа израђују најеминентније особе из области одбране и безбедности лично (начелник ГШ ВС, директори служби безбедности, полиције, начелник Управе Војне полиције, стручњаци из академске заједнице). На исти начин је пожељно уредити и сва друга документа у држави тако да буду практично примењива, односно *усаглашена* са оперативним и тактичким нивоом;

– на стратегијском нивоу *прописати нормативна акта о одвраћању* (предвидети већи део необавештајне активности, почев од политичке, економске, пропагандне, паравојне, информационе, информационо–телекомуникационе и других активности; затим предвидети структуре које ће се бавити истим, људство – кадрове, организацију, координацију, контролу, комуникацију, надлежности, послове, задатке, подршку и др.);

– предвидети обавезу *евиденције лица која због својих професионалних вештина могу учествовати у обавештајним – контраобавештајним или субверзивним активностима против Републике Србије* (стратешко контраобавештајно одвраћање између осталог

[127] Сједињене Америчке Државе кроз пројекат *Мавен* (енг. *Project Maven*) су користиле алгоритме вештачке интелигенције за идентификацију побуњеничких циљева у Ираку и Сирији. Ради се о аутоматизацији рада *људских аналитичара* преко вештачке интелигенције (Hoadley & Sayler, 2020).

унапредити прописивањем закона о регистрацији, давањем обавезе одређеном државном органу којме би био потчињен део овде наведених новоформираних целина) која бораве или планирају да бораве или су боравила у Републици Србији, која би евентуално могла бити укључена у планирање, обуку и реализацију субверзивних активности. Подсетимо да су САД ову регулативу донеле још 1917. године, а затим је унапредиле 1940. и 1956. године;

– *формирати обједињени национални центар за безбедносну и контраобавештајну заштиту* у чијем саставу би били представници све три службе безбедности, полиције, војске, војне полиције, надлежни државни органи, експерти, представници приватних организација и др. У састав овог центра требало би да уђу: *национални центар за сајбер безбедност* (државних и приватних структура; посебно одељење у саставу центра формирати за сајбер заштиту војске, служби безбедности, полиције, министарстава и вођење евиденције безбедносно интересантних специјалиста из ове области како страних тако и домаћих држављана; овај центар би могао бити саставни део претходно предложеног центра за безбедносну и контраобавештајну заштиту); *оперативно тело – центар за супротстављање пропагандним активностима* (дефанзивног карактера); *оперативно тело – центар за супротстављање економским активностима* (дефанзивног карактера); *центар за усавршавање* (који може бити и у саставу факултета из ове научне области, а који би био намењен усавршавању руководећег државног и другог политичког и безбедносног кадра у држави укљученог у супротстављање необавештајним активностима).

На крају, важно је нагласити да је обрађена тема веома актуелна и да ће, по свој прилици, бити актуелна и у наредном периоду, у коме се може очекивати да концепт одвраћања поприми нове форме. Нове форме одвраћања ће бити условљене новим претњама којима ће се државе интензивно супротстављати, развојем нових технологија и ангажовањем служби безбедности – необавештајним активностима које ће бити уграђене првенствено у спољну политику држава. Спроведеним истраживањем је дат нови поглед на одвраћање кроз разматрање употребе нових технологија и необавештајних активности, као одговор на регистроване претње по националну безбедност државе од стране служби безбедности. Проблематика представљена у спроведеном истраживању може бити од значаја доносиоцима политичких одлука, како би се упознали са комплексним активностима одвраћања као оруђа политике у постхладноратовском периоду. Одвраћање као *оруђе* политике сведочи о начину употребе нових технологија и необавештајних активности служби безбедности, како би се принудом остварили одређени уступци за матичну државу. Надамо се да ће спроведено истраживање послужити и као корисна литература академској заједници и окосница за будућа истраживања у овој области.

9. ЛИТЕРАТУРА

Adamsky, D. (2021). Deterrence à la Ruse: Its Uniqueness, Sources and Implications. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 161–175). Hague, Netherlands: T.M.C. Asser Press.

Alien Registration Act, (1940). *Act* of June 28, 1940, ch. 439, 54 Stat. 670 („Smith Act").

Ames, A. (1994). After the Soviet Union collapsed in 1991 and Cold War ended, the era of traditional spies was far from over, Famous cases & criminals, FBI, USA. Preuzeto 16.05.2022.

sa adrese https://fbi.gov.

Arbatov, A. (2021). Nuclear Deterrence: A Guarantee for or Threat to Strategic Stability? In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 65–86). Hague, Netherlands: T.M.C. Asser Press.

Army Officials Brief FY23 Department of Defense Budget Request, (2022). U.S. Army Public Affairs, *Transcript: Army Officials Brief FY23 DoD Budget Request,* March 30, 2022. Preuzeto 17.12.2022. sa adrese https://www.army.mil/article/255175/transcript_army_officials _brief_fy23_dod_budget_request.

Baezner, M. (2018). *Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict*, Zürich, October 2018, Version 2, Risk and Resilience Team Center for Security Studies, ETH Zürich, Switzerland.

Bartholomees, J. B. (2008). *National security policy and strategy*, 3rd Edition, Revised and Expanded, U.S. army war college guide to national security issues, Department of national security and strategy.

Bērziņš, J., Jaeski, A., Laity, M., Maliukevicius, N., Navys, A., Osborne, G., Pszczel, R., & Tatham, S. (2015). *Analysis Of Russia's Information Campaign Against Ukraine*. Examining non – military aspects of the crisis in Ukraine from a strategic communications perspectives. This report of the NATO StratCom Centre of Excellence, Riga.

Bijlsma, T. (2021). What's on the Human Mind? Decision Theory and Deterrence. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 437–453). Hague, Netherlands: T.M.C. Asser Press.

Bilandžić, M. (2005). Tajne operacije CIA kao komponenta vanjske politike SAD u posthladnoratovskom razdoblju, *Polemos 8 (2005.) 1–2*, Zagreb, pp. 221–238.

Birkenthal, M. S. (2013). *Grand Strategy in U.S. Foreign Policy: The Carter, Bush, and Obama Doctrines.* CMC Senior Theses. Paper 598. USA: Claremont McKenna College.

Bouwmeester, A. J. H. (2020). „*De Krim is van ons*" *Een analyse van hedendaagse Russische wijze van oorlogvoeren – inmenging door misleading*. Proefschrift ter verkrijging van de graad van doctor aan de Universiteit Utrecht, Nederlands.

Bowen, S. A. (2020). Russian Private Military Companies, September 16, 2020, IF11650, Version 8, *Congressional Research Service*, USA.

Bowen, S. A. (2021). Russian Military Intelligence: Background and Issues for Congress, Updated November 15, 2021., R46616, Version 7, *Congressional Research Service*, USA.

Bruusgaard, V. K. (2016). Russian Strategic Deterrence, *Survival, Global Politics and Strategy*, vol. 58 no. 4, August–September 2016, pp. 7–26.

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies.* UK: Cambridge University Press.

Central Intelligence Agency, (2022). *Learn About CIA – Organization*. Preuzeto 25.12.2022. sa adrese https://www.cia.gov/about/organization/.

Chernobrov, D., & Briant, E. (2020). Competing propagandas: How the United States and Russia represent mutual propaganda activities. *Politics*, Political Studies Association, Sage, pp. 1–17.

Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space, (2011). Ministry of Defence of the Russian Federation.

