CIVITAS, 2025, 15(1), 193-211
www.civitas.rs

Zoran M. *M*arjanović[*]
Marija Mićović[**]
Aleksandar Terzić[***]

UDC 327.54(4)
Pregledni rad
Primljen: 13. 05. 2024.
Prihvaćen: 12. 11. 2024.

INSTRUMENTI ODVRAĆANjA U POSTHLADNORATOVSKOM PERIODU

Apstrakt: Oslanjanje država u odvraćanju[1] samo na konvencionalne i/ili nuklearne oružane snage jedne ili više država predstavlja već od pedesetih godina prošlog veka pogrešno razmišljanje u sprovođenju spoljne politike. Na Zapadu je još u periodu posle II svetskog rata zauzeta zvanična politika (Huverova) u spoljnopolitičkim odnosima da je nophodno „igrati prljavo", dok na Istoku čuvena izjava generala Gerasimova da tek završni čin sukoba predstavlja angažovanje oružanih

[1] * Doktor nauka u oblasti nauka bezbednosti, Ministarstvo odbrane Republike Srbije, Beograd, Republika Srbija, ORCID broj 0009-0001-0087-3106; e-mail: marjanovic.cole.zoran@gmail.com
** Doktor nauka u oblasti nauka bezbednosti, Naučni saradnik, Kriminalističko-policijski univerzitet, Beograd, Republika Srbija; e-mail: marijablago*j*evic.bp@gmail.com
*** Master politikolog međunarodnih odnosa, Beograd, Repubilka Srbija; e-mail: at.terzic.93@gmail.com

Odvraćanje, prema Vojnom rečniku i sličnim terminima oružanih snaga SAD, ima sledeće značenje: „sprečavanje delovanja postojanjem verodostojne pretnje od neprihvatljivog protivljenja i/ili uverenje da su troškovi akcije veći od percipirane koristi". Dok je u istom rečniku odvraćanje *(deterrence*) izjednačeno sa terminom strateškog efekta kada se definišu zadaci, misije (odvraćanje, stabilizacija itd.), gde je „lista pojmova strateškog efekta: unaprediti, osigurati, prisiliti, takmičiti se, primorati, sadržati, obmanuti, poraziti, degradirati, odložiti, delegitimizirati, poreći, uništiti, odvratiti, diskreditovati, onemogućiti, obeshrabriti, poremetiti, preusmeriti, angažovati, poboljšati, integrisati, izolovati, ubiti, održavati, upravljati, neutralisati, sprečiti, zaštititi, stabilizovati, potisnuti, sinhronizovati" (DoD Dictionary of Military and Associated Terms, 2021, p. 2, 63). Odvraćanje koje postoji više od tri četvrtine veka (u ovom određenju), evoluiralo je zajedno sa promenama strateških uslova koji diktiraju način suprotstavljanja savremenim pretnjama.

snaga ukazuje da postoje neki sukobi koji traju u miru i da su oni bitniji, delotvorniji od oružanih. Postupanja državnih organa u odvraćanju sa ovakvim i sličnim usmerenjima najviših državnih rukovodilaca su obuhvatala prelazak sa „tvrde moći" na „meku moć" kao dominantnu u realizaciji spoljnopolitičkih sukoba. Kulminacija praktične primene nove „pametne moći" je registrovana u posthladnoratovskom periodu primenom koncepta odvraćanja, gde su nove tehnologije diktirale modifikaciju odvraćanja i njegov novi tok prilagođavanja informaciono-tehnološkim vrtoglavim promenama u ***životu*** i radu ljudi, pa samim tim i država u kojima ***žive*** (borave).

KLJUČNE REČI: *odvraćanje, instrumenti, službe bezbednosti, sajber odvraćanje, koncept Izraela.*

1. **Uvod**

Istraživanje započinjemo njegovim predmetom što predstavlja ispitivanje uslova koji su doveli u posthladnoratovskom periodu do novog koncepta odvraćanja država danas, sa posebnim osvrtom na Izrael, a sa ciljem naučnog opisa odvraćanja kako kroz analizu istraživanja sprovedenih od strane dela teoretičara koji se bave ovom problematikom na Zapadu, tako i kroz prvi javno obelodanjeni i prevedeni najbitniji strateški dokument u Izraelu koji uređuje ovu oblast i određuje državi dostupne instrumente za ovu vrstu angažovanja.

Da odvraćanje nije samo svedeno na upotrebu oružane sile jedne države sagledavamo već u početnim konstatacijama Džozefa S. Naja (*Joseph S. Nye*) u prvom poglavlju rada gde se sa pozicije moći sagledava mogući koncept odvraćanja jedne države. Pomeranjem „centra gravitacije" odvraćanja od isključive veze i oslanjanja na oružane snage, odnosno vojne moći jedne ili više država, tzv. *tvrde* moći sve brže prema *mekoj*, pa *pametnoj* moći konstatujemo da savremene pretnje, čiji je prostor delovanja pomeren u informaciono-telekomunikacionu sferu, sajber prostor, svemir, ne predstavljaju budućnost, već sadašnjost u odvraćanju država. Prinuda, odnosno instrumenti koje koriste države u odvraćanju su se iz „tenkova, aviona, oklopljenih oruđa i drugih

borbenih sredstava" težišno prvenstveno preselile u sukob dronovima (bespilotnim letelicama), putem računara, medija, u virtuelni svet, gde informacione operacije čine jedan od bitnijih instrumenata prinude. Obmane, dezinformacije, laži postale su instrumenti koji se svakodnevno koriste u realizaciji ciljeva velikih sila. Sajber odvraćanje je nešto što mora biti jedan od instrumenata odvraćanja, ali tromost glomaznih bezbednosno-obaveštajnih sistema država dovodi do toga da je pitanje koliko brzo mogu ove promene (odnosno nove pretnje) koje se odvijaju (koje nastaju) neverovatnim brzinama da budu implementirane u organizaciju. Strukture koje treba da se suprotstavljaju ovim nevidljivim (tajnim) pretnjama su prvenstveno *službe bezbednosti*[2] države, odnosno trebalo bi to da budu. Kada govorimo o odvraćanju i angažovanju državnog sektora, tada se misli na nosioce određenih angažovanja, dok je nedržavni sektor izuzetno prisutan u ovoj sferi sa obavezama koje bi trebalo da budu predviđene najvišim strateškim dokumentima države. Kada govorimo o tajnim pretnjama, tada prvenstveno mislimo na preduzimanje visokog stepena tajnosti tokom priprema, zatim tokom same realizacije određene akcije – operacije, gde se tajnost odnosi i na prikrivanje stvarnog nosioca, odnosno vrlo često i na sprovođenje obmane kako bi stvarni učinioci ostali nepoznati. Službe bezbednosti predstavljaju „produženu ruku" politike i, pored pružanja informacija (preduzimanjem obaveštajnih, kontraobaveštajnih, bezbednosnih aktivnosti) političkom rukovodstvu u vezi sa nacionalnom bezbednosti države, predstavljaju kako defanzivni, tako i ofanzivni instrument (pored navedenih aktivnosti, preduzimanjem neobaveštajnih aktivnosti službi bezbednosti, kao i angažovanjem velikog broja drugih entiteta, institucija, firmi, kompanija i sl.) pre svega velikih sila u primeni prinu-

