UNIVERZITET U SARAJEVU
FAKULTET POLITIĆKIH NAUKA
ODSJEK: SIGURNOSNE I MIROVNE STUDIJE

DEMOKRATSKI NADZOR I KONTROLA NAD CYBER RATOVANJEM

-MASTER RAD -

Kandidatkinja: Istrefi Arnela **Mentor: Doc. dr. Vajzović Emir**

Broj indexa: 702

Sarajevo, april 2021.

UNIVERZITET U SARAJEVU
FAKULTET POLITIĆKIH NAUKA
ODSJEK: SIGURNOSNE I MIROVNE STUDIJE

DEMOKRATSKI NADZOR I KONTROLA NAD CYBER RATOVANJEM

-MASTER RAD -

Kandidatkinja: Istrefi Arnela **Mentor: Doc. dr. Vajzović Emir**

Broj indexa: 702

Sarajevo, april 2021.

SADRŽAJ

UVOD

Od samih početaka ljudskog bivstvovanja, od formiranja država, i društvenih zajednica ljudi su bili skloni ratovanju. Sama modernizacija dovela je do evolucije u načinima ratovanja. Ratno bojište ne označava više bukvalno prostor na kojem su skoncentrisane sukobljene strane, gdje one ratuju na tradicionalan način. Način ratovanja je uvijek bio zavistan, i određuje ga ljudski razvoj. Činjenica je da države svake godine sve više ulažu u „moderne“ medije, odnosno internet i internetske mreže, javnog ili polujavnog tipa, te informacije i razni sistemi (recimo napajanja strujom, naftom i slično), sada su transparetni i dostupni svima. To je velika prijetnja za državu, i njenu nacionalnu sigurnost, jer transparentnost takvih podataka čine idealnu situaciju, da ona biva napadnuta unutar cyber prostora. Sun Zi smatrao je, da su najbolji rat i najbolja pobjeda, bez borbe, što se može izvesti kao jedan od pojedinosti, ali i značaja za cyber ratovanje.

Države napadaju i ratuju, ali bez fizičke prisutnosti ratovanja, izbjegavajući prevelike ratne troškove koje bi morala da obezbijedi za vojsku. Kako bismo utvrdili šta je cyber ratovanje povest ćemo se logikom Nacionalne strategije SAD-a za osiguranje cyber prostora, koja kaže da je taj prostor od vitalnog značaja, živčani sistem državne infrastrukture, meta koja, ukoliko je ispravno napadnuta može da paralizira ostatak tijela. To je prostor na kojem vojske vrlo lahko mogu manipulirati i kao i u tradicionalnom ratu težiti ka svom cilju. Ukoliko probiju odbrambeni mehanizam države, i dopru do vitalnih informacija kojima mogu da upravljaju transferima novca, nafte, povjerljivih informacija. Ova dimenzija rata možda i predstavlja najosjetljiviju dimenziju, jer ukoliko se naruši baza podataka, te se objavi ovakvu vrstu rata, ne mogu se poslati vojnici i flote da se odbrane, jer se faktički i ne zna ko stoji iza napada. Spomenuto je da ljudi najčešće uzimaju ono dobro od interneta, te samim tim što više informacija implmentiraju na internet o sebi ili slično, to ih više izlaže opasnosti. Ista je stvar i sa državama. Postoje i drugi izazovi sa kojima se države susreću, veliki problem baš kao i u tradicionalnom ratovanju su privatne vojne agencije, u cyber prostoru to su privatne cyber kompanije. Postoji niz razloga zašto se angažuju. Jedan od razloga je što te kompanije imaju iskustvo, te samim tim organ koji ih angažuje ne mora da plaća kvalifikaciju svojih radnika za cyber radnje. Pored toga, što vlada ili drugi organ, štedi vrijeme i novac, oni na ovaj način mogu da izbjegu da se te krimilane radnje dovedu u vezu sa njima. Međutim, ne mogu se ni zanemariti loše strane tih privatnih agencija, države se vode boljitkom za nacionalni interes, ono što je pokretač ovih privatnih agencija, jeste profit. Činjenica je da se sve više države, i druge organizacije odlučuju za usluge ovih nedržavnih aktera. Međutim problem je što vlast,