Connable, B., Young, S., Pezard, S., Radin, A., Cohen, R. S., Migacheva, K., & Sladden, J. (2020). *Russia's Hostile Measures, Combating Russian Gray Zone Aggression Against NATO,* RR2539, 2020 RAND Corporation, Santa Monica, Calif.

Counterintelligence and Security Enhancements Act of 1994, (1994). 50 us e 401 note. *Title VIII– Counterintelligence And Security*, Sec. 803. Rewards For Information Concerning Espionage, Oct. 14, 1994, Public Law 103–359 – Oct. 14, 1994 108 Stat. 3439.

Coy, M. (2021). *CIA Covert Warfare & U.S. Foreign Policy*. University Of Wisconsin – Madison, Department of History, Spring 2021.

Cumming, A. (2006). *Covert Action: Legislative Background and Possible Policy Questions*, CRS Report for Congress, Order Code RL33715. USA: The Library of Congress.

Darczewska, J., & Zochowski, P. (2017). Active Measures Russia's Key Export, *Point of View*, No 64, July 2017, pp.1–71. Warsaw, Poland: OSW.

Department of Defense Dictionary of Military and Associated Terms, (2021). *Standard US military and associated terminology to encompass the joint activity of the Armed Forces of the United State, Department of Defense.* USA: DoD.

DeVine, E. M. (2019a). The U.S. Intelligence Community: Homeland Security Issues in the 116th Congress, *CRS Report – Congressional Research Service*, 1 February 2019.

DeVine, E. M. (2019b). Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief. *CRS Report – Congressional Research Service*, 14. June 2019.

Doorn, C., & Brinkel, T. (2021). Deterrence, Resilience, and the Shooting Down of Flight MH17. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 365–383). Hague, Netherlands: T.M.C. Asser Press.

Douhan, A. (2022). Unilateral sanctions in the cyberworld: tendencies and challenges, United Nations A/77/296, Distr.: General 17 August 2022. *Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights,* OHCR.

Ducheine, P., & Pijpers, P. (2021). The Missing Component in Deterrence Theory: The Legal Framework. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 476–495). Hague, Netherlands: T.M.C. Asser Press.

Erickson, E. (2018). What Do We Mean by Great Power or Superpower? An Introduction to Concepts and Terms, *MCU Journal* vol. 9, no. 2, 2018.

Executive Order 12333, (2008). *United States Intelligence Activities*, Dec. 4, 1981 (As amended by Executive Orders 13284 /2003/, 13355 /2004/ and 13470 /2008/).

Executive Order 13467, (2008). Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008. *Executive Order*, Filed with the Office of the Federal Register, July 2, 2008, pp. 932–936.

Fedchenko, Y. (2016). Kremlin propaganda: Soviet active measures by other means, Dentity And Propaganda In Russian – Ukrainian Hybrid, Warfare, *Sõjateadlane* (*Estonian Journal of Military Studies*), vol. 2, 2016, pp. 140–169.

Federal Security Service of the Russian Federation, (2022). Federal Security Service of the Russian Federation, *The Structure Of The Federal Security Service*, Moscow, Bolshaya Lubyanka street, building 1. Preuzeto 28.12.2022. sa adrese http://www.fsb.ru/fsb/structure.htm.

Federation of American Scientists, (2022a). *Federation Of American Scientists*, Federation of American Scientists, Washington, USA, DC 20036. Preuzeto 18.12.2022. sa adrese https://fas.org/issues/national-security/.

Federation of American Scientists, (2022b). *Federation Of American Scientists*, Federation of American Scientists, Washington, USA, DC 20036. Preuzeto 23.12.2022. sa adrese https://fas.org/issues/disinformation-research/.

Felshtinsky, Y., & Litvinenko, A. (2002). *Blowing Up Russia* (Original title: *FSB Vzryvayet Rossiyu*), USA, Liberty Publishing House, Inc, pp. 225–237; 238–252.

Foreign and Military Intelligence, (1976). *Final Report of the Select Committee To Study Governmental Operations With Respect to Intelligence Activities, United States Senate*, Book I, 26 April 1976, Washington, Report No. 94/755, pp. 56–57.

Foreign Intelligence Surveillance Act, (1978). *Congressional Research Service*, An Overview, Updated April 6, 2021, IF11451, Version 3, Updated, USA.

Freedman, L. (2009). Framing strategic deterrence, *The RUSI Journal*, august 2009, vol. 154, No. 4, pp. 46–50, London: Routledge.

Gendlin, G. (1998). Perspectives, Dangers of the „Clinton Doctrine", *National Security Studies Quarterly*, Spring 1998, pp. 51–63.

Geneva Centre For The Democratic Control Of Armed Forces, (2003). *Intelligence practice and democratic oversight – A practitioner's view*, Intelligence working group, Geneva Centre For The Democratic Control Of Armed Forces, Paper No. 3, July 2003, Geneva, Switzerland.

Geneva Centre For The Democratic Control Of Armed Forces, (2006). *Разведывательные службы*, Женевский Центр демократического контроля над вооруженными силами, Женева**.** Geneva, Switzerland.

Gill, P. (2010). Theories of Intelligence. *Oxford University Press*, *The Oxford Handbook of National Security Intelligence*, Political Science, Mar 2010.

Giumelli, F. (2021). Targeted Sanctions and Deterrence in the Twenty – first Century. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 350–362). Hague, Netherlands: T.M.C. Asser Press.

Godson, R. (1995). Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence. In: Reagan, L. M. (Ed.) (2014). *Counterintelligence Glossary – Terms & Definitions of Interest for CI Professionals*, 9 June 2014. (pp. 81). USA: United States Defense Intelligence Agency.

Golov, A. (2016). *Israeli Deterrence in the 21st Century*. In: Landau, E. B., & Kurz, A. (Ed.), *Arms Control and Strategic Stability in the Middle East and Europe* (pp. 83–97). Tel – Aviv: Institute for National Security Studies.

Government of the Russian Federation, (2022). Government of the Russian Federation, *Economic relations with foreign countries on a bilateral basis*, *Documents and events*. Preuzeto 27.12.2022. sa adrese http://government.ru/rugovclassifier/21/events/?country=EE.

Graham, A. (2016). Deterring Terror, English Translation of the Official Strategy of the Israel Defense Forces (*Israel Defense Forces Strategy* 2016). Belfer Center for Science and International Affairs, Harvard Kennedy School.

Gray, S. C. (2016). *Strategy and Politics*. New York, USA: Routledge is an imprint of the Taylor & Francis Group.

Harder, R. (2017). Intelligence Services Roles and responsibilities in good security sector

governance, *Geneva Centre for the Democratic Control of Armed Forces, Intelligence Oversight, Security Sector Reform, Backgrounder Series*, Switzerland.

Hoadley, S. D., & Sayler, M. K. (2020). Artificial Intelligence and National Security. Updated November 10, 2020, *Congressional Research Service – R45178*, Version 10.

Iasiello, E. (2015). Are Cyber Weapons Effective Military Tools? *Military and Strategic Affairs*, vol. 7, No. 1, March 2015, pp. 23–40.

Information Security. (2022). *Information Security*. Москва, Краснопресненская наб., 2 Дом Правительства Департамент пресс – службы Правительства Российской Федерации. Preuzeto 20.12.2022. sa adrese http://government.ru/rugovclassifier/622/events/.

