NASTAVNO-NAUČNOM VEĆU FAKULTETA ORGANIZACIONIH NAUKA

Odlukom Nastavno-naučnog veća Fakulteta organizacionih nauka, br. 05-01 broj 3/65-11 od 13.05.2016., imenovani smo u Komisiju za ocenu završene doktorske disertacije kandidata mr Dragana Mladenovića, dipl. inž, pod naslovom:

MULTIDISCIPLINARNI ASPEKTI SAJBER RATOVANJA

i na osnovu toga podnosimo sledeći:

I Z V E Š T A J

1. Osnovni podaci o kandidatu

1.1. Biografski podaci o kandidatu

Dragan Mladenović je rođen 13.05.1972. godine u Doboju. Osnovnu školu i Vojnu gimnaziju je zavrsio u Beogradu sa odličnim uspehom. Zvanje diplomiranog inženjera mašinstva je stekao 1995. godine na Vojnotehničkoj akademiji u Beogradu. Zvanje magistra tehničkih nauka - područje organizacionih nauka za elektronsko poslovanje je stekao na Fakultetu organizacionih nauka u Beogradu 2011. godine odbranom magistarske teze *Međunarodni aspekt cyber ratovanja*. Magistarsku tezu je radio pod mentorstvom prof. dr Mirjane Drakulić. Magistarska teza je od strane Privredne komore Beograda proglašena za najbolju magistarsku tezu u 2011. godini.

U školskoj 2014/2015. godini završio je master studije na studijskom programu iz oblasti sajber bezbednosti na *National Defense Universiy/Information Resources Management College* (*iCollege*) u Vašingtonu, SAD, odbranom master rada pod nazivom „*International Legal Regulation of Cyber Conflict: Problems and a Proposed Solution*“ i 2016. godine stekao zvanje mastera nauka u oblasti sajber bezbednosti (*Master of Science Degree in Government Information Leadership, Cybersecurity Concentration*).

Od 1995. godine do danas je zaposlen u Vojsci Srbije kao profesionalni oficir. Pripadnik je Uprave za telekomunikacije i informatiku (J-6) Generalštaba Vojske Srbije, u činu potpukovnika. U toku

profesionalne karijere je obavljao veći broj dužnosti u oblasti tehničke službe i logistike u Gardi Vojske Srbije. Za ostvarene rezultate u toku službe je odlično ocenjivan. Veći broj puta u toku školovanja i profesionalne karijere je nagrađivan i pohvaljivan za izuzetne profesionalne i akademske rezultate. Odlikovan je ordenom za zasluge u oblastima odbrane i bezbednosti trećeg stepena.

Kao student poslediplomiskih studija na Fakultetu organizacionih nauka i na Nacionalnom univerzitetu odbrane, i kao samostalan istraživač, duži niz godina se intenzivno bavi istraživanjem sajber sukoba i ratovanja, informacione bezbednosti, međunarodnog prava oružanih sukoba, informacionih tehnologija i teorija bezbednosti. U toku profesionalne karijere je učestvovao na više međunarodnih i nacionalnih vojnih vežbi čiji je sadržaj bila sajber odbrana i informaciona bezbednost. U prethodnom periodu je bio predstavnik Ministarstva odbrane Republike Srbije na većem broju aktivnosti vezanim za sajber odbranu i informacionu bezbednost u organizaciji domaćih i međunarodnih organizacija, kao što su OEBS, DIPLO fondacija i Ženevski centar za demokratsku kontrolu oružanih snaga. U septembru 2015. godine je, u svojstvu eksperta za sajber odbranu, učestvovao na skupštinskom javnom slušanju u organizaciji Odbora za odbranu i unutrašnje poslove Narodne skupštine Republike Srbije sa temom „*Odbrana od vojnih pretnji u sajber prostoru*“.

Tečno govori engleski jezik, a pasivno ruski.

1.2. Spisak objavljenih radova

Kandidat mr. Mladenović od odbrane magistarskog rada do završetka doktorske disertacije ima 9 naučnih i stručnih radova u oblasti sajber sukoba, ratovanja, informacione bezbednosti i informaciono-komunikacionih tehnologija, i to:

1. **Dragan D. Mladenović**, Mirjana S. Drakulić, Danko M. Jovanović, „*Neutralnost i sajber ratovanje*”, Vojno delo, vol. 63, no. 3, jesen/2011, Beograd, str. 189 – 220 (M52).
2. **Dragan D. Mladenović**, Danko M. Jovanović, Mirjana S. Drakulić, „*Definisanje sajber ratovanja*”, Vojnotehnički glasnik, Beograd, 2012, vol. 60, br. 2, str. 84–117, DOI: 10.5937/vojtehg1202084M, (M52).
3. **Dragan D. Mladenović**, Danko M. Jovanović, Mirjana S. Drakulić, „*Tehnološki, vojni i društveni uzroci za primenu sajber ratovanja*”, Vojnotehnički glasnik, Beograd, 2012, vol. 60, no. 1, str. 70 – 98, (M52).
4. **Dragan D. Mladenović**, Mirjana S. Drakulić, Danko M. Jovanović, „*Međunarodno pravo i sajber ratovanje*“, Vojno delo, vol. 63, Beograd, proleće/2012, str. 9-39, (M52).

5. **Dragan D. Mladenović**, „*Primena principa prava oružanih sukoba na sajber ratovanje*“, Novi glasnik, Beograd, 2013, vol. 19-20, no. 1-4/2012-2013, str. 37-56 (M54).
6. **Dragan Mladenović**, Danko Jovanović, Nenad Denić, „*Open Source Solutions in the Development of Military Unmanned Aerial Systems*“, Scientific Technical Review, Belgrade, 2013, vol. 63, no. 1, pp. 36-46, (M51).
7. **Dragan D. Mladenović**, „*Procena ranjivosti i testiranje otpornosti na upade u sistem u vojnom kontekstu i u odnosu na Međunarodno humanitarno pravo*” (engl. *Vulnerability Assessment and Penetration Testing in the Military and IHL Context*), Vojnotehnički glasnik, Beograd, 2016, vol. 64, no. 4, DOI број чланка: 10.5937/vojtehg64-10761, (M52).
8. Nenad Denic, **Dragan Mladenovic**, Jovanovic Danko, „*Open Source UAV in MANET Combat Environment*”, Research paper presented at the 5th International Scientific Conference on Defensive Technologies (OTEH) in OTEH 2012 Proceedings, Belgrade, September 2012.
9 **Dragan D. Mladenovic**, Danko Jovanovic, „*Mobile Ad Hoc Networks Security*”, research paper presented at the 5th International Scientific Conference On Defensive Technologies (OTEH) in OTEH 2012 Proceedings, Belgrade, September 2012.