ili druge organizacije, daju svoje povjerljive podatake ovim cyber kompanijama, te se i same na takav način izlažu riziku. Mnogi autori navode da su zapravo demokratske države najranjivije u cyber prostoru, baš zbog transparentnosti i dostupnosti informacija. Neke moderne države, poput SAD-a i Kanade imaju razvijen model glasanja za predsjedničke izbore preko interneta, i to je bio jedan od glavnih motiva Ruskim hakerima za napad i obavještajno djelovanje. Oličenja demokratije jesu očuvanje ljudskih prava i sloboda, ali i očuvanje sigurnosti građana. Karakteristika demokratije je i sloboda medija, nevladinih i drugih organizacija. Koncept sigurnosti više nije tradicionalan, i on nadilazi naglašavanje sigurnosti na državnom nivou, već on zahtijeva i zaštitu građana, njihovih prava i sloboda. Da li država u želji da građanima pruži što veću sigurnost, narušava svoju demokratiju, a samim tim i slobodu građana? Činjenica je da je pojedinac, zbog svoje informacijske nepismenosti, jako izložen u cyber prostoru, te zbog toga možda neke države, u suradnji sa privatnim kompanijama, ograničavaju sadržaj dostupan na internetu. Da bi država osigurala ta ista prava i slobode, ona mora aktivirati sve grane sistema nacionalne sigurnosti i osigurati dobar nadzor i kontrolu nad istim.

Šta bi zapravo bila demokratska kontrola? Demokratski nadzor i kontrola se najprije odnosi na parlamentarni nadzor i civilnu kontrolu nad sektorom koji se kontrolira, odnosno nadzire. Ukoliko je stepen demokratije u nekoj zemlji veći, tada se i stepen demokratske kontrole povećava. Predstavljaju tendencije kojima je u cilju, da što u većoj mjeri zaštiti suverenitet, teritorijalnost, ali i svoje stanovništvo. [1]

Glavni cilj cyber napada na neku državu je njena nacionalna sigurnost. Primjer, Zapadni Balkan je podneblje koje najmanje pridodaje značaj za cyber ratovanje i sigurnost. Na nivou Bosne i Hercegovine na snazi je osam zakona koji sadrže pravnu regulativu koja tretira sigurnost na internetu, ali ne postoji zaseban zakon o cyber/informacijskoj sigurnosti. Tek nedavno su postavljene određene smjernice, uz pomoć OSCE-a, za izgradnju pravog strateškog okvira koji se odnosi na cyber prostor. Zbog kompleksnosti ovog načina ratovanja, suočavanjem sa istim, i valjan odgovor, to nadilazi državu kao pojedinca. Gdje država svoje strategije u domeni cyber ratovanja, mora da bazira na iskustvima drugih država i međunarodnih organizacija, ali i da uzme u obzir međunarodna prava.

Nakon slučaja sa Estonijom, na zahtjev NATO-oa, grupa stručnjaka je godinama marljivo radila na ovom projektu koji bi obuhvatao cyber ratovanje i pravne uredbe. Tallinski priručnik je predstavljao prvi korak ka izučavanju i razumijevanju pojmova koji se vežu za cyber

[1] Beridan, Izet, Politika i sigurnost, Fakultet političkih nauka, Sarajevo 2008. str. 225.