[2] *Službe bezbednosti*, kao pojam u ovom istraživanju, odnosiće se na sve državne službe koje se bave kontraobaveštajnim, obaveštajnim, neobaveštajnim i bezbednosnim aktivnostima koje predstavljaju najčešće preduzimanje tajnih delatnosti. Službe bezbednosti predstavljaju deo jedinstvenog bezbednosno-obaveštajnog sistema jedne države. U Republici Srbiji je Zakonom o osnovama uređenja službi bezbednosti Republike Srbije određeno šta sve spada u službe bezbednosti, dok u drugim državama iste ili slične organizacije i službe nose nazive elementi, kancelarije, uprave, agencije, državne službi i sl. Radi izbegavanja različitih terminoloških određenja, za sve ove celine koristimo jedinstven termin – službe bezbednosti.

de u odvraćanju. Sagledavanjem pretnji na dnevnom nivou (radi brzine njihovih promena) jedino je moguće primeniti kvalitetno odvraćanje i preventivno delovati na određenu pretnju.

2. Instrumenti odvraćanja u posthladnoratovskom periodu

Američki teoretičar, tvorac pojma „meka" moć u spoljnoj politici, Džozef S. Naj, ukazuje na izmenjeno razumevanje prirode moći u savremenom svetu, razmatrajući sposobnost države da utiče na druge, da nameće svoju volju primenom demokratije (unutrašnje i spoljne politike) ili masovne kulture itd. a ne vojnom i ekonomskom silom (što bi predstavljalo „tvrdu" moć).

Iz tog razloga, u teoriju međunarodnih odnosa uvodi još jedan termin – „pametnu" moć koji kombinuje prinudu, ekonomski pritisak i ubeđivanje. Naj navodi da je informacija uvek značila moć, a da savremena informaciona tehnologija širi informacije šire i brže nego ikada ranije u istoriji. Zbog toga je značaj informacije kao elementa moći porastao. Naj ističe da se priroda moći promenila u poslednjih pedeset godina, posebno nakon poslednje informacione revolucije koja je učinila računare i internet neophodnim u svim oblastima života. Naj ističe da će nuklearno odvraćanje, oružane snage u zemlji i stacioniranje trupa u inostranstvu biti važni čak i u informacionom dobu, ali neće biti dovoljni da obezbede nacionalnu bezbednost (Putnik, 2012). Ovde napominjemo da je Naj još 1990. godine nagovestio transformaciju strategije odvraćanja koja bi se danas mogla uporediti sa strategijom sajber odvraćanja i najavom potrage za drugim instrumentima odvraćanja.

U svom istraživanju, Sten Rining (*Sten Rynning*) navodi obnovljenu stratešku konkurenciju između Ruske Federacije (RF) i NATO-a, što je dovelo do razvoja strategija odvraćanja u svetlu raznolikosti strateških perspektiva između država NATO-a. NATO percipira i reaguje na ratovanje nove generacije od strane Ruske Federacije, što u suštini predstavlja strategiju prinude, često usmerenu na informacioni prostor protivnika. Sukobi nove generacije koriste niz alata za ubeđivanje i odvraćanje neželjene politike, a što je najvažnije, u ovoj vrsti sukoba se ne pravi razlika između rata i mira. NATO je primetio nekoliko novih načina

razmišljanja koje je Ruska Federacija primenila o brojnim političkim aspektima, naime o otpornosti društva, poboljšanju saradnje bezbednosnih službi, sajber bezbednosti i potrebi za brzim donošenjem odluka. Zajedničko odeljenje za obaveštajne i bezbednosne aktivnosti osnovano je u NATO-u 2014. godine i predstavlja jedan od instrumenata za rano otkrivanje namera Ruske Federacije. Međutim, nedostatak je što političko-vojni štab NATO-a ne okuplja bezbednosne službe država članica, već samo koordinira, a ono što države članice nude integriše se u kolektivni pregled politike i delovanja Ruske Federacije. Što se tiče hibridnih pretnji, ova koordinacija je posebno sporna, jer seje seme konfuzije u savezničkim informacionim prostorima. NATO je poboljšao svoju sajber odbranu i koordinaciju bezbednosnih službi, a koordinacija sa Evropskom unijom u vezi sa hibridnim pretnjama je posebno poboljšana od 2016. godine kada je doneta zajednička deklaracija, što je dovelo do zajedničkog programa rada sa Centrom za odlučno suprotstavljanje hibridnim pretnjama koji se nalazi u Helsinkiju (*Centre of Excellence for Countering Hybrid Threats, located in Helsinki*). NATO uvodi kombinaciju odvraćanja poricanjem (sukob u sivoj zoni, društvena otpornost, reakcija i raspoređivanje raspoređenih snaga za suprotstavljanje ograničenom otimanju teritorije) i odvraćanja kažnjavanjem (pun lanac reakcija i snaga koje se mogu rasporediti, od konvencionalnih do nuklearnih) kao odgovor na aneksiju Krima od strane Ruske Federacije 2014. godine. NATO je u velikoj meri posvećen odvraćanju Ruske Federacije kažnjavanjem. U Hladnom ratu, strategija fleksibilnog odgovora NATO-a odražavala je politički kompromis (Rynning, 2021).

Nacionalna bezbednost može biti ugrožena ne samo od strane oružanih snaga, već i od strane vlada, grupa, pojedinaca i drugih nedržavnih aktera ili onih koji se predstavljaju kao nedržavni akteri.