Knjigu od 559 strana pod nazivom „*Međunarodni aspekt sajber ratovanja*” objavio je 2013. godine u izdanju Medija centra Odbrana.

2. Osnovni podaci o doktorskoj disertaciji

Doktorska disertacija Dragana Mladenovića pod naslovom ***MULTIDISCIPLINARNI ASPEKTI SAJBER RATOVANJA*** urađena je na 354 strana, ima 13 tabela i 30 slika, uz dodatnih 36 strana bogate bibliografije, sa listom od 526 bibliografskih jedinica.

Disertacija ima i prateće sadržaje (sažetak na srpskom i engleskom jeziku sa ključnim rečima; sadržaj; spisak skraćenica; spisak ilustracija; spisak tabela; bibliografiju, biografiju i priloge).

2.1. Predmet i cilj disertacije

Predmet disertacije je utvrđivanje ontološke prirode sajber ratovanja i sukoba u sajber prostoru, kao novog i različitog oblika primene sile u u međunarodnim odnosima, i načina njihove međunarodnopravne regulacije. Uži predmet istraživanja je utvrđivanje odnosa između sukoba, ratovanja, napada, kriminala i drugih oblika agresije u sajber prostoru u međunarodnim odnosima. Multidisciplinarni pristup ovom problemu predstavlja primenu znanja, tehnika i veština iz oblasti računarskih nauka, informacione i sajber bezbednosti, vojnih, pravnih i sociooloških nauka u cilju objedinjenog pristupa predmetu istraživanju i formiranju jedinstvenog sistema znanja o fenomenu

sajber ratovanja i sajber sukoba. Posebna pažnja je posvećena ulozi, odgovornosti i suverenitetu država, kao osnovnih učesnika sukoba u ovom prostoru.

Opšti cilj istraživanja je bio utvrđivanje prirode i karakteristika sajber ratovanja i sajber bezbednosti i povezivanje saznanja iz različitih naučnih oblasti radi njihovog šireg sagledavanja.

Posebni ciljevi su sledeći:

- Ukazati na specifičnosti sajber prostora.
- Sveobuhvatno i na sistematičan način sagledati i proučiti nedostatke informacione infrastrukture i problem ugroženosti sajber prostora sa posebnim naglaskom na sajber ratovanje, kao novi, teorijski nedovoljno istražen, fenomen.
- Analizirati preduslove za pokretanje sajber ratovanja.
- Ukazati na vrste i karakteristike dejstava sajber ratovanja polazeći od njihovog definisanja i analize oblika u odnosu na vrstu, područje primene i posledice.
- Proučiti odgovornost država za sajber napade.
- Analizirati postojeću regulativu (međunarodnu, nacionalnu i samoregulaciju) u oblasti sajber ratovanja, sajber kriminala, sajber terorizma i telekomunikacija i ukazati na otvorena pitanja.
- Analizirati kako sajber ratovanje utiče na suverenitet i neutralnost država.
- Proučiti koji su modeli sajber bezbednosti i regulacije sajber ratovanja i utvrditi polazna stanovišta za izgradnju nacionalnih doktrina za sajber ratovanje država male i srednje veličine.
- Utvrditi vrstu i sadržaj najvažnijih aspekata sajber ratovanja.
- Sagledati koji su društveni aspekti sajber rata.
- Proučiti prirodu vojnog aspekta sajber ratovanja, utvrditi glavna područja i osnovne specifičnosti i ukazati na moguću nacionalnu vojnu primenu.
- Odrediti kako na sajber ratovanje reaguje pravo sa aspekta Međunarodnog prava, Prava oružanih sukoba, Međunarodnog prava ljudskih prava, Međunarodnog humanitarnog prava i drugih grana prava.
- Proučiti prirodu bezbednosnog aspekta sajber ratovanja i utvrditi odnos sajber ratovanja sa sajber kriminalom, terorizmom, špijunažom i drugim područjima sajber bezbednosti i mogućnost njihove integrisane prevencije i regulacije.
- Obezbediti sociološkoj, pravnoj, informatičkoj, vojnoj, ali i drugim relevantnim disciplinama, osnovu za buduća teorijska i praktična istraživanja.

2.2. Osnovne hipoteze istraživanja

Dragan Mladenović u doktorskoj disertaciji, kroz metodološki dobro potkrepljeno istraživanje, potvrđuje jednu opštu i sedam posebnih hipoteza.

Opšta hipoteza istraživanja je bila:

Razvoj sajber ratovanja se ne može predvideti u dužem vremenskom periodu, niti se može regulisati primenom tradicionalnih grana prava.

Posebne hipoteze su sledeće:

- Sajber ratovanje je specifičan koncept sukoba koji se po uzrocima, izvođenju i rešavanju značajno razlikuje od koncepata sukoba u fizičkom okruženju.
- Sajber ratovanje se ne može praktično i efektivno regulisati primenom Međunarodnog prava oružanih sukoba po principu analogije sa tradicionalnim ratovanjem.
- Sajber ratovanje se primarno zasniva na upravljanju znanjem i na organizaciji strukture na nacionalnom nivou, a ne na posedovanju materijalnih resursa za vođenje borbe.
- Zbog tehnološkog ograničenja u primeni sajber ratovanja bez greške napadača nije moguće pouzdano otkriti tok i proces napada, identitet napadača i utvrditi odgovornost države za sajber napad.
- Neregulisana praksa sukoba u sajber prostoru ugrožava mogućnost za njegovu mirnodopsku primenu, i narušava odbranu i bezbednost svih nacija.
- Primena sajber napada u svrhu vođenja sukoba je karakteristična podjednako u stanju mira, kao i rata. Efektivno rešenje regulisanja sukoba u sajber prostoru mora imati sposobnost primene podjednako u stanju rata kao i u stanju mira.
- Zbog složene prirode i višedimenzionalnosti sukoba u sajber prostoru fokus naučnog istraživanja održivog modela njegove regulacije mora bit pomeren sa monodisciplinarnog na multidisciplinaran i interdisciplinarni pristup.

Istraživanjem je potvrđeno da je priroda sajber ratovanja kompleksna, da se proces sajber napada pokrenut od strane država može preduzimati u stanju rata i mira, kao latentni i prikriveni sukob. Kao posledica specifične prirode sajber napada i odsustva postojanja oružja u smislu fizičkog naoružanja, sajber napadi se zasnivaju na namernom narušavanju informacione bezbednosti protivničkih sistema. Taj postupak se u velikom broju slučajeva ne može preduzimati primenom univerzalnog koncepta međunarodnih sukoba.