Ivanov, V. T. (2017). Competitive Intelligence And Counterintelligence – *Modern Tools For Generating Proactive Corporate Security International Scientific Journal* „*Security & Future*", Year I, Issue 1, 2017, pp. 7–10.

Jakobsen, V. P. (2021). Deterrence in Peace Operations: Look Beyond the Battlefield and Expand the Number of Targets and Influence Mechanisms. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 327–345). Hague, Netherlands: T.M.C. Asser Press.

Johnson, K. L. (Ed.), (2007a). *Strategic Intelligence 3, Covert action: Behind the veils of secret foreign policy.* Westport, Connecticut, London: Praeger Security International.

Johnson, K. L. (Ed.), (2007b). *Strategic Intelligence 4, Counterintelligence and counterterrorism: Defending the nation against hostile forces.* Westport, Connecticut, London: Praeger Security International.

Johnson, K. L. (2012). Intelligence Analysis and Planning for Paramilitary Operations, *Journal Of National Security Law & Policy*, vol. 5: 481–505.

Johnson, K. L. (2017). *National Security Intelligence, Secret Operations in Defense of the Democracies*, Second Edition. Cambridge, UK.

Joint Publication 2–01. (2017). Joint and National Intelligence Support to Military Operations, 5 July 2017. JP 2–01. Washington, USA: Headquarters Department of the Army.

Joint Publication 3–13. (2016). Information Operations, *Field Manual – FM No. 3–13*, 6 December 2016. JP 3–13. Washington, USA: Headquarters Department of the Army.

Karloš, B. (2019). *Rat na balkanu, džihadizam, geopolitika i dezinformacija*, doživljaji jednog oficira portugalske vojske u službi OUN, Knjiga komerc.

Kibbe, D. J. (2017). *Covert Action*, Oxford Research Encyclopedias, International Studies. Pensilvanija. USA: Franklin & Marshall College.

Kissinger, H. (1994). *Diplomacy*. New York, USA: Simon & Schuster.

Kitzen, M., & Kuijck, C. (2021). All Deterrence Is Local: The Utility and Application of Localised Deterrence in Counterinsurgency. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 287–310). Hague, Netherlands: T.M.C. Asser Press.

Klaus, M. (2021). Trusting ICT Providers – Can Corporate Cyber Confidence – Building Measures Help? *Connections:The Quarterly Journal* (*connections–qj*), vol. 20, No. 2, Spring 2021, pp. 21–31.

Knopf, W. J. (2010). The Fourth Wave in Deterrence Research, *Contemporary Security Policy*, 31:1, April 1, 2010, pp. 1–33.

Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., & Oberholtzer, J. (2017).

Lessons from Russia's Operations in Crimea and Eastern Ukraine. Santa Monica, Calif.: RAND Corporation.

Kotler, P., Berger, R., & Bickhoff, N. (2010). *The Quintessence of Strategic Management*, Springer – Verlag Berlin Heidelberg, pp. 6, 7 (Original Title: *Quintessenz des strategischen Managements*, Springer – Verlag 2008, Translation: Claire Jokubauskas, London).

Krepinevich, F. A. (2019). *The Decline of Deterrence*. Washington, USA: Hudson Institute.

Krishnan, A. (2018). *Why Paramilitary Operations Fail*, Department of Political Science East Carolina University Greenville, NC, USA, Zuma Press, Inc., Palgrave Macmillan, pp. 1–20.

Kristek, R. M. (2017). The nature of Russia's threat to NATO's enhanced forward presence in the Baltic States. (*Master's thesis*). Monterey, California: Naval Postgraduate School.

Lamarque, K. (2020). Ubistvo Solejmanija deo nove strategije odvraćanja neprijatelja, *Reuters*, 14.01.2020. godine. Preuzeto 26.06.2021. sa adrese https://rs.n1info.com/svet/a560311-pompeo-ubistvo-solejmanija-deo-nove-strategije-odvracanja/.

Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs*, 92(1), University of London, pp. 175–195.

Lieberman, A. V. (2017). Terrorism, the Internet, and Propaganda: A Deadly Combination. *Journal Of National Security Law & Policy*, vol. 9: 95, pp. 95–124.

Litvinenko, A., & Felshtinsky, Y. (2013). *Blowing Up Russia – The Secret Plot To Bring Back KGB Terror*, Acts Of Terror, Abductions, And Contract Killings Organized By The Federal Security Service Of The Russian Federation, Translated From Russian By Geoffrey Andrews And Co., Gibson Square, London.

Lowenthal, M. M. (2009). *Intelligence: from secrets to policy*, 4th ed., Covert action, Chapter 8. Washington, USA: CQ Press is a division of SAGE.

MacDuffee, M. M., & Tucker, J.A. (2017). Social Media and EuroMaidan: A Review Essay. *Slavic Review*, 76, no. 1, Spring 2017, pp. 169–191.

Marchetti, V., & Marks, J. D. (1983). *The CIA and the Cult of Intelligence.* First publish 1974, 1980, 1983. New York, USA: Alfred A. Knopf Publisher.

Mazarr, J. M. (2018). *Understanding Deterrence*. Santa Monica, CA: RAND Corporation. Preuzeto 30.05.2022. sa adrese https://www.rand.org/pubs/perspectives/PE295.html.

McCurdy, D. (1991). *Joint Explanatory Statement of the Committee of Conference*, H.R. 1455, July 25, 1991, Sec. 503, (e).

Mearsheimer, J. J. (2001). The tragedy of great power politics. New York, USA: W.W. Norton & Company.

Miniats, M. A. (2019). War of Nerves: Russia's Use of Cyber Warfare in Estonia, Georgia and Ukraine. *Senior Projects* Spring 2019, 116. Bard College, New York.

Ministry of Defence Russian Federation, (2022). Ministry of Defence of the Russian Federation, *Russian Federation Armed Forces' Information Space Activities Concept*. Preuzeto 21.12.2022. sa adrese https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

Ministry of Foreign Affairs of the Russian Federation, (2022a). Ministry of Foreign Affairs of the Russian Federation, *Reviews of foreign policy activity*. Preuzeto 30.12.2022. sa adrese https://www.mid.ru/ru/activity/review/.

Ministry of Foreign Affairs of the Russian Federation, (2022b). Ministry of Foreign Affairs of the Russian Federation, *Repressions against Russian media and journalists abroad*. Preuzeto 31.12.2022. sa adrese https://www.mid.ru/ru/press_service/journalist_help/repressions/.

Monaghan, S. (2022). *Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice*, Hybrid CoE Paper 12 2, The European Centre of Excellence for Countering Hybrid Threats.

Morgan, M. P. (2012). The State of Deterrence in International Politics Today, *Contemporary Security Policy*, vol. 33, No.1, April 2012, pp. 85–107, Taylor & Francis.

National Defense Business Operations Plan. (2022). *FY 2018 – FY 2022 National Defense Business Operations Plan*, USA, Generated on April 9, 2018.

National Defense Strategy. (2018). Of Sharpening the American Military's Competitive Edge, Summary of the 2018. The United States of America: U.S. Department of Defense.

National Defense Strategy. (2022). National Defense Strategy, October 27, 2022. The United States of America: U.S. Department of Defense.

National Military Strategy of the United States. (1992). BMD Technical information center, Balistic Missile defense organization. Pentagon, Washington, DC: U.S. Government.

National Military Strategy of the United States of America. (1995). Superintendent of Documents. Washington, DC: U.S. Government.