Naime, u eri razvoja novih tehnologija, primat dimenzije sukoba više nije kopno, vazduh ili more. Umesto toga, pre nekoliko godina je to postala dimenzija sajber prostora. Velike sile (Sjedinjene Američke Države, Ruska Federacija i druge zemlje) odavno su formirale snage i centre koji se bave zaštitom, kao i sukobima u sajber prostoru. Generalni sekretar NATO-a, Jens Stoltenberg, dao je 2018. godine izjavu u kojoj je izneo svoje mišljenje o načinu tumačenja člana 5 Osnivačkog ugovora NATO-a o pitanjima sajber napada sa teritorije Ruske Federacije. Ge-

neralni sekretar NATO-a, alijanse za koju se zna da je predvode SAD, tumači napade u sajber prostoru kao napade na članice NATO-a.

U zavisnosti od prirode sajber napada, NATO namerava da koristi član 5 i da o tome obavesti sve zemlje, što podrazumeva da se ovaj član neće automatski primenjivati za svaki sajber napad. Međutim, generalni sekretar nije želeo da objavi konkretne uslove pod kojima će se ovaj član koristiti. Ono što je pratilo sve sajber napade u poslednjih nekoliko godina bile su optužbe uglavnom od strane najviših zvaničnika SAD, Francuske i Velike Britanije o počiniocima sajber napada za koje se pretpostavljalo da su iz Ruske Federacije, kao i demanti iz Ruske Federacije (već dugi niz godina u etru, potpuno kontradiktorne izjave i na Zapadu i na Istoku). Samo nekoliko godina kasnije, 2021. godine, pored pomenute četvrte dimenzije sukoba (sajber prostor), NATO je dodao i petu dimenziju sukoba (u svemiru), što bi moglo biti proširenje člana 5 za njegovu aktivaciju. U njemu se navodi da bi članice Alijanse bile spremne da odgovore i na napade u svemiru i iz svemira (Stoltenberg, 2018; 2021).

Soesanto i Smits (Stefan Soesanto & Max Smeets) posmatraju sajber odvraćanje u vojnom konceptu, i prema njima, ono ima najmanje tri različita značenja. Može se odnositi na odvraćanje od (vojnog) napada, zatim na upotrebu (vojnih) sredstava za odvraćanje (vojnih) sajber napada i upotrebu (vojnih) sajber sredstava za odvraćanje kao (vojni) sajber napad. Naučnici se trenutno ne slažu oko stepena u kojem je generalno moguće odvratiti neprijateljski sajber napad, što verovatno proizilazi iz zapažanja da sajber prostor sadrži mnoštvo aktera sa pristupom ofanzivnom sajber oružju. Neki veruju da je strateška vrednost štete koju uzrokuju sajber napadi generalno ograničena. Pretnje od sajber napada, stoga, nemaju dovoljno mogućnosti za efikasno odvraćanje. Zagovornici sajber odvraćanja generalno govore o sledeće četiri logike odvraćanja: *odvraćanje uskraćivanjem* (što je sinonim za sajber bezbednost), *odvraćanje kažnjavanjem* (troškovi će nadmašiti koristi), *odvraćanje ispreplетavanjem* (međuzavisnost može obeshrabriti države da pokrenu sajber napade) i *odvraćanje delegitimizacijom* (smanjenje bojnog polja samo na vojne borce). Sajber prostor može biti prepoznat kao novi domen ratovanja, ali van vojske, korisnost sajber napada i sajber odbrane u podršci odvraćanju je još uvek neizvesna. Politički motivisanih sajber na-

pada sa strateškim uticajem je malo, većina dokumenata je zaista visoko poverljiva, ali postoji mali pristup sajber operaterima, a postojeće vojne sajber organizacije su još uvek u razvoju. Stoga, Soesanto i Smits navode četiri buduća pravca istraživanja sajber odvraćanja: sajber odvraćanje u sveobuhvatnijim pozicijama odvraćanja u kontekstu konkurencije u više domena, veći fokus na tehničke aspekte na operativnom i taktičkom nivou, veći naglasak na kompetenciji i na kraju, obuzdavanje i ublažavanje neprijateljske agresije u sajber prostoru (Soesanto & Smeets, 2021). Ne postoji konsenzus među naučnim istraživačima u ovoj oblasti.

Od napada 11. septembra 2001. godine, studije o borbi protiv terorizma fokusirale su se na pitanje da li nedržavni akteri mogu da odvrate. Šamir (Eitan Shamir) pronalazi vezu između odvraćanja i nasilnih nedržavnih aktera u kontekstu sprečavanja terorističkih pretnji. Šamir navodi da je Izrael razvio koncept odvraćanja od nasilnih nedržavnih aktera. On uključuje aspekte odvraćanja usmerene na obuzdavanje sposobnosti protivnika. Pored obuzdavanja, Šamir navodi da je cilj obrazovanja pristup zasnovan na procesima koji predviđaju kontinuirani odnos između odvraćajućeg i odvraćenog. Stavovi da je teroristička grupe (posebno verski motivisane) teško odvratiti, sadržani su uglavnom u sledećim faktorima: zato što često nisu monolitne organizacije, sastoje se od skrivene mreže, autonomnih ćelija, ne postoji obavezujući vođa, šef, rukovodilac, osoba sa kojom bi predstavnik države komunicirao ili mogao da komunicira; takođe, kada govorimo o ideologijama, one isključuju normalne diplomatske pregovore i sl. Dakle, Šamir smatra da se odvraćanje nasilnih nedržavnih učesnika ne može postići u potpunosti i da je restriktivan pristup ovoj vrsti odvraćanja pre potreban.