Daljim istraživanjem je pokazano da je primena (međunarodnog) prava oružanih sukoba u sajber okruženju vrlo ograničena i da se ne može pouzdano upotrebiti u cilju univerzalnog regulisanja sukoba, kao što je to slučaj sa oružanim sukobima u fizičkom okruženju.

Analizom poznatih modela sajber napada i utvrđivanjem prakse informacione bezbednosti utvrđen je model sajber bezbednosti zasnovan na ranjivostima u informacionim sistemima, odnosno na posedovanju podataka i informacija o ranjivostima i znanju kako da se one iskoriste. U tom pogledu potvrđena je hipoteza da se sajber ratovanje primarno zasniva na upravljanju znanjem i na uspostavljanju održive strukture za sticanje i razvoj tog znanja.

Sajber napad je definisan kao proces iskorišćavanja ranjivosti, a ne kao postupak upotrebe naoružanja. Sajber prostor je definisan kao okruženje zasnovano na umrežavanju informacionih sistema na nivou podataka. Priroda informaciono-komunikacionih tehnologija i umrežavanje informacionih sistema omogućavaju napadačima da ostvare prikriveno delovanje i anonimno preduzimaju napade u sajber prostoru. Istaknuti su različiti modeli napada s obzirom na broj i odnose napadača, ciljeva i mogućnost odlaganja efekata dejstva, Posledica toga je da nije moguće utvrditi odgovornost države za sajber napad, pa samim tim ni primeniti Međunarodno pravo oružanih sukoba.

Analizom društvenih sukoba na međunarodnom nivou, definisanjem sukoba kao prirodnog procesa ispoljavanja moći u ostvarivanju nacionalnih interesa, pokazano je da je mogućnost zloupotrebe informaciono-komunikacionih tehnologija otvorena i da zavisi od volje i odluke napadača. Time je potvrđena teza da je neregulisana praksa sukoba u sajber prostoru faktor ugrožavanja mira i bezbednosti nacija i predstavlja zloupotrebu ovih tehnologija.

Utvrđivanjem prirode sukoba u sajber prostoru zasnovanom na ranjivostima, nevezano za stanje rata ili sukoba, potvrđeno je da se sajber napadi mogu izvoditi diskontinuirano, van stanja sukoba i odloženo i da se rešenje za njihovo regulisanje mora bazirati na regulaciji sajber sukoba istovremeno u obe situacije, u miru i ratu.

Ključni faktor je nemogućnosti da se sa postojećim pravnim teorijama vezanim za sukobe u sajber prostoru ostvari praktičan i efektivan doprinos rešavanju problema. Primena analogije tradicionalnog prava na situacije stvorene korišćenjem novih tehnologija prepoznat je kao jedan od pristupa. Imajući u vidu ograničenost takvog pristupa, utvrđena je potreba za multidisciplinarnim i interdisciplinarnim pristupom u rešavanju problema kompleksne prirode kakvi su sukobi u sajber prostoru.

2.3. Kratak opis sadržaja disertacije

Disertacija je strukturirana u dvanaest poglavlja:

1. UVOD
    - 1.1. Izbor discipline
    - 1.2. Problemi

Kroz poglavlja rad je formiran na sledeći način:

U **Uvodu** je definisan širi i uži kontekst fenomena sajber ratovanja i sajber sukoba. Analiziran je predmet i cilj istraživanja. Obrađena je geneza, uzroci i ciljevi sukoba i ratovanja između širih društvenih zajednica. Analiziran je uticaj tehnologije na uzroke za izbijanje sukoba i na njihovu formu, pri čemu je posebno obrađen uticaj informaciono-komunikacionih tehnologija. Objašnjeno je poreklo potrebe međunarodne zajednice da u pozitivnom smislu reguliše i ograničava sukobe između država i nacija. Dati su uzroci i sadržaj problema koji prate nastojanje međunarodne zajednice, posebno iz aspekta prirode i izgradnje međunarodnog prava i specifične prirode sajber prostora i aktivnosti u njemu, uključujući sukob i ratovanje. Analizirana je uloga Međunarodnog prava oružanih sukoba u regulisanju međunarodnih sukoba u sajber prostoru i njegov kapacitet da te sukobe efikasno reguliše i ograničava. Navedeni su, objašnjeni i analizirani ontološki, epistemološki, taksonomski, terminološki i metodološki problemi u širem skupu pojmova, kategorija i fenomena u području sukoba i ratovanja u sajber prostoru. Izloženi su osnovni problemi vezani za fenomen sajber ratovanja, proces i metodologiju istraživanja navedenog fenomena. Posebna analiza je izvedena u pogledu uticaja informaciono-komunikacionih tehnologija na predmet istraživanja, sa osvrtom na nemogućnost dugoročnog predviđanja tehnološkog razvoja.

Kao rezultat analize ističe se potreba usmeravanja na suštinu opštih kategorija u području istraživanja, koje su od ključnog značaja za predmet istraživanja.

Izvršena je analiza i izbor ključnih naučnih disciplina i oblasti naučnog istraživanja od značaja za istraživanje predmeta istraživanja. Obrađeni su problemi različitog metodološkog pristupa izabranih naučnih disciplina iz područja društvenih, formalnih i tehničkih nauka i izvršen je izbor zajedničkih metoda i tehnika istraživanja koje su pogodne u svim izabranim područjima istraživanja. Analizirane su specifičnosti različitih disciplinarnih pristupa, posebno u području hibridnih predmeta istraživanja, poput sukoba i ratovanja u sajber prostoru koji su istovremeno predmet istraživanja računarskih, pravnih, vojnih, sociooloških i nauka iz područja bezbednosti, koje se tiču predmeta istraživanja sa kompleksnom prirodom. Na osnovu analize se došlo do zaključka o potrebi opšteg multidisciplinarnog i specifičnog interdisciplinarnog pristupa istraživanju, kao i primeni sistemskog pristupa. Postavljene su polazne hipoteze i opisani naučni metodi koji su primenjeni u istraživanju. Posebno su istaknuti očekivani rezultati i naučni doprinos disertacije. Izvršen je izbor primarnih naučnih disciplina, metoda i tehnika istraživanja. Definisana je osnovna i posebne hipoteze istraživanja.