National Military Strategy Document of the United States of America. (2004). A Strategy for Today; A Vision for Tomorrow, 2004. Washington, DC: U.S. Government.

National Military Strategy of the United States of America, Redefining America's Military Leadership. (2011). February 8, 2011. Washington, DC: U.S. Government.

National Military Strategy of the United States of America. (2015). The United States Military's Contribution To National Security, June 2015. Washington, DC: U.S. Government.

National Military Strategy of the United States of America. (2018). Strategy Development Division, Deputy Directorate for Joint Strategic Planning, Directorate for Strategy, Plans, and Policy (J–5), The Joint Staff, June 2018. Washington, DC: U.S. Government.

National Security Act of 1947. (2021). Chapter 343; 61 Stat. 496; approved July 26, 1947, As Amended Through P. L. 116–283, Enacted January 1, 2021.

National Security Act of 1947. (2022). National Security Act of 1947 [50 U.S.C. 3001], Chapter 343; 61 Stat. 496; approved July 26, 1947, As Amended Through P. L. 117–103, Enacted March 15, 2022, Section 503e, pp. 90.

National Security Action Memorandum No. 303. (1964). Foreign Relations Of The United States, 1964–1968, vol. XXXIII, Organization And Management Of Foreign Policy; United Nations, *204. National Security Action Memorandum No. 303*. USA, Washington, June 2, 1964.

National Security Council 10/2. (1948). Foreign Relations Of The United States, 1945–1950, Emergence Of The Intelligence Establishment. *292. National Security Council Directive on Office of Special Projects*. Washington, June 18, 1948.

National Security Council 10/5. (1951). Actions Taken By The National Security Council On Scope And Pace Of Covert Operations, *Note From the Executive Secretary of the National Security Council* (*Lay*) *to the National Security Council*, *Foreign Relations*, The Intelligence Community, USA, Washington, October 23, 1951, pp. 207, 208.

National Security Council 48/5. (1951). Policies and Courses of Action in Asia, *Report to the National Security Council by the Executive Secretary* (*Lay*), Foreign Relations Of The United States, 1951, Asia And The Pacific, vol. VI, Part 1, United States, Washington, May 17, 1951.

National Security Council 4–A. (1947). Foreign Relations, 1945–1950, Emergence of the Intelligence Establishment, *Document 257*, December 17, 1947.

National Security Council 5412. (1954). National Security Council – Directive On Covert Operations, Foreign Relations Of The United States, 1950–1955, The Intelligence Community, 1950–1955, *171. Note From the Executive Secretary of the National Security Council* (*Lay*) *to the National Security Council*, NSC 5412, USA, Washington, March 15, 1954.

National Security Council 5412/1. (1955). Covert Operations, Foreign Relations Of The United States, 1950–1955, The Intelligence Community, *212. National Security Council Directive*, Washington, March 12, 1955.

National Security Council 5412/2. (1955). Covert Operations, Foreign Relations Of The United States, 1950–1955, The Intelligence Community, *250. National Security Council Directive*, USA, Washington, undated.

National Security Council Intelligence Directive No. 7. (1948). National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lot 66 D 95, Box 1799, NSC IDs. Secret. Washington, February 12, 1948.

National Security Decision Memorandum 40. (1970). Responsibility for the Conduct, Supervision and Coordination of Covert Action Operations, *National Security Decision Memorandum 40*, The White House, Washington, February 17, 1970.

National Security Strategy for a new century. (1999). President Bill Clinton, The White House, Washington, December 1999.

National Security Strategy of the United States of America. (2006). President George W. Bush, The White House, Washington, March 16, 2006.

National Security Strategy of the United States of America. (2017). President Donald J. Trump, The White House, Washington, DC, December 2017.

National Security Strategy of the United States of America. (2022). President Joe Biden, The White House, Washington, October 2022.

Naval Postgraduate School, (2022). Naval Postgraduate School, *Our Capabilities – We deliver solutions to the Fleet*, Monterey. Preuzeto 26.12.2022. sa adrese https://nps.edu/capabilities.

Nye, S. J. (1990). *Bound to lead: The Changing Nature of American Power*, Basic Books, New York, 1990. In: Путник, Н. (2012). Кибер ратовање – нови облик савремених друштвених конфликата. (*Докторска дисертација*). Београд: Факултет безбедности.

O'Brien, A. K. (2007). Covert Action: The „Quiet Option" in International Statecraft. In: Johnson, K. L. (Ed.), (2007). *Strategic Intelligence 3, Covert action: Behind the veils of secret foreign policy* (pp. 774). USA: Greenwood Publishing Group, Inc.

Organization for Security and Co – operation in Europe. (2014). *Sprečavanje terorizma i suzbijanje nasilnog ekstremizma i radikalizacije koji vode ka terorizmu: Pristup kroz rad policije u zajednici.* Organizacija za evropsku sigurnost i saradnju, mart 2014. godine, Beč, Austrija.

Organization for Security and Co – operation in Europe. (2018). *The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Focus on South – Eastern Europe*. Organizacija za evropsku bezbednost i saradnju, avgust 2018, Beč, Austrija.

Orlov, A. (1963). *The Handbook of Intelligence and Guerrilla Warfare, Ann Arbor, University of Michigan Press.* In: Riehle, K. P. (2022). Russian Intelligence – A Case – Based Study Of Russian Services And Missions Past And Present, *National Intelligence University Bethesda*, MD, National Intelligence Press.

Osinga, F., & Sweijs, T. (2021). *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice.* The Hague, The Netherlands: T.M.C. Asser Press, pp. 503–529.

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. Proceedings of the *7th European Conference on Information Warfare and Security*, Plymouth, 2008. Tallinn, Estonia: Academic Publishing Limited, pp. 163–168.

Owens, T. M. (1999). In Defense of Classical Geopolitics, *Naval War College Review*, vol. 52, No. 4, autumn 1999, pp. 59–76.

Prunckun, H. (2019). *Counterintelligence theory and practice*, Second Edition. London, United Kingdom: Rowman & Littlefield.

Radin, A., Demus, A., & Marcinek, K. (2020). Understanding Russian Subversion, Patterns, Threats, and Responses, *PE–331–A, RAND Corporation*, United States Army, pp. 9.

Radio Slobodna Evropa. (2022). *Belgija Kongu vratila zlatni zub Patrisa Lumumbe*. Preuzeto 17.01.2023. sa adrese www.slobodnaevropa.org/a/lumumba--belgija-kolonijalizam/31906306.html.

Reagan, L. M. (2014). Terms & Definitions of Interest for CI Professionals, *Counterintelligence Glossary*, 9 June 2014. USA: Department of Defense.

Redmond, J. P. (2010). The Challenges of Counterintelligence, Chapter 33. In: Johnson, L. (2010). *The Oxford Handbook of National Security Intelligence* (pp. 537–554). New York: Oxford University Press.

Reese, S. (2021). National Special Security Events: Fact Sheet, *CRS Reports – Congressional Research Service* (crsreports.congress.gov), January 11, 2021.

Registration of Certain Persons Trained in Foreign Espionage Systems. (1956). *Act* of Aug 1, 1956, ch. 849, Sec. 2, 70 Stat. 899.

Reporters Without Borders. (2022). Reporters Without Borders, *World: Abuses In Real Time*. Preuzeto 30.12.2022. sa adrese https://rsf.org/en/barometer?exaction_pays_pays=210&exaction_pays_annee=2014&exaction_pays_statut=prison#exaction-pays.