Ovo implicira da se ne očekuje da efekat odvraćanja države proizilazi iz simboličkih napada na nasilne nedržavne učesnike, već iz ponovljenih protesta, odgovora, kad god se neka norma prekrši (prema Šamiru, tzv. pristup košenja trave). Restriktivno i kumulativno odvraćanje nasilja od strane nedržavnih aktera više je inspirisano kriminološkim shvatanjima pojma, nego hladnoratovskim konceptima apsolutnog odvraćanja (Shamir, 2021). Kao i u velikom broju životnih primera, za ovaj oblik odvraćanja možemo reći da se strateško iskustvo i kultura neće samo kopirati iz jednog entiteta u drugi (kako je naglasio Šamir), dok bismo ovome mogli dodati i kompletne ekonomske, vojne, političke i druge

sile koje imaju važan uticaj na koncepte odvraćanja i važno je znati da se odvraćanje neće samo kopirati iz jedne države u drugu ili iz jedne kulture u drugu, već da se mogu koristiti neka pozitivna rešenja. Praktično, pretnja sankcijama neće dati iste rezultate prema ekonomski nezavisnoj državi i državama koje nisu nezavisne, i prema određenoj definiciji, nikada neće biti korišćena samo jedna vrsta aktivnosti u odvraćanju, već niz aktivnosti u koje su uključene ili njima upravljaju službe bezbednosti kako bi se ostvarili politički ciljevi jednog društva, u jednom trenutku države, u drugom možda isključivo samo takozvanih elita određenog društva. Neki teoretičari definišu hibridno ratovanje kao brak između konvencionalnog odvraćanja i pobunjeničke taktike. Pitanje uopšte je da li je to novi oblik ratovanja ili strategija koju države koriste da bi ostvarile prvenstveno političke ciljeve i u miru i u ratu, a najčešće primenom subverzivnih aktivnosti (neobaveštajnih aktivnosti). Hibridni rat eksploatiše nacionalističke identitete, čime se prikriva odgovornost izvršilaca i čak dobija politička podršku među stranim posmatračima.

Strategija Ruske Federacije ima za cilj da oslabi spremnost NATO-a da se nosi sa sopstvenim pretnjama odvraćanja (i obrnuto). Vojni stratezi su odavno svesni da bi, kako bi se postigla pobeda, strana u sukobu trebalo da se pobuni kako bi lakše savladala tog protivnika. Direktne vojne sukobe države izbegavaju, a oni bi koristili samo velikim silama. Shodno tome, suptilnije i indirektne tehnike rešavanja problema su prikladnije. Ove tehnike uključuju upotrebu propagande za mobilizaciju podrške pobunjenika i demoralizaciju neprijateljskih snaga, kao i napad na slabe tačke suprotstavljenih snaga. Krizne situacije u zemlji ili na planeti (kao što su epidemije, pandemije) dovode do pojave nove vrste pretnje koja, bez obzira na prioritetno angažovanje, npr. zdravstvenog aparata u zemlji, zahteva angažovanje službi bezbednosti, počev od registrovanja pretnji, nabavke sredstava, opreme, uređaja širom planete, sprečavanja dezinformacija, sprečavanja defetizma i panike, kao i drugih aktivnosti (Marjanović i Mićović, 2022).

Kao jedan od važnijih instrumenata odvraćanja navodimo „kopnenu moć", koja u svetlu ekonomske nezavisnosti, kako energetske tako i poljoprivredne, i u pogledu drugih resursa neophodnih za funkcionisanje preduzeća, organizacija, stanovništva, vojske i države, predstavlja moć koja anulira sve instrumente odvraćanja vezane za prinudu u

ekonomskoj sferi i sankcije u ovoj oblasti (Marjanović i Mićović, 2023). Dakle, ekonomske aktivnosti (sankcije) primenjene na Saveznu Republiku Jugoslaviju 1999. godine i one korišćene protiv Ruske Federacije u 21. veku, kao energetski nezavisne zemlje, ne mogu imati isti efekat na rukovodstvo zemlje i narod uopšte.

Postoje različiti instrumenti koji se mogu primeniti u hibridnom ratovanju. *Propaganda* – predstavlja uticaj na stavove članova ciljanog društva i služi da ometa sposobnost ciljane grupe da se osloni na podršku javnosti u sprovođenju svojih politika i mobilizaciji svojih resursa. Sledeća je *špijunaža* putem koje agenti tajno prikupljaju obaveštajne podatke kako bi sukobljenoj strani dali prednost u prinudnim pregovorima. Zatim, upotreba agenata u ciljanom, namernom *širenju lažnih informacija* među nesumnjivo članovima javnosti u vezi sa stvarnim namerama određenih organizacija ili stvaranjem nesporazuma i razdora (koji još uvek ne postoji) unutar ciljanog društva. Sledeći instrument je kriminalno ometanje, pri čemu agenti strana u sukobu učestvuju u napadima, sajber napadima, sabotažama ili otmicama i drugim vrstama subverzije. Stvaranje, obuka i korišćenje *pete kolone*[3] (pojedinci, grupe, koji obično deluju tajno i koji su ugrađeni u mnogo veću populaciju protiv koje deluju), u ulozi „neobeleženih vojnika" omogućavaju posedovanje kontrolnih punktova, zauzimanje vladinih zgrada i drugih objekata, osoba itd. od strateškog značaja (do određenog trenutka). Strana u sukobu može pokrenuti granične sukobe kako bi uznemirila drugu stranu i testirala njene slabosti, a zatim nastaviti sa iscrpljivanjem snaga i resursa i povlačenjem iz centra akcije upotrebom gerilaca. SSSR je primenio ove tehnike odmah nakon Drugog svetskog rata, sponzorišući komunističke pokrete u Evropi i na drugim lokacijama kako bi potkopao kapitalistički poredak. Moderna vojna doktrina Ruske Federacije naglašava potrebu da se odgovori i na spoljne i na unutrašnje pretnje, ne samo od drugih velikih sila, već i od subverzivnih organizacija koje

[3] Izraz *peta kolona* potiče još iz španskog građanskog rata kada je 1936. godine španski general Emilio Mola u radio-proglasu stanovnicima Madrida objavio da se prema glavnom gradu kreću četiri nacionalističke kolone, ali da u gradu postoji i *peta* koja će im udariti u leđa. Ovaj termin se zatim u II svetskom ratu koristio mnogo u opisu svih saradnika neprijatelja koji su tajno delovali u njihovu korist, pa i decenijama nakon ovog rata.

deluju u oblastima koje kontroliše Ruska Federacija. Vojni teoretičari su decenijama unazad bili svesni da su SAD stekle prednost u preciznim udarima i informaciono-komunikacionim tehnologijama i da države mogu postati predmet informacionog rata. Početne faze rata uključivale bi kampanje dezinformisanja. Informaciona superiornost je postala neophodna u savremenom ratovanju (Lanoszka, 2016). S obzirom na to da teorijska definicija hibridnog rata još uvek „luta" i da ne postoji sveobuhvatna definicija ovog fenomena, razlog je taj što mnogi koriste ovaj termin u neskladu sa onim što žele da kažu, tj. da je hibridni rat u toku, a nije isključeno da postoji i tekući deo tajnih operacija ili neobaveštajnih aktivnosti službi bezbednosti. Kada se gore navedeno dešava, trebalo bi da to nazovemo pravim imenom, obaveštajnim, kontraobaveštajnim ili neobaveštajnim aktivnostima službi bezbednosti koje su manje-više prisutne od postojanja službi bezbednosti, osim tehnika prilagođenih napretku novih tehnologija. Kada koristimo konceptualnu definiciju rata, trebalo bi da pođemo od njegove teorijske definicije, kao i pravne, normativne, i da vidimo da li je ovaj koncept hibridnog rata adekvatno definisan (Lanoszka, 2016).