U **drugom poglavlju** su obrađeni osnovni fenomeni predmeta istraživanja: sukobi i ratovi u fizičkom i sajber prostoru. U okviru analize koncepta sukoba obrađene su najpoznatije sociološke teorije sukoba i definisani su njihovi uzroci. Kao najpogodniji za primenu u međunarodnim odnosima u sajber prostoru izabran je pristup političkog realizma u međunarodnim odnosima. Obrađeni su ključni principi Morgentaua i Frimena u odnosu na ispoljavanje državne moći u sajber prostoru u cilju ispoljavanja nacionalnih interesa. Utvrđeno je da su uzroci sukoba na međunarodnom nivou u sajber prostoru društveno-političke prirode, da se tiču nacionalnih interesa, izvora i načina ispoljavanja nacionalne moći, i da su širi od primene informaciono-komunikacionih tehnologija, koje im određuju formu, sadržaj i metode manifestacije. Analizirana je teorija Naja o „pametnoj moći“ u kontekstu primene nacionalnih sposobnosti u sajber prostoru za ispoljavanje moći primenom kombinovanih aktivnosti prisile i privlačenja, kroz aktivnosti „tvrde moći“, odnosno preduzimanje napada u sajber prostoru i mera ekonomske prisile; primenu „meke moći“ kroz ispoljavanje informacionih aktivnosti i kulturne dominacije u odnosu prema drugim nacijama; i njihovu kombinaciju u primeni koncepta „pametne moći“. Istaknuti su rezultati analize sukoba i ratovanja u sajber prostoru po kojima se zaključuje da postoji neophodna potreba da se ti sukobi regulišu na međunarodnom nivou, kao dugoročna potreba međunarodne zajednice i pojedinačnih nacija.

Obrađena je razlika između fenomena sukoba i rata, analizom stavova Klauzevica, Sun Cua, rezultata istraživanja forme, vrste i frekvencije oružanih ratnih sukoba Kendea, i primenjeni su rezultati analize na kontekst savremenih sukoba u sajber prostoru koje karakteriše primena

informaciono-komunikacionih tehnologija kao osnovnih sredstava sukoba i faktora koji omogućavaju njihovo okruženje.
Dat je pregled relevantnih i karakterističnih definicija osnovnih pojmova od značaja za istraživanje sukoba i ratovanja u sajber prostoru: borba, boj, bitka, oružana borba, rat, sukob i suživot i izvršena je analiza njihovih karakteristika. Napravljena je razlika između rata i sukoba u smislu njihove savremene primene u sajber prostoru.

Treće poglavlje je posvećeno fenomenu sajber prostora, njegovog sadržaja, elemenata i kontekstualnih nivoa njegove manifestacije - slojeva. U poglavlju je obrađena geneza nastanka sajber prostora, analizirani su uzroci nastanka i izgradnje i prikazana evolucija njegovog poimanja i primene. Poseban značaj u analizi je dat primeni sajber prostora od strane država u svrhu ispoljavanja državne moći i ostvarenja nacionalnih interesa. Na osnovu analize ključnih momenata u razvoju Interneta u SAD došlo se do zaključka da je sajber prostor, kao koncept informacionog tehnološkog okruženja, nastao kao manifestacija nacionalnog i državnog interesa SAD, pre svega u svrhu odbrane. Analizirano je savremeno značenje pojma „sajber“ u lingvističkom (morfološkom i etimološkom pogledu), kao i njegovo savremeno ontološko značenje. Za potrebe istraživanja ratovanja i sukoba u sajber prostoru, izvršeno je definisanje pojma „sajber prostor“. U tu svrhu je izvršen izbor relevantnih izvora na nacionalnom, akademskom i stručno-profesionalnom nivou i dat je pregled 21 definicije sajber prostora datih od strane najvažnijih relevantnih izvora u međunarodnim okvirima. Izbor izvora tih definicija je izvršen na osnovu analize sedam najuticajnijih studija i izveštaja o dostignutom stanju sajber bezbednosti i razvoja u području primene informaciono-komunikacionih tehnologija u područjima industrijske primene, nacionalne bezbednosti, konkurentnosti poslovanja i odbrane. Izvršen je izbor 20 vodećih država u pogledu dostignutog nivoa razvoja sajber bezbednosti i odbrane, kao i vodećih međunarodnih standarda u oblasti informacione bezbednosti, izveštaja i studija stručnih organizacija. Za potrebe istraživanja fenomena sajber ratovanja i sajber sukoba, na osnovu analize definicija datih od strane izabranih autora i u okviru dokumenata, izvršeno je utvrđivanje i analiza pojedinačnih karakteristika sajber prostora, kao i sinteza njegovih najvažnijih zajedničkih, opštih i posebnih, karakteristika. Konačno, izvršeno je sopstveno definisanje samog pojma sajber prostora od strane kandidata.
Za uvid u način manifestovanja upotrebe sajber prostora u sukobima, pružen je i objašnjen model sajber prostora koji se sastoji od tri nivoa/sloja: fizičkog, logičkog i kognitivnog. Izvršena je njihova deskripcija i analiza načina funkcionalne povezanosti. Analiziran je model Raušera po kome su elementi od značaja za sajber prostor široki i sveobuhvatni, i uključuju sve načine uticaja na funkcionisanje i upotrebu informaciono-komunikacionih tehnologija, počevši od ljudi i propisa zaključno sa fizičkom infrastrukturom i geografskim okruženjem u kome se prostire. Zaključuje se da je sajber prostor sveobuhvatan i da uključuje sve oblike primene informaciono-komunikacionih

tehnologija, i da se u tom kontekstu treba posmatrati mogućnost narušavanja bezbednosti u cilju preduzimanja napada u njemu, kao elementa međunarodnih sukoba. Ističe se logički sloj sajber prostora kao ključni i objašnjava način njegove interakcije sa ostala dva. Kao osnovni gradivni element sajber prostora se navode podaci, koji mogu imati logičku vrednosti, kognitivnu vrednost kao informacije i fizičku vrednost kao signali koji su nosioci podataka.

Četvrto poglavlje se odnosi na sukobe u sajber prostoru. Analizom teorijske misli i prakse razvoja nacionalnog sistema odbrane SAD, slikovito se ističe potreba i praksa razvoja svesti i sistemske teorije u području bezbednosti i odbrane. Objašnjava se komplementarnost tog razvoja sa raznim modelima, naročito Šelingovim modelom „strategije sukoba“, Vordenovim modelom „Centra gravitacije“, modelom „mrežnocentričnog ratovanja“ Ovensa i Cebrovskog. Nacionalni sistem bezbednosti i odbrane se predstavlja kao „sistem sistema“ sa rastućom kompleksnošću. Zaključuje se da je za uspešno razumevanje i razvoj adekvatnog modela odbrane u sajber prostoru neophodno primeniti sistemski pristup naučnog istraživanja u oblasti prirodnih, logičkih i društvenih nauka, a kao metod se, u skladu sa pogodnošću u svakom konkretnom slučaju, može izabrati multidisciplinaran i interdisciplinaran pristup. U tom kontekstu se analizira potreba izgradnje koncepta objedinjenog multidimenzionalnog „borbenog prostora“ umesto jednodimenzionalnog koncepta „bojišta“.