Riehle, K. P. (2022). Russian Intelligence – A Case – Based Study Of Russian Services And Missions Past And Present, *National Intelligence University Bethesda*, MD, National Intelligence Press.

Roberts, B. (2020). On Theories of Victory, Red and Blue, *Livermore Papers on Global Security No. 7*, Lawrence Livermore National Laboratory, Center for Global Security Research, June 2020.

Rosoboronexport. (2022). Rosoboronexport, *Каталог – Рособоронэкспорт*, Москва, Российская Федерация. Preuzeto 27.12.2022. sa adrese http://roe.ru/catalog/.

Rothman, M. (2021). This Has Triggered a Civil War: Russian Deterrence of Democratic Revolts. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 311–325). Hague, Netherlands: T.M.C. Asser Press.

Rynning, S. (2021). Deterrence Rediscovered: NATO and Russia, *Annual Review of Military Studies 2020*, NL Arms Netherlands. Hague, Netherlands: T.M.C. Asser Press.

Schelling, C. T. (2008). *Arms and influence: With a New Preface and Afterword*. Printed in the United States of America, New Haven and London Yale University Press.

Schoen, F., & Lamb, C. J. (2012). *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference.* Center for Strategic Research Institute for National Strategic Studies National Defense University. June 2012. Washington, D.C.: National

Defense University Press.
Science & Technology. (2022). Science & Technology, U.S. Department of Defense. Preuzeto 22.12.2022. sa adrese https://www.defense.gov/Spotlights/Science-and-Technology/.
Scott, D. K. (2018). Joint Doctrine Note 1–18, *Strategy*, 25 April 2018.
Scott, L., & Jackson, P. (2004). The Study of Intelligence in Theory and Practice. *Intelligence and National Security,* vol. 19, No. 2, Summer 2004, Taylor & Francis Ltd., pp. 139–169.
Security Executive Agent. (2022). Security Executive Agent, *The National Counterintelligence and Security Center*. Preuzeto 05.05.2022. sa adrese https://dni.gov.
Shamir, E. (2021). Deterring Violent Non – state Actors. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 263–286). Hague, Netherlands: T.M.C. Asser Press.
Sipher, J. (2018). Russian „Active Measures", CHACR – Centre for Historical Analysis and Conflict Research, *Global Analysis Programme Briefing Robertson House*, Slim Road, Camberley, pp.1–9.
Soesanto, S., & Smeets, M. (2021). Cyber Deterrence: The Past, Present, and Future. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 385–399). Hague, Netherlands: T.M.C. Asser Press.
Spiegel, C. (2017). Securing Cyberspace: Nato's Cyber Defence Policy As A Security Dispositive. (*Master's Thesis*) MA International Relations in Historical Perspective 2016/2017 Utrecht University.
Stewart, P. (2020). Spies behind 2008 cyber attack, U.S. official says, *Reuters*. Preuzeto 03.08.2022. sa adrese https://www.reuters.com/article/us-usa-cyber-attack-idUSTRE67P00X20100826.
Stoltenberg, J. (2018). „*Stoltenberg: NATO može da iskoristi član 5. Povelje u slučaju ruskog sajber – napada*". Preuzeto 10.04.2022. sa adrese https://Vostok.rs, i Stoltenberg, J. (2021). „*Svi za jednog, jedan za sve: NATO uvodi promjenu*". Preuzeto 10.04.2022. sa adrese https://rtvbn.com.
Stratcom Centre UA. (2022). *Russia has agents of influence – and entire parties of supporters – all across Europe*. Mapa objavljena 4. Septembra 2022. godine. Preuzeto 24.09.2022. sa adrese https://mobile.twitter.com.
Strategic Plan 2018 – 2022. (2017). National Counterintelligence and Security Center, *Strategic Plan 2018 – 2022*, Office Of The Director Of National Intelligence, USA, 2017, pp. 1–29.
Suitability Executive Agent. (2022). *U. S. Office of Personnel Management*. Preuzeto 05.05.2022. sa adrese https://opm.gov.
The Intelligence Community. (2022). *Intelligence Community*, званичан сајт обавештајне заједнице САД. Preuzeto 27.05.2022. sa adrese https://www.intelligence.gov.
The National Geospatial – Intelligence Agency. (2022). The National Geospatial – Intelligence Agency, *GEOINT* Drive, Springfield, VA 22150. Preuzeto 16.12.2022. sa adrese https://usa.gov & https://www.nga.mil/about/About_Us.html.
The Russian Federation's National Security Strategy. (2009). Russian Federation Presidential Edict 537 dated 12 May 2009, „On the Russian Federation's National Security Strategy Through 2020", *Sobraniye zakonodatelstva Rossiyskoy Federatsii*, Moscow, the Kremlin.
Timothy, L. T. (2019). *Russian Military Thought: Concepts and Elements*, August 2019, The MITRE

Corporation, US European Command.

Title 50 *U.S. Code,* § 3093. (2014). Presidential approval and reporting of covert actions, *Title 50* – War And National Defense, pp. 506–508.

Training and Doctrine Command G2 Handbook No. 1.08. (2010). *Irregular Forces*, US Army Training and Doctrine Command, TRADOC G2, Intelligence Support Activity (TRISA), 20 December 2010, Fort Leavenworth, Kansas (This *publication 1.08* will be a baseline for transition of *FM 7–100.3 to Training Circular 7–100.3*).

Trapara, V. (2017). Does Trump Have A Grand Strategy? *The Review of International Affairs,* vol. LXVIII, No. 1168, October – December 2017, pp. 56–70.

Turunen, M., & Kari, M. J. (2022). The Cumulative Cyber Deterrence, Proceedings of the *17th International Conference on Information Warfare and Security*, 2022. Finnish National Defence University, Finland, University of Jyväskylä, Finland.

United Nations Educational, Scientific and Cultural Organization. (2017). *Preventing violent extremism through education: A guide for policy – makers*. Paris, France, Published in 2017 by the United Nations Educational, Scientific and Cultural Organization.

United States Information Agency. (2022). *United States Information Agency*, USA. Preuzeto 05.08.2022. sa adrese https://govinfo.library.unt.edu/npr/library/status/mission/musia.htm.

Uram, A. D. (2005). *Covert Action: A Useful Tool for United States Foreign Policy?* Canada: University of Victoria.

Warner, M. (2002). Wanted: A Definition of „Intelligence", *Studies In Intelligence,* vol. 46, No. 3, 46:3, 2002. Central Intelligence Agency, Center for the Study of Intelligence, Washington, DC, pp. 15–22

Weapons of Mass Destruction. (2005). The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005.

Wheaton, J. K., & Beerbower, T. M. (2006). Towards A New Definition Of Intelligence, *Stanford Law And Policy Review*, vol. 17: 317, May 19, 2006, pp. 319–330.

Wilde, G. (2022). Cyber Conflict In The Russia – Ukraine War, Cyber Operations in Ukraine: Russia's Unmet Expectations, *Carnegie Endowment for International Peace*, December 2022. Massachusetts, Washington, USA.

Williams, D. P. (2008). *Security studies: an introduction.* New York, USA: Taylor & Francis Group, pp. 26, 27.

Wilner, A., & Babb, C. (2021). New Technologies and Deterrence: Artificial Intelligence and Adversarial Behaviour. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 402–417). Hague, Netherlands: T.M.C. Asser Press.