prostor. Cilj je bio da se sa već postojećim deklaracijama i uredbama o upotrebi sile, humanizaciji rata u tradicionalnom ratovanju, te deklaracije izjednače i urede i za cyber ratovanje. Priručnik u velikoj mjeri ograničava upotrebu zabranu sile, odnosno konvencionalnog oružja, u međunarodnim odnosima, gdje se izuzima pravo na silu u slučaju samoodbrane. Glavni akcenat priručnik stavlja na očuvanje suvereniteta. Cyber prostor nije ničiji, država ima pravo jedino da očuvaju svoj suverenitet i općenito ono što spade u tu domenu. NATO je oformio svoje odredbe o cyber prostoru i ratovanju. 2002. godine je na summitu NATO-a u Pragu identificirana potreba da NATO ojača svoje sposobnosti da se obrani od cyber napada, također utemeljen je Cyber Defense program. Ovaj je program stvorio NATO Computer Incident Response Capability (NCIRC) kako bi NATO bio efikasniji i uspješniji u borbi protiv cyber prijetnji. [2]Što se tiče Vijeća Evrope, ono je zbog prijetnje koja vreba unutar cyber prostora donijelo Konvenciju o cyber kriminalu, koja stupa na snagu 2004. godine, i do danas predstavlja najoštrij zakon i regulative koje se vežu za zločine unutar cyber prostora. Organizacija Američkih Država je također usvojila „sveobuhvatnu Strategiju kibernetičke sigurnosti američkih zemalja“ kojoj je cilj između ostalog usvojiti politike i zakonodavstvo protiv cyber kriminala koji će štititi korisnike interneta i spriječiti kaznenu zloupotrebu računala i računarskih mreža uz poštivanje privatnosti i individualnih prava korisnika interneta.

Također tu su i Međunarodne konvencije o zabrani cyber ratovanja, te međunarodni cyber sporazumi. Povelja UN-a glavni je izvor koji može regulirati cyber ratovanje. OSCE je recimo institucija koja radi preventivno na cyber prijetnjama. OSCE zajedno sa svojim institucijama oformljava platforme i radi promicanja adekvatnih i pravovremenih reakcija nacionalnih vlasti na ove razvijajuće se prijetnje, u rasponu od bolje forenzike do inovativnih pristupa.

[2]Sadržaj dostupan na: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf Pristup: 02.05.2020.

II TEORIJSKO-METODOLOŠKI DIO RADA

2.1. Problem istraživanja

Demokratski nadzor i kontrola se najprije odnosi na parlamentarni nadzor i civilnu kontrolu nad sektorom koji se kontrolira, odnosno nadzire. Ukoliko je stepen demokratije u nekoj zemlji veći, tada se i stepen demokratske kontrole povećava. Predstavljaju tendencije kojima je u cilju, da što u većoj mjeri zaštiti suverenitet, teritorijalnost, ali i svoje stanovništvo.[3]

Demokratija je prvo polazište i garant, zaštita ljudi i njihovih prava od autoritativnih režima. U tu svrhu u demokratskim režimima je došlo do podjele vlasti na izvršnu, zakonodavnu i ustavnu. Demokratski nadzor je podrazumijevajući, jer je činjenica da nije rijetkost i nepoznanica da se desi udar na državu, vojne pučeve, građanske ratove i slično.

Prema tome, problem magistarskog rada je uočavanje samog pristupa demokratskog nadzora kad je riječ o cyber ratovanju u svijetu.

2.2. Predmet istraživanja

Cyber ratovanje moglo bi se reći da je jedan novi oblik ratovanja. U cyber ratovanju, de facto nema oružane borbe, ali je intenzitet prisutan. Samim tim, je ispunjen jedan od načela rata. Mnoge nevladine organizacije rade baš na reformi međunarodnog prava, koje mora da se implementira i u cyber ratovanju.

Stoga, predmet ovog rada je utvrditi načine na koji parlamentarni nadzor djeluje kad je riječ o cyber ratovanju.

2.3. Ciljevi istraživanja

2.3.1. Naučni ciljevi istraživanja

Sama nedovoljna informisanost fenomena cyber rata danas je nedovoljno istražena. Prema tome, očekuje se da će naučni cilj biti značajan iz razloga što će poslužiti kao poluga stvaranju nekih novih, a opet na temelju postojećih, formiranih istraživanja na zadatu tematiku.