Proučava se najveće postojeće vojno multidimenzionalno „združeno informaciono okruženje“ Ministarstva odbrane SAD i vrši se njegova analiza kao sistema. Isti pristup se, po analogiji, primenjuje i u analizi sistema nacionalne bezbednosti SAD zasnovanom na prikupljanju i obradi elektronskih podataka lične komunikacije pojedinaca ove zemlje i svetu. Objašnjava se sposobnost nacionalnog sistema bezbednosti SAD i država članica saveza „Pet očiju“ da skupljaju, obrađuju i koriste lične podatke građana. Na njihovom bezbednosnom modelu zasnovanom na sajber prostoru objašnjava se pristup „prikupi sve“ umesto odvojenog praćenja individualnog cilja i ističu se problemi pravnog regulisanja ovakve prakse primenom tradicionalnih nacionalnih i međunarodnih akata.

U **petom poglavlju** se identifikuju osnovne kategorije učesnika sukoba i ratovanja u sajber prostoru. Kao centralni akter sukoba su prepoznate države, a ostali su naddržavni savezi, organizacije i pojedinci. Izvršena je analiza organizacije naddržavnog nivoa u izgradnji i primeni sposobnosti za sajber obranu. Na osnovu izvršene studije slučaja i analize kapaciteta i sposobnosti za sajber odbranu pojedinačnih zajednica (Evropske Unije, NATO saveza i zajednice „Pet očiju“) dolazi se do zaključka da na razvoj sposobnosti za sajber odbranu veći uticaj ima nacionalna moć i komplementarnost nacionalnih interesa od formalnog integrativnog procesa, bez obzira na značaj organizacije. Kao važniji faktor uspostavljanja sposobnosti za sajber odbranu prepoznaje se isto

poreklo i bliskost nacionalne kulture, više nego isti političko-ideološki ciljevi ili formalna pripadnost vojno-političkom savezu. Centralni faktor od značaja za izgradnju sposobnosti sajber odbrane je upravljanje relevantnim znanjem iz oblasti informacione bezbednosti, koje se uspostavlja na individualnom, grupnom i nacionalnom nivou. Najviši entitet objedinjenog planiranog upravljanja znanjem prepoznata je država.

Nacionalni nivo u razvoju i ispoljavanju sposobnosti odbrane i bezbednosti u sajber prostoru se analizira u sklopu teorije racionalnog izbora političkog realizma Morgentaua, teorije rata Klauzevica, i tehnološki zasnovanih sukoba van Krevelda. Takođe, razmatra se i u okviru međunarodnopravnih odnosa na osnovu zaključaka studije Goldsmita i Posnera koja primenjuje teoriju racionalnog izbora u međunarodnopravnim odnosima država zasnovanim na nacionalnim interesima.

Za razliku od političkih interesa koji pokreću učesnike sukoba na državnom i naddržavnom nivou, subnacionalni nivo poslovnih organizacija kao učesnika sukoba u sajber prostoru se analizira u kontekstu ekonomskih interesa. Pravi se razlika između zakonitih i nezakonitih organizacija i proučava sticanje finansijske dobiti na legalnom i "crnom" tržištu informacija o ranjivosti informacionih sistema i eksploita za iskorišćavanje u napadima. Identifikuju se terorističke organizacije i veza sa državnim nivoom, posebno u području antiterorističkih aktivnosti.

Šesto poglavlje se bavi fenomenom sajber ratovanja i definiše u najopštijem smislu kao "ratovanje u sajber prostoru". Pojam ovog ratovanja se shvata u širem i užem smislu. Analizira se odnos specifičnih faktora koji na njega utiču i kako se to odražava na međunarodnopravno regulisanje, pre svega zbog relativno velike brzine razvoja informaciono-komunikacionih tehnologija u odnosu na brzinu ekonomskih, političkih i društvenih promena. To se prepoznaje kao faktor tehnološki indukovanih promena i nastanka novih koncepata i modela vođenja sukoba. Predstavljen je model sajber prostora kao faktor ratovanja i koncepata sukoba koji se zasnivaju na brzini.

Posebno se analizira i ističe koncept ratovanja "četvrte generacije" u okviru koga istaknuto mesto zauzima sajber ratovanje. Navodi se retrospektiva i uporedna analiza različitih generacija ratovanja, u okviru koje se koncept sajber ratovanja izvodi istovremeno u više ravni.

Obrađuju se rezultati relevantnih studija i istraživačkih baza podataka o sukobima u svetu, pri čemu se sajber ratovanje razmatra u odnosu na njihove nalaze, pri analizi uzroka njegovog nastanka i modela primene. U okviru provere hipoteze da je dovoljan uslov za izgradnju kapaciteta i primenu sajber ratovanja razvoj sposobnosti za upravljanje znanjem u specifičnom području informacione i sajber bezbednosti i u pravilnoj organizaciji resursa, a da je postojanje uzroka sukoba u konkurenciji nacionalnih interesa samo potreban, ali ne i nužno neophodan uslov, izvodi se studija slučaja država Podsaharske Afrike i Jugoistočne Azije kao regiona u kojima se desio najveći broj

sukoba u svetu i u kojima postoji snažan trend razvoja i primene informaciono-komunikacionih tehnologija, ali i istovremeno odsustvo znanja i kapaciteta za tehnološko istraživanje.