Profesor Ilija Kajtez je izneo[4] podatak da su još posle Drugog svetskog rata počele pripreme za špijuniranje širom planete od strane SAD i da su 1970. godine službe bezbednosti SAD CIA, NSA i Nemačke BND zaključile tajni sporazum o ilegalnom globalnom prisluškivanju velikog dela planete (tačnije 130 zemalja i UN). Operacija je nazvana *Rubicon* (kodni naziv za BND, prelazak na Rubikon znači, još od vremena Julija Cezara, preduzimanje nepovratnog koraka koji počinje u određenom kursu. Naziv je simboličan, iako je operacija prvobitno imala drugi kodni naziv – *Teazaurus*), dok je ista ova operacija u CIA delovala pod kodnim imenom *Minerva*. Većina ovih aktivnosti službi bezbednosti sprovedena je preko kompanije u Švajcarskoj *Kripto AG*, koju je navodno osnovao Hagelajn (*Boris Hagelajn*), koji se bavio šifrovanjem. Ova kompanija je u svom radu ostvarivala veliki profit, a novac je navodno usmeravan u crne fondove službi bezbednosti SAD i Nemačke, odnosno korišćen je za potrebe ekonomskih aktivnosti ovih službi, koje su najve-

[4] Ilija Kajtez, profesor, penzionisani pukovnik Ministarstva odbrane Republike Srbije, gostujući u TV emisiji u Beogradu 21. 08. 2022. godine izneo je navedene podatke.

rovatnije osnovale CIA i BND.

BND je navodno prodao svoju imovinu tek u septembru 1993. nakon hapšenja Hansa Bilera (*Hans Biler*) u Teheranu, gde je proveo devet meseci kada je BND izgubio podršku nemačke vlade za ovu operaciju, dok su SAD navodno nastavile ove ilegalne aktivnosti do 2018. Početkom 2020. Miler (*Peter Miler*) je snimio dokumentarni film o ovoj operaciji za drugi program televizije u Nemačkoj, gde se SFRJ takođe pominje kao zemlja koja je bila kupac uređaja za šifrovanje još 1957. i 1978. godine, kao i nemački i švajcarski javni servisi ZDF i SRF i američki Vašington post. Neke zemlje su otkrile da su to uređaji koje druga strana može da čita, uključujući Austriju i SFRJ. S obzirom na to da je reč o izuzetno velikoj operaciji, na planetarnom nivou, treba biti oprezan u sagledavanju ovih podataka, koje ponovo ustupaju isti akteri koji su sve vreme učestvovali u nizu, između ostalog, neobaveštajnih aktivnosti SAD, Nemačke i Švajcarske, te da se ne radi o pripremi nove ili obnovljene stare operacije.

Jakobsen (*Peter Viggo Jakobsen*) vidi odvraćanje u drugom obliku, onom koji uključuje i državne i nedržavne aktere, a reč je o *multinacionalnim operacijama*. Jakobsen ovu vrstu operacije vidi kroz sprovođenje napada na mirovne snage (one sastavljene od zapadnih zemalja) koje su bile raspoređene na teritoriji bivše SFRJ. Upotrebu mirovnih snaga u drugim zemljama Jakobsen opisuje kao delovanje u promenljivom kontekstu u kome su stroga razgraničenja između odvraćanja i prinude urušavaju. Jakobsen posmatra ova razgraničenja kroz sledeće faktore: pretnju prinudom koja može da demonstrira sposobnost da se protivnik brzo i uz minimalne troškove pobedi; rok za usklađenost treba da stvori osećaj hitnosti; uverenje da neće biti dodatnih zahteva nakon usklađenosti i konačno, uključivanje pozitivnih podsticaja za smanjenje troškova usklađenosti.

Sledeća stvar koju Jakobsen ističe jeste potreba da se istovremeno odvraćaju i prisiljavaju različiti učesnici na i van bojnog polja tokom multinacionalnih operacija. Jakobsen tako razlikuje četiri grupe učesnika odvraćanja (pozitivne i negativne) u mirovnim operacijama, i to: borce koji koriste silu na bojnom polju; saveznike koji pružaju materijalnu podršku borcima; pristalice boraca, koji blokiraju akcije u regio-

nalnim ili globalnim institucijama; kao i druga lica, posmatrače na bojnom polju na globalnom nivou koji ne izvode borbene akcije. Jakobsen zaključuje da bi odvraćanje bilo uspešno, učesnici odvraćanja ne mogu se oslanjati samo na pretnje i upotrebu sile, to nije dovoljno. Prema njegovim rečima, potrebno je dopuniti njihovo dejstvo tako da se upotreba prinude dopuni ubeđivanjem i ohrabrivanjem, osmišljavanjem, sprovođenjem strategije uticaja koja bi se u potpunosti oslanjala na sve ove tri komponente (Jakobsen, 2021). U ovom istraživanju, Jakobsen je potvrdio da specifičnost određenih kultura, zemalja, fenomena, a posebno u ovom slučaju aktivnosti, ima svoje karakteristike, faktore koji čine konkretno odvraćanje jedinstvenim, tako da šablon primene u drugim slučajevima nije adekvatan način povezivanja sa odvraćanjem. Međutim, mogu se videti dobra rešenja i moguća se mogu implementirati. U sledećem poglavlju videćemo kako Izrael reguliše odvraćanje.