2.3.2. Društveni ciljevi istraživanja

Društveni cilj ogleda se u spoznaji društva kao cjeline kad je riječ o cyber ratovanju. Vjeruje se da će ovo istraživanje potaknuti društvo u cjelini kako bi shvatilo cyber kriminala te ulogu parlamentarnog nadzora kad je riječ o istom.

[3] Beridan, Izet Politika i sigurnost, Fakultet političkih nauka, Sarajevo, 2008. str. 225.

2.3.3. Vremensko određenje predmeta istraživanja

Vremensko određenje predmeta istraživanja u ovom istraživanju obuhvata period od razvoja cyber prostora pa do pretpostavki kraja 2020. godine.

2.3.4. Prostorno određenje predmeta istraživanja

Prostorno određenje predmeta istraživanja se odnosi na prostor koji pokrivaju međunarodne institucije zadužene za bezbjednost i cyber sigurnost. To su NATO, UN, OSCE itd. Što jasno pokazuje da se prostorno odnosi na cijeli svijet gdje god postoji izražen cyber razvoj i napredak. Što dalje jasno pokazuje da je ovo istraživanje bez prostornih ograničenja ako u vidu imamo cijeli svijet.

2.4. Sistem hipoteza

2.4.1. Generalna hipoteza istraživanja

Demokratski nadzor i kontrola nad cyber ratovanjem nije dovoljno i jasno definisan, kako u domaćem tako i u međunarodnom pravnom okviru.

2.4.2. Posebne hipoteze istraživanja

Pravo oružanih sukoba se primjenjuje na sve aktivnosti poduzete tokom trajanja oružanog sukoba, i na sve posljedice nastale na teritoriji država koje su uključene u oružani sukob ne ograničavajući se samo na prostor gdje se vrše vojne operacije.

Cyber napadi podliježu primjeni pravila jus ad bellum koja se odnose na pravo države na upotrebu sile u cilju realizacije svoje nacionalne politike.

2.4.3. Sistem indikatora

Sistem indikatora kad je riječ o određenoj tematici jasno, koncizno i adekvatno služi da bi se upotpunilo znanje o postojećoj problematici. U ovom radu korišteni su deskriptivni indikatori.

2.5. Način istraživanja

Prva faza istraživanje je prikupljanje adekvatnih izvora na zadanu tematiku.

Druga faza odnosi se na analizu i interpretaciju datih izvora.

Treća faza je prikazivanje rezultata datih izvora te davanje suda o istim.

2.6. Naučna i društvena opravdanost istraživanja

2.6.1. Naučna opravdanost

Naučna opravdanost bitna je zbog spoznaje temelja sukoba u cyber prostoru te njihovim inkorporiranjem u današnju literaturnu tematiku.

2.6.2. Društvena opravdanost

Kad je riječ o društvenoj opravdanosti same analize, potrebno je usmjeriti se na one pojmove koji pružaju ključni doprinos suštinskom razumijevanju i normativnom definisanju kategorija poput „cyber sukoba“, „cyber ratovanja“ i „cyber napada“. Potrebno je, dakle razumjeti samu suštinu prirode agresije u cyber prostoru i karakter cyber sukoba i rata kao i uloge parlamentarnog nadzora.

2.7. Pojmovno određenje

Kako bi što bolje razumjeli predmet istraživanja ovog rada, kako stručnjaci ove oblasti tako i drugi ljudi koji su zainteresirani za ovo istraživanje, u nastavku ćemo pojasniti i analizirati ključne pojmove iz ovog rada.