Rasvetljavanje fenomena sajber napada je predmet **sedmog poglavlja**. Utvrđuju se ključni elementi oružanih sukoba i vrši se njihova analiza na primeru sajber ratovanja u kontekstu Međunarodnog prava oružanih sukoba. Uvodi se pojam ranjivosti informacionih sistema, kao ključne kategorije koja omogućava izvođenje napada u sajber prostoru. Sajber napadi se dovode u direktnu vezu sa informacionom bezbednošću. Razmatra se sadržaj i pojam sajber napada.
U ovom poglavlju se analiziraju postojeće definicije sajber napada u vojnom, tehnološkom i bezbednosno-političkom smislu. Kao rezultat analize se ističe zaključak da pojam sajber napada nema isto značenje. Tehnološki orijentisana definicija sajber prostora se uzima kao referentna, s obzirom da pruža najveći potencijal za suštinsko razumevanje koncepta sajber ratovanja. Vrši se komparativna analiza pristupa NATO, država Šangajske organizacije za saradnju i Ministarstva odbrane SAD. Upoređuju se koncepti sajber sukoba, sajber ratovanja i informacione bezbednosti u različitim političko-bezbednosnim konceptima, i u odnosu na međunarodno pravo. Vrši se izbor kriterijuma za određivanje prirode sajber napada, pri čemu se odbacuje princip kvalifikacije na osnovu objekata napada, a prihvata se princip na osnovu sredstva i okruženja u kome je napad izveden, kao tehnološki i pravno relevantan. Razmatra se značaj koncepta ranjivosti u pogledu informacione bezbednosti, koji se kvalifikuje kao najznačajniji faktor za preduzimanje napada i primenu sajber ratovanja. Kao rezultat analize utvrđuje se konceptualna nemogućnost međunarodnog prava da ima praktičnu primenu u regulisanju postupka iskorišćenja ranjivosti u informacionim sistemima i definiše se pojam sajber oružja kao sredstva upada. U tehničko-tehnološkom pogledu izjednačava se postupak različitih kategorija napadača (kriminalaca, haktivista, terorista, špijuna, boraca) za iskorišćavanje ranjivosti. To se kvalifikuje kao osnovna nemogućnost za efikasnu primenu tradicionalnog Međunarodnog prava oružanih sukoba na sajber ratovanje. Sajber napadi se manifestuju kao procesi iskorišćavanja ranjivosti sistema, a ne kao tehnika upotrebe oružja u sajber prostoru. Izvodi se analiza dva referentna modela sajber napada i to model kompanije Lokid-Martin i PrEP model. Vrši se komparativna analiza i analogija postupaka ovih modela sa napadima u fizičkom okruženju. Dovodi se u vezu koncept „ljudi, procesi i tehnologije“ koji se primenjuje u upravljanja informacionom bezbednošću sa tri nivoa sajber prostora u cilju opisivanja prirode sajber napada.

U **osmom poglavlju** se analizira koncept sajber oružja. Vrši se komparativna analiza više referentnih definicija sajber oružja i procena karaktera savremenih sukoba na shvatanje ovog pojma. Navode se osnovni izvori ranjivosti i ističe se značaj ranjivosti softvera kao ključnog izvora sajber napada. Proverava se standard ISO/IEC 9126 i ISO/IEC 25010 i izvodi zaključak da je u najvećem

broju slučajeva bezbednost softvera mera kontrole pristupa podacima od značaja za izvršenje njegove funkcije.

Softverski nedostaci i ranjivosti se ocenjuju kao ključni faktor koji omogućava sajber ratovanje i ističe se da ih je na sadašnjem nivou razvoja nemoguće u potpunosti izbeći, kao i napade koji su zasnovani na njihovom iskorišćavanju. Predviđa se izmena prirode sajber ratovanja u budućnosti kada se očekuje značajno smanjivanje broja ranjivosti u softveru kao posledica primene veštačkih inteligentnih sistema. Obrađuju se brojni primeri katastrofalnih posledica postojanja grešaka u informacionim sistemima i kao verovatnom se prihvata mogućnost izbijanja širokih posledica dejstvom sajber napada na informacionu bezbednost napadnutog sistema. Kao primer softverskih grešaka navodi se analiza softverskih sistema upotrebljenih na američkom vojnom avionu F-35 i vrši predviđanje o lakoći preduzimanja napada na sisteme koju neprekidno evoluiranju i nužno sadrže nedostatke informacione bezbednosti.

Deveto poglavlje je posvećeno konceptu sajber bezbednosti i utvrđivanju odnosa i razlika između koncepata "informaciona bezbednost" i "sajber bezbednost" baziranim na specifičnostima sajber napada. Navode se relevantne definicije i vrši se njihova analiza. Utvrđuje se funkcionalna veza između ova dva koncepta. Sajber bezbednost se opisuje kao informaciona bezbednost u sajber prostoru i definišu se razlike, zajedničke karakteristike i sadržaji od značaja za sukobe u ovom prostoru. Definišu se ključni faktori uspostavljanja, upravljanja i napadnja na sajber bezbednosti.

U **desetom poglavlju** se, kao studija slučaja, prezentira koncept sajber prostora radi nacionalne odbrane i sajber bezbednosti SAD-a. Navodi se istorijski razvoj shvatanja ovog koncepta i vrši se komparativna analiza pojmova, koncepata i pristupa, posebno Ministarstva odbrane. Poseban deo se odnosi na analizu preklapanja nadležnosti i aktivnosti državnih organa na poslovima bezbednosti i odbrane u sajber prostoru, posebno u odnosu na prava američkih građana. Zaključuje se da postoji jasan trend preklapanja (sukoba) nadležnosti, interesa, aktivnosti i potrebe izvršavanja sličnih i istorodnih aktivnosti u okviru nacionalne bezbednosti i odbrane, posebno u pogledu ustavnih nadležnosti i nacionalnog prava. Ističe se trend "privatizacije" sajber ratovanja i razvoja obaveštajnih sajber operacija koji je prepoznat kao širi globalni model.

U **jedanaestom poglavlju** je izvedena analiza relevantnog prava koje je moguće primeniti na sukobe, ratovanje i napade u sajber prostoru. Posebno se razmatra primena Međunarodnog prava oružanih sukoba na ove specifične sukobe. Kao osnovni problemi koji onemogućavaju praktičnu primenu ovog prava na sajber ratovanje ističu se nemogućnost utvrđivanja događanja napada; identifikacije i atribucije napadača; sukob nadležnosti suvereniteta država u sajber prostoru i nadležnosti nacionalnih organa u poslovima bezbednosti i odbrane na nacionalnim nivoima, odnosno utvrđivanje i dokazivanje državne odgovornosti za sajber napade. Proučava se realnost i

prihvatljivost da se dilema rešava uspostavljanjem novog područja u okviru Sajber prava ili pronalaženjem novih modela primene tradicionalnih pravnih postulata Međunarodnog prava oružanih sukoba.

Razlog za formiranje takvog stava je nedosledna primena osnovnih pojmova od značaja za Međunarodno pravo oružanih sukoba, poput „sajber agresije“, „sajber napada“ i „primena sile u sajber prostoru“. Vrši se analiza odnosa značenja pojmova „primena sile“, „primena oružane sile“ „agresija“ navedenih u Povelji UN i u smislu izvedenom iz dokumenata Međunarodnog prava oružanih sukoba u odnosu na kontekst vođenja neoružanih sukoba i ratovanja u sajber prostoru. Analizaju se definicije agresije iz Rezolucije Generalne skupštine UN (broj 3314/74) vezane za operacije i dejstava država u sajber prostoru. Kao jedino moguća praksa primene tradicionalnog Međunarodnog prava oružanih sukoba na situacije i aktivnosti država u sajber prostoru prepoznaje se test efektivne kontrole koji je 1986. godine primenjen od strane Međunarodnog suda pravde u slučaju Nikaragva protiv SAD, kao i Šmitov test obima i posledica sajber napada. To je poslužilo međunarodnoj grupi stručnjaka pri izradi Talinskog priručnika o primeni međunarodnog prava na sajber ratovanje. Analizirana je i procenjena primena testa u realnim situacijama u sajber prostoru, kao i stav Vlade SAD (Kohovo mišljenje) o legalnosti primene sajber napada izjednačavanju značenja „primena sile“ i „oružanog napada“, ali u specifičnom okruženju, kakav je, sajber prostor. Na osnovu rezultata izveo se zaključak o teoretskoj mogućnosti ovakvog pristupa u regulisanju sajber sukoba i ratovanja, uz konstataciju da je ovakav pristup teško primenljiv u praksi.