3. Specifičnosti odvraćanja u strategiji izraelskih odbrambenih snaga

Analiza strateškog dokumenta Izraela, strategije Izraelskih odbrambenih snaga (IDF), ukazuje da strateški odnos između dve države, odnosno države i velike sile, Izraela i SAD, igra važnu dvostruku ulogu u izraelskom odvraćanju, što se ogleda u sledećem. Veoma bliska saradnja sa SAD povećava domet Izraela za političke i operativne manevre kao odgovor na agresiju protiv Izraela, i poboljšava operativne sposobnosti Izraela da nanese štetu svojim neprijateljima kroz veće jačanje snaga, kao i kroz pretnju američkom intervencijom u njegovo ime. Prilagođavanje koncepta odvraćanja iz 21. veka u politici SAD, promena prirode američke posvećenosti kao dela proširenog modela odvraćanja, izraelsko odvraćanje u 21. veku i proširenje koncepta odvraćanja kako bi se u strategije uključili nevojni alati i jačanje veze između odbrane i odvraćanja su glavne karakteristike ove strategije (Golov, 2016).

U avgustu 2015. godine objavljena je prva obelodanjena strategija Izraelskih odbrambenih snaga, prevedena na engleski jezik u avgustu 2016. godine (*Israel Defense Forces Strategy*, 2016). Koliko ozbiljno jedna od najugroženijih zemalja na planeti shvata mesto i ulogu bezbed-

nosnih službi za opstanak nacije i poštovanje njenih pripadnika, zarad odvraćanja, najbolje možemo videti posmatrajući citat koji je izdvojen u strategiji Izraelskih odbrambenih snaga. To je misao Jadlina (Amos Yadlin), bivšeg šefa Vojnoobaveštajne službe Izraela, koja glasi: „Hamas i Hezbolah nismo uništili, ali smo uspeli da uspostavimo odvraćanje. To je u osnovi zato što smo ih snažno udarili i zato što su teroristi, na neki način, postali kao nepotpuni državni entiteti, ali su kao poludržavni entiteti. Teroristi su otkrili da kada su odgovorni za svoju ekonomiju, za obrazovanje, za živote svog naroda, odjednom se ne usuđuju da koriste teror ceo dan i to mnogo govori o efektima odvraćanja u državi" (Grejem, 2016, str. 24). Odvraćanje se stvara u percepciji, ali se zasniva i na fizičkim i konkretnim elementima. Izraelsko odvraćanje oslanja se na superiornost izraelskih odbrambenih sistema, ali sa naglaskom da je ograničenije nego u prošlosti, jer se pretnja promenila. Odvraćanje mora biti specifično i prilagođeno svakom neprijatelju. Odvraćanje protiv bilo kog neprijatelja mora biti generalizovano i kumulativno za sve vreme (kako bi se održala postojeća situacija), biti u kontekstu određene krize – specifično i precizirano tako da je neprijatelj primoran da deluje ili izbegne određenu akciju kako bi zaustavio rat ili sprečio pogoršanje situacije ili situacija. Prema ovoj strategiji, sledeće komponente su komponente odvraćanja: verodostojna pretnja teškim ofanzivnim operacijama koja se zasniva na izgradnji sile, javna percepcija akcija koje pokazuju našu spremnost da preuzmemo rizike i ograničene ofanzivne akcije. Neophodno je da oružane snage održe imidž odvraćanja i sposobnosti, kao nepredvidivog neprijatelja sposobnog da reaguje na veoma ozbiljan način. Izrael periodično izvodi vazdušne napade u Siriji i Libanu kako bi nametnuo „crvene linije" protiv terorističke organizacije, kao što je vazdušni napad u decembru 2015. na Samira Kuntara, iz vrha operative Hezbolaha (Graham, 2016, p. 25).

Akcije odvraćanja neprijatelja biće sprovedene u okviru *Kampanje između ratova* (Campaign between wars – CBW). Obrazloženje za upotrebu sile u CBW jeste slabljenje komponente negativne sile, minimiziranje neprijateljskih mogućnosti i jačanje sopstvenih snaga, stvaranje optimalnih uslova za pobedu u budućem ratu, stvaranje legitimiteta za sprovođenje izraelske akcije i poricanje legitimiteta neprijateljske akcije. Takve akcije, koje se sprovode između ratova, zahtevaju multidiscipli-

narni koncept, tj. korišćenje sledećih sfera: vojne, ekonomske, pravne, medijske i političke, a ideja operacija treba da bude sa jednim ciljem – strateškim. Takve ideje za upotrebu ofanzivne sile uključuju upotrebu, kombinaciju tajnih operacija (*Covert operations*) i prikrivenih operacija (*Clandestine operations*), na svim frontovima i dimenzijama van granica Izraela. Važno je naglasiti da se ova politika zasniva na podacima dobijenim angažovanjem službi bezbednosti i da je usmerena na nanošenje štete neprijateljskim akcijama ili namerama. Potrebno je napomenuti da ovaj dokument reguliše otvorenu akciju za stvaranje odvraćanja, što naglašava granice izraelske obuzdanosti. Vodeći principi za upotrebu sile u CBW tajnim i prikrivenim akcijama ili kampanjama su da su takve operacije inicirane, kontinuirane i kontrolisane, operacije u kojima snage deluju na tajan i prikriven način u kratkim vremenskim periodima, da ih karakteriše međuorganizaciona saradnja operativne prirode kao i sa bezbednosnim službama, međunarodna saradnja u cilju obavljanja obaveštajnog rada i osujećivanja neprijatelja i očuvanja legitimiteta delovanja izraelske odbrane i smanjenja legitimiteta neprijateljskog delovanja, kao i delovanje u javnoj percepciji, ekonomskoj i pravnoj oblasti kao deo napora da se smanje mogućnosti i legitimitet neprijatelja uz potrebu za pristupačnim i tačnim obaveštajnim podacima (Graham, 2016, p. 26).