CYBER KRIMINALITET – pojedinci ili grupe koji ciljaju IKT sisteme za finansijsku protupravnu dobit ili za pravljenje (društvene, ekonomske, političke, sigurnosne) dusrupcije. Govorimo o obliku kriminalnog ponašanja kod kojeg a se korištenje IK tehnologije i sistema upotrebljava kao sredstvo ili cilj izvršenja čime se ostvaruje neka krivično-pravno relevantna posljedica. [4]

GRAĐANSKI RAT – jeste masovan i intenzivan oružani sukob između različitih političkih struktura unutar jedne države. Građanski ratovi su se najčešće javljali kao oblici oružane borbe za vlast unutar jedne države.[5]

CYBER RATOVANJE - upotrebu računara, interneta i drugih sredstava za pohranu ili širenje informacija za provođenje napada na neprijateljske informacijske sisteme pomoću sredstava informatičke tehnologije. [6]

PARLAMENT - državno zakonodavno tijelo. Članom parlamenta može se postati biranjem na izborima, ili nekim drugim kriterijem. Predstavnička je institucija političkoga sustava, koja obavlja zakonodavnu vlast. Sastoji se od predstavnika građana biranih općim pravom glasa. Najstariji parlament u svijetu je islandski Althing, uspostavljen 930. U srednjem vijeku, parlament se sastojao od predstavnika vlastele, odnosno aristokracije. U talijanskim renesansnim gradovima prvi put parlament čine predstavnici građana.[7]

---

[4] Krivični zakon Federacije Bosne i Hercegovine Službene novine Federacije BiH, br. 36/2003, 21/2004. ispr. 69/2004. 18/2015. gl. XXXII

[5] Beridan I. *Politika i sigurnost*, Fakultet političkih nauka Sarajevo 2008., str. 121.

[6] Robić, T. *Cyber ratovanje* http://web.studenti.math.pmf.unizg.hr/~trobic/CW.html Pristup: 22.05.2020.

[7] Parlamentarna skupština BiH 2016. https://www.parlament.ba/Content/Read/25?title=FunkcijeParlamentarneskup%20tineBiH Pristup: 22.05.2020.

CYBER – odnosi se na ljude, stvari, politike, pojmove i ideje povezane sa računarskim uređajima i računarskim mrežama, a posebno Internetom i informacijskim tehnologijama. [8]

EVROPSKA UNIJA – Evropska unija je nadnacinala zajednica evropskih država nastala kao rezultat saradnje i integracije koji je počeo 50-ih godina 20.-og vijeka. Ona nije država niti međunarodna organizacija nego predstavlja sui generis tvorevinu. Ciljevi Evropske unije su promocija ekonomskog i socjalnog napretka, balansiran i održiv razvoj, afirmiranje vlastitog identiteta na međunadrodnoj zajednici. [9]

SIGURNOST – Pojam sigurnost je jedan od najčešće upotrebljavanih i najslabije objašnjenih pojmova u terminologiji međunarodnih odnosa. Sigurnost se u međunarodnim odnosima pojavljuje kao najvažniji cilj međunarodnog djelovanja država i jedno od područja gdje se dodiruju unutrašnja i vanjska politika.[10]

Sigurnost općenito podrazumjeva stepen zaštičenosti ljudi od različitih oblika ugrožavanja, zaštitu materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu nacije, države, svjetske zajednice od svih vidova ugrožavanja, a naposljetku sigurnost podrazumjeva stepen zaštićenosti od ugrožavanja na kozmičkom i planetarnom nivou života općenito, ljudskog roda u cjelini.[11]

CYBER SIGURNOST – Podrazumjeva stanje i praksu zaštite infrastrukture, informacijsko-komunikacijskih sistema, mreža, uređaja i informacija od umnožavanja u cilju zaštite ljudi, materijalnih i kulturnih dobara u ličnoj i društvenoj svojini.[12]

KONFLIKT – riječ potiče od riječi conflictare što znači udariti nešto od nešto, boriti se, sukob, spor, rasprava koja prijeti da će se još više zaplesti, oružani sudar.[13]