Poseban problem je utvrđivanje namere napadača. Model sajber napada „Cyber kill chain“ kompanije Lokid Martin i utvrđene karakteristike napada, baziraju se na dokazivanju namere napadača da izvede sajber napad na protivnički sistem. To je moguće dokazati samo na osnovu identifikacije i atribucije napadača. Ključni atributi metrike dejstva napadačkih aktivnosti u sajber prostoru (ozbiljnost, neposrednost, direktnost, invazivnost, merljivost, pretpostavljeni legitimitet i odgovornost države i vojni karakter napada) su u proceni legalnosti sajber napada.

Definiše se model moguće strukture odnosa između napadača i ciljeva u sajber prostoru i u odnosu na njega se analizira primena osnovnih principa Međunarodnog prava oružanih sukoba: razlikovanje osoba i objekata u sajber napadima i proporcionalnosti napada.

Utvrđuju se mogućnosti detekcije napada, identifikacije i atribucije napadača i odgovornosti.

Analiza modela Goldsmita i Posnera sa četiri moguća stanja odnosa između država u ispoljavanju nacionalnih interesa dovodi do zaključka o potrebi neposrednog sporazumevanja između država u cilju regulisanja sukoba u sajber prostoru. I to ne samo u vreme mira već i radi prevencije izbijanja ratnih sukoba kao njihove posledice. Kreira se model promenljivosti nadležnih pravnih sistema u odnosu na karakter sukoba, njegove posledice, učesnike i formalni status sukoba između subjekata međunarodnog prava.

Analizira se primenljivost izvora međunarodnog prava u slučaju sukoba i ratovanja u sajber prostoru poput propisa Međunarodne telekomunikacione unije. Utvrđuje se da li je moguća legalnosti sajber napada i navode se ključni elementi te procene. Na osnovu izvršene analize, izvodi se zaključak o potrebi unapređenja praktičnosti i efikasnosti međunarodnog prava na regulisanje sukoba u sajber prostoru. U tom pogledu se posebno analiziraju koncepti primene prava u slučaju deklarisanog i *de facto* sukoba napadača i napadnutih. Obrađuje se problem neprecizne formulacije fenomena od značaja za razmatranje sajber ratovanja i sukoba.

U **dvanaestom poglavlju** se prezentiraju zaključci o prirodi, karakteru i načinu izvođenja sukoba i ratovanja u sajber prostoru. Zaključuje se da je sajber ratovanje kompleksan proces koji se zasniva na logičko-matematičkim operacijama manipulacije podacima u elektromagnetnom spektru, čiji se efekti manifestuju na svim nivoima sajber prostora: logičkom, fizičkom i kognitivnom. Sajber ratovanje nije trend prolaznog karaktera, već fenomen i oblik sukoba koji će nastaviti da se primenjuje i razvija u budućnosti.

U vojnom pogledu, vođenje sukoba u sajber prostoru ima specifičnu formu, s obzirom da se ne može odvojiti od stanja mira i da je, u skladu sa utvrđenom prirodom procesa sajber napada, pogodnije za primenu u toku mira. Zbog toga je primenljivost Međunarodnog prava oružanih sukoba za regulisanje sajber sukoba i ratovanja ograničena. Sajber ratovanje se konceptualno predstavlja kao izvođenje skupa operacija u sajber prostoru, odnosno sajber napada, koji se mogu posmatrati u vojnom, krivično-pravnom i društveno-političkom smislu, te se regulišu različitim pravnim rešenjima.

Zbog tehničko-tehnoloških ograničenja otežana je praktična primena Međunarodnog prava oružanih sukoba na sajber ratovanje, prvenstveno zbog nemogućnosti detekcije svih sajber napada, identifikacije i atribucije napadača i utvrđivanja odgovornosti država za napade. Sajber ratovanje se ne mora izvoditi u kontinuitetu kao oružani sukobi u fizičkom okruženju, ne koristi se tradicionalno naoružanje koje je svojstveno vojnim organizacijama i efekti mu mogu biti vremenski odloženi. Zbog toga ono predstavlja novu formu sukoba, koji se odvijaju u toku ratnog sukoba, ali još češće, u toku mirnodopskih odnosa. Uzroci za primenu doktrine sajber ratovanja su ispoljavanje nacionalnih interesa država, primena informaciono-komunikacionih tehnologija u sajber prostoru i postojanje ranjivosti u informacionim sistemima koji su podložni namernom narušavanju informacione bezbednosti od strane napadača. Nacionalna prava moraju na to reagovati odgovarajućim normama usklađenim sa međunarodnim.

Zaključuje se da je za razvoj i primenu sajber ratovanja neophodno uspostaviti sistem upravljanja specifičnim znanjem iz oblasti računarskih nauka, informaciono-komunikacionih tehnologija i informacione bezbednosti, kao i obezbediti odgovarajuću organizaciju u cilju dostizanja i primene

tog znanja. Shodno utvrđenom karakteru sajber sukoba koji se odvijaju tokom stanja rata i mira, neophodno je primeniti rešenje koje podiže kapacitete za ograničavanje broja i posledica napada. Optimalan način uspostavljanja regulacije sajber ratovanja i sukoba je izgradnja i usvajanje postulata Sajber prava, a imajući u vidu specifičnost postupka izgradnje pravnih okvira i trajanje tog postupka, kao jedini praktičan način za ostvarenje ciljeva postizanja mira u sajber prostoru predlaže se zaključivanje bilateralnih i multilateralnih međudržavnih sporazuma čiji je predmet regulisanje međusobnih aktivnosti država, međusobne kontrole stanja, aktivnosti i posledica sajber napada.

U posebnom delu **Literatura** su navedeni izvori literature (bibliografija), kao direktni izvori korišćeni u toku spovođenja istraživanja.