Kako načelnik Generalštaba oružanih snaga Izraela Eizenkot (*Chief of General Staff Lt. Gen. Gadi Eisenkot*) iznosi svoje mišljenje o „drugačijoj situaciji": „U prošlosti smo imali vojsku u jednoj od dve situacije, bila je spremna za rat ili je bila u ratu. Ali trenutno to nije stvarnost. Ne spremamo se za rat, niti smo u ratu. Nalazimo se u drugačijoj situaciji gde smatramo da se cela kampanja sa drugačijim percepcijama oslanja na bezbednosne službe i tajne i otvorene sposobnosti da spreče našeg protivnika da ojača, da pokušaju da oslabe neprijatelja na način koji mu neće doneti ubrzanje" (Graham, 2016, p. 26). Posle iznošenja citata Amosa Jadlina (Amos Yadlin) ovo viđenje Eizenkota je takođe naglašeno u strategiji Izraelskih odbrambenih snaga, gde se još jednom potvrđuje da je ključ svih aktivnosti u periodu CBW, zapravo, aktivnost službi bezbednosti. Iz ovog segmenta strategije, svi analitičari na planeti trebalo bi da zaključe mnogo toga o zemlji koja možda ima najviše iskustva u pitanjima suprotstavljanja pretnjama nacionalnoj bezbednosti.

Izuzetno je važno naglasiti da je od teorijskog koncepta odvraćanja, Izrael možda najviše postigao svojim radom, gde odmah predlaže izgradnju snaga za CBW, gde je potrebno postupiti na sledeći način: uspostaviti koordinacioni centar za CBW operacije koji uključuje međuorganizacione i međuministarske elemente, zatim razviti kapacitete za tajne i prikrivene operacije za CBW (Graham, 2016, p. 44). S obzirom na to da operacije ovog tipa uvek uključuju veliki broj specijalista iz jedne zemlje, koji nisu zaposleni u jednoj organizaciji, centar koji je pomenut predstavlja prvi korak u formiranju snaga, dok je stvaranje kapaciteta za prikrivene i prikrivene akcije klasičan „zanatski deo" svake bezbednosno interesantne profesije neophodne za sprovođenje takvih operacija. Jedna od takvih profesija je segment poznavanja aktuelnih trendova u informaciono-telekomunikacionim sistemima - ITS. Sajber sfera je jedno od područja odbrane gde se sprovode takve operacije, ofanzivne aktivnosti i prikupljanje obaveštajnih podataka. Izgradnja snaga u ovoj sferi zasniva se na sledećim akcijama. Osnivanje sajber ogranka koji će biti direktno potčinjen sedištu načelnika Generalštaba Oružanih snaga Izraela za rad i izgradnju sajber kapaciteta. Taj ogranak ima obavezu da planira, organizuje i sprovodi sukobe u sajber prostoru. Međutim, kao posebna obaveza dat je razvoj tehnoloških kapaciteta za sajber odbranu svih operativnih sistema i odbrambenih kapaciteta sistema podrške (ljudstvo, logistika) (Graham, 2016, p. 44).

Radi poboljšanja uslova rada i izgradnje mogućih kapaciteta, neophodno je razviti jedinstveni zajednički jezik za komandovanje i kontrolu u svim štabovima Izraelskih odbrambenih snaga koji deluju ili funkcionišu u sferama između ratova, što će se sprovoditi kroz uspostavljene škole komandovanja i kontrole. Razviti sposobnost korišćenja kvalitetnih bezbednosnih službi, njenih usluga (aktivnosti koje preduzimaju) na svim nivoima operacija: nacionalnoj, strateškoj i operativnoj bezbednosnoj službi (njenoj aktivnosti). Izgradnja snaga u oblasti službi bezbednosti zasniva se na sledećim akcijama: razvoj i unapređenje sposobnosti integracije informacija, razvoj sposobnosti držanja susedne teritorije na osnovu obaveštajnih podataka neophodnih za kreiranje ciljeva sa visokom preciznošću u kratkom vremenskom periodu, praćenje neprijateljskih doktrina, iskorišćavanje bezbednosnih službi (njenih aktivnosti, podataka), njihovo analiziranje i stavljanje na raspolaganje

na svim nivoima: od štaba, komande okruga, do taktičkog nivoa u bataljonima i komandama koje vrše silu, kao i potreba da se predstavi slika stanja neprijateljskih formacija i izmeri efikasnost ofanzivnih napora Izraelskih odbrambenih snaga protiv njih. Potrebno je održati očuvanje osnovne spremnosti, radi kvalitetnog odvraćanja, uz očuvanje mehanizama za ubrzanje neophodne nabavke. Izgradnja kapaciteta u ovom kontekstu biće zasnovana na sledećim aktivnostima: jačanje strateškog i taktičkog odvraćanja putem sajber ratovanja, dostupnost podataka od bezbednosnih službi kao rano upozorenje za pokretanje preventivnih aktivnosti kao i sposobnost preventivnog udara u skladu sa indikacijama ranog upozorenja kako bi se osujetio pokušaj napada na Izrael (Graham, 2016). Potrebno je još jednom naglasiti da su osnova delovanja u *CBW* delovanje i podaci dobijeni od službi bezbednost, gde se u strateškom dokumentu, prvom objavljenom javnom dokumentu u Izraelu, ističe značaj neobaveštajnih aktivnosti i bezbednosnih službi kao osnove stuba odvraćanja.

4. **Zaključak**

Teorija na Zapadu je kvalitativno pokrila većinu segmenata odvraćanja u svojim konceptualnim i instrumentalnim definicijama, ali postoji veoma malo ili minimalno mesto i uloga službi bezbednosti u odvraćanju, odnosno primeni neobaveštajnih aktivnosti u sprovođenju ciljeva spoljne politike, što je delimično razjašnjeno kroz ovo istraživanje.

Kada govorimo o kreiranju strategija na najvišem državnom nivou (što je, u poslednje vreme, možda postalo više promašaj), moramo biti svesni da informacija kao dokument, papir ili propis, ne znači ništa ako nije adekvatno propisana ili primenjena.

Ukoliko postoji propisivanje velikog broja dokumenata, na strateškom nivou, i oni se stavljaju u operativnu upotrebu, to dovodi do prekomernog broja važećih propisa, gde u složenim profesijama, jedna od njih je profesija lica koja se bave odvraćanjem (svako u svojoj oblasti rada), to dovodi do problema realne sposobnosti izvršioca da se pridržava svih propisa, da prepozna svoje obaveze i da ih primenjuje u odvraćanju. Postavlja se pitanje koordinacije i regulisanja ostalih podzakonskih akata

u ovoj oblasti, jer ideja koju je postavio državni rukovodilac mora biti operacionalizovana počev od vrha države, pa sve do najnižih izvršilaca.