[8] OSCE https://www.osce.org/bs/mission-to-bosnia-and-herzegovina Sarajevo 2019. Pristup: 21.05.2020.
[9] Direkcija za evropske integracije, Pojmovnik evropskih integracija Sarajevo,2010. str. 73.-74.
[10] Mario Nobilo, *Pojam sigurnosti u terminologiji međunarodnih odnosa*, Pol. Misao, Vol. XXV Zagreb 1988. str. 69.-80.
[11] Beridan I. *Politika i sigurnost*, Fakultet političkih nauka Sarajevo 2008. str. 101.
[12] Beridan I. *Politika i sigurnost*, Fakultet političkih nauka Sarajevo 2008. str 125.
[13] Beridan I., Tomić I., Kreso M., *Leksikon sigurnosti* – Drugo izmjenjeno i dopunjeno izdanje Sarajevo. 2001. str. 83.

III PRINCIPI DEMOKRATSKOG NADZORA I KONTROLE

3.1. Promjena koncepta sigurnosti

Unazad 10 godina promjenila se globalna sigurnosna situacija. Svako društvo posjeduje konkurenciju i vrlo često suprostavljena stajališta o velikom broju pitanja. Demokratsko društvo posjeduje slobodu izražavanja gdje ljudi izraze svoje mišljenje, koje prenose na izabane predstavnike, koji opet dalje razmatraju o pitanjima preko javne debate.

Na ovaj način demokratske zemlje imaju manju opasnost od javljanja sukoba. Nepostojanje demokratskih institucija dovodi do širenja tenzija van kontrole koje ubrzo eskaliraju u sukob dok demokratija vodi ka miru i sigurnosti. Opšta sigurnost vodi ka dobrotiti cijelog čovječanstva. Demokratija ima korjene u djelotvornom radu parlamenta. Suverenitet zajedničke države postoji ako se polazi od suvereniteta ljudskog bića.[14]

Nacionalna sigurnost na početak stavlja čovjeka, a zatim ljudsku zajednicu. Dolazi do stvaranja sve većeg konsenzusa kako bi se sigurnosti pristupilo na sveobuhvatan način uz obavezno praćenje svih faktora koji nisu vojni. Ovaj program sigurnosti daje opširnije razumijevanje prijetnji sigurnosti i određenju moguću reakciju. Službe sigurnosti u ogranizacijama sa zakonskim ovlastima imaju zadatak da upotrebe silu u cilju zaštite države i građana. Sektor sigurnosti nije stručan da odgovori na te izazove. U dvadesetom vijeku su napredak doživjele organizacije za kolektivnu sigurnost, npr. Liga naroda i njen nasljednik, Ujedinjeni narodi kao i kolektivna odbrambena organizacija NATO.

Unutarnji sukobi su dosegli svoj vrhunac. Vijesti o terorizmu i porast unutarnjih sukoba su prepravili sredstva informisanja. Ovisnost država je ojačala globalizacija. Ako se poremeti sigurnost u jednoj državi može da se ugrozi sigurnost u Svijetu. Kolektivna sigurnost zadužena je za mir u unutrašnjosti zajednice. Veliku sigurnost u mir ulijevaju Ujedinjeni narodi. Kooperativna sigurnost veže kolektivnu sa ukupnim konceptom sigurnosti. Kolektivni odbrambeni aranžman je jedan vid saradnje. Sva ova saradnja pojaćava sigurnost u zemlji i čini otpor svim prijetnjama izvan zemlje. Zemlja čelnica ima obavezu da se prilagodi ciljevima i uslovima. Ona utiče i na parlamentarni nadzor, a proces odlučivanja prelazi na međunarodnu scenu.

[14] Carter/Trimble/Bradley. (2003) International Law, forth edition. New York: Aspen Publisher. Dinstein, Y.: War, Agression and Self -Defence, Cambridge University Press, 1994. str. 433.