Wirtz, J. J. (2017). *Understanding intelligence failure – Warning, response and deterrence*. USA: Routledge, Taylor & Francis Group.

Woolf, F. A. (2021). Russia's Nuclear Weapons: Doctrine, Forces, and Modernization, *Congressional Research Service – R45861*, Version 7, September 13, 2021, pp. 1–43.

Zilincik, S., & Duyvesteyn, I. (2021). Deterrence: A Continuation of Emotional Life with the Admixture of Violent Means. In: Osinga, F., & Sweijs, T. (Ed.), *NL Arms Netherland Annual Review of Military Studies 2020, Deterrence in the 21st Century – Insights from Theory and Practice* (pp. 455–474). Hague, Netherlands: T.M.C. Asser Press.

Арежина, С. (2011). Запажена студија о феномену моћи, *Политеиа, број 5*, Бања Лука, јун 2013. (Džozef S. Naj, The Future of Power, *Public Affairs*, New York, 2011, pp. 300), стр. 293–296.

Бајагић, М. (2009). Иностранa искуства у развоју теоријског и организационог концепта контраобавештајне активности, *часопис Безбедност 1–2*/2009, стр. 370–385.

Бајагић, М. (2010). *Шпијунажа у 21. веку – Савремени обавештајно – безбедносни системи*, друго допуњено издање. Београд: МАРСО.

Бајагић, М. (2013). Обавештајна активност у функцији изградње система националне безбедности. *Политика националне безбедности број 1*/2013, стр. 61–86.

Бајагић, М. (2015a). *Методика обавештајног рада*. Друго, измењено и допуњено издање, Београд: Криминалистичко полицијска академија.

Бајагић, М. (2015b). Обавештајно – безбедносни систем Републике Аргентине, Криминалистичко полицијска академија, Београд, *Наука, Безбедност, Полиција, Журнал за криминалистику и право*, 2015, *20, 1,* стр. 31–46.

Бороган, И., & Солдатов, А. (2022). *Пригожин спешит на помощь*, 13 ноября, 2022. Преузето 19.12.2022. са адресе https://agentura.ru/investigations/prigozhin-speshit-na-pomoshh/.

Војна доктрина Руске Федерације – Военная доктрина Российской Федерации. (2014). Председник Руске Федерације, В. Путин, 25. децембра 2014. N Пр – 2976.

Врачевић, Н. и Цветковић, М. В. (2019). Приватне војне компаније у модерном добу, Међународно окружење, *Војно дело, 2*/2019, Београд, стр. 42–54.

Вујанић, М., Гортан – Премк, Д., Дешић, М., Драгићевић, Р., Николић, М., Ного, Љ., Павковић, В., Рамић, Н., Стијовић, Р., Радовић – Тешић, М. и Фекете, Е. (2011). *Речник српског језика*, Измењено и поправљено издање, Нови Сад, Република Србија, Матица српска.

Деспотовић, Љ. и Јевтовић, З. (2019). Геополитика медија, *Култура полиса*. Нови Сад, Сремски Карловци: Каирос.

Димитријевић, И. (2022). Отворени извори података као фактор трансформације обавештајног рада. (*Докторска дисертација*). Београд: Факултет безбедности.

Димитријевић, И. и Параушић, А. (2017). *Каталог база података за истраживања у области безбедности.* Београд: Факултет безбедности.

Драгишић, З. (2020). Национална безбедност – алтернативе и песпективе. У В. Н. Цветковић (ур.), *Науке безбедности: врсте и облици* (стр. 39–55). Београд: Факултет безбедности.

Ђорић, Р. М. (2012). Теоријско одређење екстремизма, *Култура полиса, год. IX, 2012, бр. 17*, Монографска студија, Нови Сад, стр. 45–62.

Закон РФ „О безопасности". (1992). *Закон О безопасности,* Ведомости Съезда народных депутатов и Верховного Совета Российской Федерации, 5 март 1992. г. № 2446 – I (с изменениями от 25 декабря 1992 г., 24 декабря 1993 г., 25 июля 2002 г., 7 марта 2005 г., 25 июля 2006 г., 2 марта 2007 г., 26 июня 2008 г.).

Зечевић, М. (1990). *Војна дипломатија*. Београд: Војноиздавачки и новински центар.

Јефтић, З., Мишев, Г., Обрадовић, Ж. и Станојевић, П. (2018). Савремени конфликти и њихове тенденције, *Војно дело, 7*/2018, Београд, стр. 23–40.

Ковачев, Д. (2018). Шта је астротурфинг или од Гебелса до „ботова". Преузето 27.06.2022. са адресе https://standard.rs/2018/10/02/d-kovacev-sta-je-astroturfing-ili-od-gebelsa-do-botova/.

Конатар, Б. В. (2015). Ефикасност обавештајних служби и професионална етика. (*Докторска*

дисертација). Београд: Факултет безбедности.

Кривични законик. (2019). Кривични законик, *Службени гласник РС*, бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019, Република Србија.

Кусовац, М. (2021). Украјина између Запада и Руске Федерације, *Матица, број 86, лето 2021.* године, Подгорица, РЦГ, стр. 169–184.

Лабовић, Д. (2015). Приватне војне компаније као фактор безбедности – предности и недостаци, *часопис Безбедност, 3*/2015, Београд, стр. 142–157.

Лабовић, Д. и Марјановић, З. (2021). Нормативни аспекти унутрашње контроле Војнобезбедносне агенције Републике Србије, *часопис Безбједност, полиција, грађани,* број *2*/21, Бања Лука, Министарство унутрашњих послова Републике Српске, Република Српска, БиХ.

Лукашук, И. И. (2005). *Международное право – Великие и малые державы*. У: Волтерс Клувер, 2005, § 5, Глава XI, стр. 335–336.

Марјановић, З. (2015). Утицај војне дипломатије на међународне војне односе у региону. (*Мастер рад*). Београд: Војна академија.

Марјановић, З. (2022, април). Утицај нових технологија на концепт стратешког одвраћања великих сила, *Осма међународна научна конференција „Примена нових технологија у менаџменту*", *Зборник радова*, АНТиМ 2022, 15.04.2022. г, Београд, Србија, стр. 253–268.

Марјановић, З. и Мићновић, М. (2022). Утицај кризне ситуације изазване епидемијом и пандемијом (ковид 19) на корпоративну безбедност, *часопис Безбедност, 3*/2022, LXIV, Београд, стр. 100–119.

Марјановић, З. и Мићновић, М. (2023). Географски вектор националне одбране – Копнена моћ, *часопис Политичка ревија, број 1*/2023, Година (XXXI) XXIII, vol. 75, Београд, стр. 183–209.

Марјановић, З., Лабовић, Д. и Браковић, Ж. (2022). Нормативни аспекти тајних метода рада Војнобезбедносне агенције у Републици Србији, *Дипломатија и безбедност,* Година 5, број 1/2022, Београд, стр. 203–223 (*Diplomacy and Security*, vol. V, Number 1/2022, pp. 225–245).

Мельникова, О. А. (2020). Информационное обеспечение внешнеполитической деятельности современных государств (политологический анализ). (*Диссертация на соискание ученой степени кандидата политологических наук*). РФ, Москва.

Мијалковић, С. (2010). О недржавном сектору националног Система безбедности – иностранa и домаћа искуства, *Страни правни живот, 2*/2010, Криминалистичко – полицијска академија, Београд, стр. 251–270.