3. Ostvareni rezultati i naučni doprinos disertacije

U doktroskoj disteraciji *MULTIDICIPLINARNI ASPEKTI SAJBER RATOVANJA* mr Dragana Mladenovića ostvareni su sledeći rezultati i naučni doprinosi:

- Dat je novi multidisciplinarni pristup sajber prostoru, sukobima, ratovanju, napadima, kao i oružju i učesnicima, čime se prevazišao dosadašnji partikularni, koji je doveo rasvetljavanju ovih fenomena samo sa stanovišta određene nauke, odnosno naučne discipline i onemogućavao odgovarajuće definisanje, klasifikovanje i tumačenje.
- Data je nova definicija sajber prostora izvedena na osnovu komparativne analize i sinteze većeg broja stavova autora, dokumenata nacionalnih organa dvadeset vodećih država i više releventnih međunarodnih organizacija uz određenje značenja termina sajber i porekla pojma ovog prostora.
- Definisani su slojevi sajber prostora i determinisane veze između fizičkog, logičkog i kognitivnog nivoa.
- Utvrđena je dinamična i promenljiva priroda sukoba, ratovanja i napada u sajber prostoru i predložena su rešenja i modeli koji su pogodni za primenu u dužem periodu bez obzira na budući razvoj tehnologije.
- Kao rezultat multidisciplinarnosti istraživanja došlo je do novog definisanja sajber ratovanja i formiranja sistematizovnih znanja o njegovoj prirodi i načinu rešavanja.
- Definisani su kriterijumi za određivanje prirode sajber napada polazeći od sredstva, funkcije ili namere i područja vođenja sukoba.
- Kreiran je i razrađen model sajber napada zasnovan na ranjivostima. Utvrđena je priroda sajber napada kao procesa iskorišćavanja ranjivosti, a ne kao postupak upotrebe naoružanja u svrhu vođenja sukoba.

- Objašnjena je geneza sistemske organizacije za potrebe mrežnocentičnog ratovanja i utvrđena uzročno-posledična povezanost sa primenom informaciono-komunikacionih tehnologija.
- Potvrđeno da je razvoj sposobnosti za sajber odbranu i ratovanje na nacionalnim nivou isključivo zasnovan na upravljanju znanjem iz oblasti računarskih nauka, informaciono-komunikacionih tehnologija i informacione bezbednosti, te da nije dovoljan tradicionalni pristup uspostavljanja organizacionih celina i tehničkog opremanja sistema.
- Prikazan je novi pristup pravu. Proces sajber napada primarno je zasnovan na primeni tehnologije i postojanju ranjivosti u sistemima, a ne na političkoj volji za manifestaciju agresije prema protivniku. Oni se dešavaju nezavisno od stanja rata ili mira. To je dovelo do prihvatanja koncepta da se sukobi i ratovanje u sajber prostoru mogu regulisati isključivo primenom sistemskog pristupa koji obuhvata Međunarodno pravo oružanih sukoba, međunarodno javno i ugovorno pravo u procesu zaključivanja neposrednih međunarodnih bilateralnih i multilateralnih sporazuma. Kako rešenja koja nudi ovaj koncept imaju sve više manjkavosti i teškoća to se u pravnim naukama počinje razvijati novi koncept – uključivanje u Sajber pravo, kao novu granu prava, koja bi obuhvatila i (međunarodne) aspekte sukoba, rata i napada u sajber prostoru, uz preuzimanje određenih, prihvatljivih koncepata Međunarodnog prava oružanih sukoba, ali i drugih grana prava. Novi koncept bi bio, u slučaju integracije i inkorporacije ovih fenomena u Sajber pravo, povoljnije i efikasnije rešenje jer se ne bi remetili postojeći koncepti tradicionalnog prava, s jedne strane, i na odgovarajući, konzistentan, način formirao novi kompleksni, multidisciplinarni i interdisciplinarni pravni pristup koji respektuje sve specifičnosti sajber prostora, s druge strane. Na taj način, forma i sadržaj prava se prilagođavaju realnim problemima i fenomenima u sajber prostoru koje to pravo reguliše, pri čemu se izbegava potreba da se sporo promenljivo tradicionalno pravo formalno prilagođava novim pojavama u realnom svetu. Ipak, je danas je preuranjeno primeniti ovo rešenje dok se ne razviju principi, koncepti, teorijske osnove nove grane prava.

Originalni pristup i višegodišnje istraživanje, bili su osnova da kandidat istakne da će rešenja dobijena primenom koncepta i modela tretiranja i rešavanja sajber sukoba, ratovanja i napada, doprineti daljem razvoju informacionog društva i izgradnji standrada sajber bezbednosti i odbrane što se ogleda kao stručni doprinos doktorske disertacije.

S obzirom na očekivanu i poželjnu mogućnost primene razvijenog koncepta bezbednosti i odbrane u sajber prostoru, sa ciljem njihovog povećanja na globalnom, nacionalnom i organizacionom, odnosno individualnom nivou, postignut je društveni doprinos doktorske disertacije.

Novi pristup pravu i regulaciji sajber prostora, sukoba, ratovanja, napada, oružja i učesnika kroz novu granu prava, Sajber pravo, je pored društvenog, strateškog i konceptualni doprinos.

4. Zaključak

Tema koja je obrađena u doktorskoj disrtaciji kandidata Dragana Mladenovića je aktuelna, provokativna i relevantna. Disertacija predstavlja novu oblast računarskih nauka, prava, sociologije, sa elementima ontologije bezbednosti i odbrane. Na osnovu obrazloženja analizirane doktorske disertacije, Komisija zaključuje da je disertacija urađena prema odobrenoj prijavi, da predstavlja originalno i samostalno naučno delo, da je njenim sadržajem ostvaren očekivani naučni doprinos, da je sistematično izrađena, da je pokazana sposobnost kandidata za samostalni naučno-istraživački rad, da je suvereno korišćena literatura i da su se stekli uslovi za njenu javnu odbranu. Komisija pozitivno ocenjuje završenu doktorsku disertaciju i sa zadovoljstvom predlaže Nastavno-naučnom veću Fakulteta organizacionih nauka da se mr Draganu Mladenoviću, dipl. inž., odobri javna odbrana doktorske disertacije pod naslovom: „MULTIDISCIPLINARNI ASPEKTI SAJBER RATOVANJA“.

U Beogradu, 26. 05. 2016.

KOMISIJA

1. dr Mirjana Drakulić, redovni profesor Univerziteta u Beogradu - Fakultet organizacionih nauka
2. dr Dejan Simić, redovni profesor Univerziteta u Beogradu - Fakultet organizacionih nauka
3. dr Slobodan Miladinović, redovni profesor Univerziteta u Beogradu - Fakultet organizacionih nauka
4. dr Branko Kovačević, redovni profesor univerziteta u Beogradu - Elektrotehnički fakultet (spoljni član)
5. dr Danko Jovanović, vanredni profesor Univerzitet odbrane - Vojna akademija (spoljni član)