Izrael je urađen po uzoru na SAD i NATO (u proteklih nekoliko godina u SAD su sprovedene najveće organizacione promene vezane za rad i koordinaciju službi bezbednosti, uspostavljanjem centara za objedinjavanje bezbednosnih i kontraobaveštajnih komponenti službi bezbednosti; 2016. godine u NATO-u, Centar za suprotstavljanje neobaveštajnim aktivnostima i poboljšana koordinacija bezbednosnih službi), pa je otišao i korak dalje gde je strategija Izraelskih odbrambenih snaga – IDF, pored preciziranja instrumenata odvraćanja u primeni neobaveštajnih aktivnosti u odvraćanju, predvidela izgradnju snaga za neobaveštajne aktivnosti, tj. kampanje između ratova – CBW, koje uključuju obaveze date na najvišem državnom nivou – ministrima, organizaciona prilagođavanja i obuku lica za planiranje, učešće i sprovođenje tajnih i prikrivenih operacija za CBW. Isticanje sajber odvraćanja uz stvaranje strukture za suprotstavljanje sajber pretnjama, direktno potčinjene Izraelskim odbrambenim snagama, naglašava koji će instrument suprotstaviti ovoj vrsti pretnji i ističe mesto i ulogu službi bezbednosti u odvraćanju tokom CBW. Pošto je reč o izuzetno dobro urađenom dokumentu IDF-a koji sadrži citate načelnika Generalštaba Oružanih snaga Izraela i bivšeg šefa Izraelske vojnoobaveštajne službe, što uz gore navedene konkretne predloge za rešavanje problema formiranjem potrebnih državnih jedinica, snaga i određivanjem učesnika u odvraćanju, uz lično učešće, najstručnijih ljudi u ovoj oblasti čini ovaj dokument možda jedinstvenim na planeti, i kao takav može poslužiti kao model iz kojeg se mogu preuzeti delovi koji bi bili prilagodljivi u drugim zemljama.

Velika količina i brzina informacija koje se nalaze u svakodnevnoj upotrebi pogoduju lakoj primeni dezinformacija i obmana prema ciljnoj grupi, što stvara pogodno tlo za donošenje pogrešnih odluka državnih lidera u korišćenju instrumenata odvraćanja. Sada se suočavamo sa novom pretnjom, a to je izuzetno kratak vremenski period za proveru informacija. Ova pojava dovodi do ozbiljnih pretnji po nacionalnu bezbednost države, jer kada znamo da imamo određene važne informacije o registrovanoj pretnji po nacionalnu bezbednost, a ništa se ne preduzima povodom toga kako bi se preduzele preventivne mere, to je isto kao, ili čak i gore, da te informacije još uvek nemamo (uzmimo za primer 11. septembar u SAD i posledice koje je imao).

Literatura

DoD 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 (DoD)*.

Golov, A. (2016). *Israeli Deterrence in the 21st Century*, (Arms Control and Strategic Stability in the Middle East and Europe. Emily B. Landau and Anat Kurz, editors. Tel-Aviv: Institute for National Security Studies, p. 83–97.

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.

Jakobsen, V. P. (2021). Deterrence in Peace Operations: Look Beyond the Battlefield and Expand the Number of Targets and Influence Mechanisms, Denmark (In: Osinga, F. & Sweijs, T. 2021. Deterrence in the 21st Century-Insights from Theory and Practice, Annual Review of Military Studies 2020, NL Arms Netherlands, T.M.C. Asser Press, Hague, Netherlands, p. 327–345).

Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs*, 92(1), University of London, p. 175–195.

Rynning, S. (2021). Deterrence Rediscovered: NATO and Russia, *Annual Review of Military Studies* 2020, NL ARMS Netherlands, T.M.C. ASSER PRESS, The Hague, The Netherlands.

Shamir, E. (2021). Deterring Violent Non-state Actors, Political Science Department, The Begin Sadat Center for Strategic Studies (BESA Center), Bar Ilan University, Ramat Gan, Israel (In: Osinga, F. & Sweijs, T. (2021). Deterrence in the 21st Century-Insights from Theory and Practice, *Annual Review of Military Studies* 2020, NL Arms Netherlands, T.M.C. Asser Press, Hague, Netherlands, p. 263–286).

Soesanto, S., & Smeets, M. (2021). Cyber Deterrence: The Past, Present, and Future, Center for Security Studies (CSS), ETH Zurich, Zurich, Switzerland (In: Osinga, F. & Sweijs, T. (2021). Deterrence in the 21st Century-Insights from Theory and Practice, *Annual Review of Military Studies* 2020, NL Arms Netherlands, T.M.C. Asser Press, Hague, Netherlands, p. 385–399).

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.

Bajagić, M. (2010). **Špijunaža** *u 21. veku-Savremeni obaveštajno-bezbednosni sistemi*, drugo dopunjeno izdanje. Beograd: MARSO.

Bajagić, M. (2013). Obaveštajna aktivnost u funkciji izgradnje sistema nacio-

nalne bezbednosti. *Politika nacionalne bezbednosti* broj 1/2013, str. 61–86.

Bajagić, M. (2015). *Metodika obaveštajnog rada*. Drugo, izmenjeno i dopunjeno izdanje, Beograd: Kriminalističko policijska akademija.

Marjanović, Z. i Mićović, M. (2022). Uticaj krizne situacije izazvane epidemijom i pandemijom (kovid 19) na korporativnu bezbednost, **Časopis** *Bezbednost*, 3/2022, LXIV, Beograd, str. 100–119.

Marjanović, Z. i Mićović, M. (2023). Geografski vektor nacionalne odbrane-Kopnena moć, **Časopis** *Politička revija*, broj 1/2023, Beograd, 183–209.

Mijalković, S. (2011). Obaveštajno-bezbednosne službe i nacionalna bezbednost. *Časopis Bezbednost*, 1/2011, Beograd, str. 74–92.

Mijalkovski, M. i Konatar, V. (2010). *Neobaveštajna rovarenja obaveštajaca u lavirintima specijalnih operacija*. Novi Sad: Prometej.

Milošević, M. (2005). *Odbrana od terorizma*. Beograd: Edicija, Nauka, Svet knjige.

Putnik, N. (2012). Kiber ratovanje-novi oblik savremenih društvenih konflikata. (*Doktorska disertacija*). Beograd: Fakultet bezbednosti.

Trbojević, M. (2017). Neobaveštajni oblik delovanja obaveštajnih službi. *Srpska politička misao* broj 4/2017., god. 24.,Vol. 58., str. 319–334.