Мијалковић, С. (2011). Обавештајно – безбедносне службе и национална безбедност, *часопис Безбедност, 1/2011,* Београд, стр. 74–92.

Мијалковић, С. (2015). *Национална безбедност*. Београд: Криминалистичко – полицијска академија.

Мијалковски, М. (2009). *Обавештајне и безбедносне службе.* Београд: Факултет безбедности.

Мијалковски, М. и Конатар, В. (2010). *Необавештајна роварења обавештајаца у лавиринтима специјалних операција*. Нови Сад: Прометеј.

Миленковић, М. (2020). Западни балкан као поткомплекс у теорији регионалног

безбедносног комплекса. (*Докторска дисертација*). Београд: Универзитет у Београду, Факултет политичких наука.

Милосављевић, Б. (2015). *Правни оквир и пракса примене посебних поступака и мера за тајно прикупљање података у Републици Србији*, Београдски центар за безбедносну политику, Београд, 12–23, стр. 6–8.

Милошевић, М. (2001). *Систем државне безбедности.* Београд: Полицијска академија, Војна штампарија.

Милошевић, М. (2005). *Одбрана од тероризма*. Београд: Едиција, Наука, Свет књиге.

Милошевић, М. (2008). Закони Републике Италије о обавештајно – безбедносном систему и режиму државне тајне, *Страни правни живот, год. 52, бр. 3, 2008, 3/2008*, стр. 262–274.

Милошевић, М. (2011). *(Контра)шпијунажа.* Београд: Медија Центар „Одбрана", Војна књига.

Миљковић, М. (2016). Посебност информационих операција у раду савремених обавештајних служби. (*Докторска дисертација*). Београд: Факултет безбедности.

Миљковић, М. и Марјановић, З. (2023). Мере стратешког одвраћања Руске Федерације: терминологија, дефиниције и неки аспекти примене у сукобу у Украјини 2022. године (The strategic deterrence measures of the Russian Federation: terminology, definitions and some aspects of implementation in the Ukraine conflict in 2022), *часопис Војно дело, број 1/2023,* vol. 75, Београд, стр. I/32–I/45 (pp. II/32–II/45).

Мирковић, Т. (1999). Специјалне акције и операције обавештајних служби Сједињених Америчких Држава, *Војно дело, 3–4*/1999, мај – август, Београд, стр. 11–29.

Митић, М. (1999). *Дипломатија*. Београд: Завод за уџбенике и наставна средства.

Мићовић, М. и Марјановић, З. (2022, September). Critical Infrastructure Defense Policy of The Republic of Serbia in The Light of The Law Provisions, *8th International Professional and Scientific Conference Occupational Safety and Health, Book of Proceedings*, Karlovac University of Applied Sciences, Copyright, Karlovac University of Applied Sciences 2022, pp. 824–831.

Муса, А. (2016). Внешняя политика великих держав. *Международный журнал экспериментального образования*, Политические Науки, 2016. № 9–2. стр. 296–298 (*International Journal Of Experimental Education* № 9, 2016).

О противодействии терроризму. (2006). *Федеральный закон* от 06.03.2006 N 35–ФЗ (ред. от 26.05.2021). Москва, РФ: Принят Государственной Думой.

О федеральной службе безопасности. (2022). *Федеральный закон* от 03.04.1995 N 40–ФЗ (ред. от 04.08.2022) „О федеральной службе безопасности". Москва, РФ: Принят Государственной Думой.

Путник, Н. (2012). Кибер ратовање – нови облик савремених друштвених конфликата. (*Докторска дисертација*). Београд: Факултет безбедности.

Путник, Н. (2022). *Сајбер рат и сајбер мир*. Београд: Универзитет у Београду – Иновациони центар Факултета безбедности и Академска мисао.

Путник, Н. и Милосављевић, Б. (2021). Руске информационе операције у украјинском оружаном сукобу, *часопис Безбедност, година LXIII, 1/2021*, Београд.

Расторгуев, С. П., & Литвиненко, М. В. (2014). Информационные операции в сети Интернет. *Центр стратегических оценок и прогнозов Воробьев А. В.*, РФ, Москва.

Савић, А. (2006). *Обавештајне службе и национална безбедност*, Универзитет у Крагујевцу, Правни факултет, Институт за правне и друштвене науке, Крагујевац.

Савић, А., Делић, М. и Бајагић, М. (2002). *Безбедност света: од тајности до јавности*.

Београд: Институт безбедности, Полицијска академија, Виша школа унутрашњих послова.
Савић, А. и Бајагић, М. (2003). Улога обавештајне активности у спољној политици, *Наука, безбедност, полиција* – Београд, vol. VIII, Број 1, 17-50, 2003.
Служба Внешней Разведки Российской Федерации. (2022). Служба Внешней Разведки Российской Федерации (Structure And Leadership – Foreign Intelligence Service Of The Russian Federation). Преузето 29.12.2022. са адресе http://svr.gov.ru/svr_today/struktur.htm.
Стајић, Љ. (2013). Основи система безбедности, Правни факултет у Новом Саду, Нови Сад, стр. 221. У: Љ. Стајић и Р. Лазић (2015). *Увод у националну безбедност*. Београд: Академија за националну безбедност, Јавно предузеће „Службени гласник", стр. 188.
Стајић, Љ. и Лазић, Р. (2015). *Увод у националну безбедност*. Београд: Академија за националну безбедност, Јавно предузеће „Службени гласник".
Стекић, З. Н. (2021). Војне интервенције и постконфликтна изградња државе у ери униполарности: случај Савезне Републике Југославије, Авганистана и Ирака. (*Докторска дисертација*). Београд: Факултет безбедности.
Стојановић, Б. (2020). Хиперсонично оружје: Поремећај стратешког баланса или нова трка у наоружању?, *Човек, простор, технологија, идеје: међународна безбедност у трећој декади 21. века, НИП* „*Србија и изазови у међународним односима 2020. године*", Министарство просвете, науке и технолошког развоја Републике Србије; реализовао Институт за међународну политику и привреду током 2020. године, стр. 155–177.
Стојановић Такић, Г. (2022). Трансформација рата: од Хладног рата до хибридног ратовања. (*Докторска дисертација*). Београд: Факултет безбедности.
Стратегија националне безбедности Републике Србије. (2019). *Службени гласник Републике Србије, бр. 94/2019.*
Стратегија одбране Републике Србије. (2019). *Службени гласник Републике Србије, бр. 94/19.*
Стратегия национальной безопасности Российской Федерации. (2021). National Security Strategy of the Russian Federation, 2021, *July 2, 2021*. Москва, Кремль, 2 июля 2021 года, N400.
СТРАТЕГІЯ інформаційної безпеки. (2021). *РІШЕННЯ* Ради національної безпеки і оборони України від 15 жовтня 2021 року, Про Стратегію інформаційної безпеки, Введено в дію *Указом Президента України* від 28 грудня 2021 року № 685/2021. Преузето 14.04.2022. са адресе https://www.rnbo.gov.ua/ua/Ukazy/5203.html.
Telegraf.rs. (2019). „*Ruski Posejdon može da uništi svet: Amerika nema odgovor na moćno oružje koje je u stanju da izbriše život na kopnu*". Преузето 14.04.2022. са адресе https://www.telegraf.rs/vesti/svet/3024000-ruski-posejdon-moze-da-unisti-svet-amerika-nema-odgovor-na-mocno-oruzje-koje-je-u-stanju-da-izbrise-zivot-na-kopnu.
Тимофеев, И. Н. (2017). Тезисы по внешней политике и позиционированию России в мире (2017–2024. г.), РФ, Москва, Июнь 2017.
Трбојевић, М. (2017). Необавештајни облик деловања обавештајних служби. *Српска политичка мисао* број 4/2017., год. 24., vol. 58., стр. 319–334.
Уголовный кодекс Российской Федерации. (1996). *Уголовный кодекс Российской Федерации* от 13.06.1996 N 63–ФЗ (ред. от 29.12.2022).
Уредба о ратификацији конвенције о статусу избеглица са завршним актом конференције опуномоћеника уједињених нација о статусу избеглица. (1960). *Службени лист ФНРЈ – Међународни уговори и други споразуми*, број 7/60 од 14.07.1960. године, верзија на снази

од 22.07.1960. године, а унето у базу 02.03.2004. године.

Факултет за дипломатију и безбедност. (2016). *ЦИА и МИ6 у организацији опозиције у Русији*, чланак објављен 14.04.2016. године на сајту факултета за Дипломатију и безбедност у Београду. Преузето 17.09.2022. са адресе https://www.diplomatija.com.

Федеральный Закон „*О Внешней Разведке*". (1996). *О Внешней Разведке*, 10 января 1996 года № 5 – ФЗ.

Федеральный закон „*О противодействии экстремистской деятельности*". (2021). Федеральный закон от 25 июля 2002 г. N 114 – ФЗ „О противодействии экстремистской деятельности", *Савезни закон* број 148 – ФЗ од 27. јула 2006. године (са изменама и допунама 2014, 2020, 2021).

Федеральный Закон N 586 – ФЗ. (2022). *Федеральный Закон О Внесении Изменений В Уголовный Кодекс Российской Федерации и Уголовно* – Процессуальный Кодекс Российской Федерации 29. Декабря 2022 года N 586 – ФЗ. Москва, Кремль, Российская Федерация.

Форца, Б. (2018). Стратегија реформе стратегија. *Војно дело, 3/2018*, Београд, стр. 176–192.

Форца, Б. (2022). Нова стратегија националне безбедности Руске Федерације, *часопис Безбедност, 1/2022*, Београд, стр. 53–71.

Форца, Б. и Стојковић, Б. (2014). О хијерархији стратегијских докумената. *Војно дело,* Безбедност, *лето/2014*, Београд, стр. 145–165.

Цветковић, С. (2009). Методе и облици рада служби државне безбедности у Социјалистичкој Југославији, *часопис Историја 20. века,* број 2/2009, Институт за савремену историју, Београд, стр. 131–144.

Шаваев, А. Г., & Лекарев, С. В. (2003). *Разведка и контрразведка. Фрагменты мирового опыта и теории.* Москва: Издательская группа „БДЦ – пресс".

Шариков, П. А. (2020). Информационные операции в современной военной стратегии США. *Анализ доктринальных документов министерства обороны и государственного департамента США – Россия и Америка в XXI веке*. 2015. Выпуск № 1, Российская Федерация, Москва.

Юрьевич, Д. М. (2014). Разведка В Государственном Механизме США (Историко – Правовой Аспект). *Диссертация на соискание ученой степени доктора юридических наук*, Московский государственный университет имени М. В. Ломоносова, Российская Федерация, Москва.

Ясенев, В. Н. (2017). *Конспект лекций по информационной безопасности*, Институт экономики и предпринимательства, Российская Федерация, Нижний Новгород.

10. БИОГРАФИЈА АУТОРА

Зоран М. Марјановић је рођен 22. октобра 1978. године у Сарајеву, БиХ. Завршио је Војну гимназију у Београду, опште – ваздухопловни смер, у саставу 23. класе. Након завршене гимназије, уписао је Војну академију, одсек Копнена војска, смер пешадија, коју завршава 2001. године у саставу 122. класе са успехом одличан и просечном оценом (9,36) као 1. у рангу у класи – Копнене војске. Након завршетка Војне академије, завршио је следеће студије, усавршавања, курсеве, положио испите – тестове и то: курс за стицање другог степена знања енглеског језика у Центру за изучавање страних језика Министарства одбране Републике Србије, курс за сузбијање криминалитета и корупције (у Центру за безбедносне студије у Београду), оспособљавање за рад на рачунару према енг. *ECDL* стандарду у тестном центру Министарства одбране Републике Србије, успешно положен испит из Енглеског језика по стандарду енг. *STANAG 6001* (два пута). Марјановић је завршио и студије II степена на Факултету политичких наука, Универзитета у Београду, специјалистичке струковне студије на студијском програму Тероризам и организовани криминал (први дипломирао у генерацији са просечном оценом 10,00). Завршетком ових студија стекао је стручни назив струковни политиколог – специјалиста из области тероризма и организованог криминала. Мастер академске студије II степена на Војној академији Министарства одбране Републике Србије, Марјановић је похађао у периоду 2013./2014. годину (мастер студије упоредо са још једним једногодишњим усавршавањем II степена на Војној академији Министарства одбране Републике Србије које је успешно завршио и одбранио завршни рад 2014. године), а мастер рад на мастер студијама одбранио 2015. године. Завршетком ових студија стекао је академски назив мастер менаџер. Уписао је докторске академске студије наука безбедности III степена на Факултету безбедности, Универзитета у Београду школске 2019./2020. годину, на којима је положио све испите и стекао услов за пријаву теме докторске дисертације коју је пријавио 2022. године са насловом „Одвраћање као стратешки концепт у постхладноратовском периоду". Након уписа докторских академских студија Марјановић је објавио више академских радова у оквиру образовно – научног поља Друштвено – хуманистичких наука из области наука безбедности, војних наука и политичких наука у водећим националним и регионалним часописима. Осим тога кандидат је учествовао на две међународне научне конференције. Сви објављени радови су комплетни или по сегментима директно везани за тему докторске дисертације.

Изјава о ауторству

Име и презиме аутора Зоран М. Марјановић

Број индекса 5Д/19

Изјављујем

да је докторска дисертација под насловом
Одвраћање као стратешки концепт у постхладноратовском периоду

• резултат сопственог истраживачког рада;
• да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
• да су резултати коректно наведени и
• да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, _____

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Зоран М. Марјановић

Број индекса 5Д/19

Студијски програм Студије наука безбедности

Наслов рада Одвраћање као стратешки концепт у постхладноратовском периоду

Ментор проф. др Ненад Путник

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао ради похрањивања у **Дигиталном репозиторијуму Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора

У Београду, _____

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић" да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Одвраћање као стратешки концепт у постхладноратовском периоду

која је моје ауторско дело.

Дисертацију са свим прилозима предао сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (*Creative Commons*) за коју сам се одлучио.

(1) Ауторство (CC BY)

2. Ауторство – некомерцијално (CC BY-NC)

3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)

4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)

5. Ауторство – без прерада (CC BY-ND)

6. Ауторство – делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци. Кратак опис лиценци је саставни део ове изјаве).

Потпис аутора

У Београду, _____

1. **Ауторство**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. **Ауторство – некомерцијално**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. **Ауторство – некомерцијално – без прерада**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. **Ауторство – некомерцијално – делити под истим условима**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. **Ауторство – без прерада**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. **Ауторство – делити под истим условима**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.