3.2. Uslovi djelotvornog parlamentarnog nadzora

Sigurnosna politika posjeduje potrebno znanje i može brzo djelovati. Najtemeljniji problem politike je izbjegavanje autokratske vladavine. Vrši se sistem promjena i balansa kao protuteza moći izvršne vlasti. Parlamentarni nadzor je osnovni element raspodjele vlasti na državnom nivou i ako je djelotvoran on ograničava moć izvršne vlasti.

Budžet je jedan od važnih mehanizama parlamenta za kontrolu izvršne vlasti. U Zapadnoj Evropi parlamenti su tražili glas u političkim pitanjima jer nema oporezivanja bez zastupljenosti organizacije sigurnosnog sektora kontrole državnog budžeta, a parlament nadgleda korištenje javnih sredstava na efikasan način.

Izvršna vlast utvrđuje zakone koji regulišu pitanje sigurnosti. Članovi parlamenta imaju ulogu u razmatranju zakona. Parlament vodi računa o tom da li je zakon u potpunosti primjenjen. Članovi parlamenta imaju kontakt s građanima i ocjenjuju njihova gledišta.

Zakoni o trajnosti mogu ograničavati i ugroziti parlamentarni nadzor nad sektorom sigunosti. Ne postoje zakonski propisi kojim se reguliše sloboda informisanja. Parlament vrši nadzor nad pitanjima npr.nabavka naoružanja, kontrola naoružanja, spremnost vojnih jedinica i sl. Mandati u parlamentu su vremenski ograničeni i nemaju pristup ekspertima u zemlji i inostranstvu. Parlament je u mogućnosti da doprinosi donošenju odluka na međunarodnom planu.

3.3. Parlamentarni mehanizmi primijenjeni na sektor sigurnosti

Državni sistem daje parlamentu sredstva za pribavljanje informacija, kontrolu politike i uprave, zaštititu pojedinca, otklanjanje nepravde i zloupotreba. Tri su zakonske mogućnosti za sticanje informacija od vlade:

- Parlamentarne debate
- Parlamentarna pitanja i upiti
- Parlamentarna istraživanja.[15]

Parlamentarne debate po pitanju sigurnosti daju mogućnost razmjene mišljenja i prikupljanje informacija u vezi sa namjerama vlade. One se odvijaju u sljedećim vrstama sigurnosti: nakon što izvršna vlast iznese izvještaj za godišnji vojni budžet, zatim, nakon zvaničnih i nezvaničnih izjava resornih ministara (ministra odbrane i ministra vanjskih poslova), predočavanje bijele knjige za odbranu u vezi sa vladinim programima koji se prenose poslije

[15] Brownlie, J: International Law and the use Force by States, Oxford University Press 1963. str. 225.

izbora, te bilo koje pitanje parlamenta koje sadrži parlamentarnu debate npr. skandal ili veći problem koji ugrožava sigurnost.

Pitanja čine glavni dio parlamentarne funkcije i sadrže jedan od najvažnijih procedura za nadzor nad mjerama vlade. Poslanička pitanja daju članovima mogućnost da članovi imaju tačne informacije o sigurnosnoj politici vlade. Poslanička pitanja pomažu parlamentu da kontroliše kako se primjenjuje Zakon o sigurnosti koji parlament usvaja. Pomažu usmjeravanju pažnje javnosti kad se odgovor na postavljena pitanja emituje putem medija. Ima važnu ulogu i u uticaju političkog programa po pitanju sigunosti.

Također, daje se mogućnost članovima opozicije da pokrenu pitanja za koja su zainteresovani. Pitanja poslanika su vrlo osjetljiva kad je u pitanju sigurnost. Za davanje odgovora nadležan je ministar. Dokumenti u vezi državne sigurnosti su povjerljivi i nisu dostupni ni parlamentu ni javnosti. Ovlasti izvršnih vlasti su povjerljive i zakonski su ograničene. Zna se tačno i koji dokumenti mogu biti povjerljivi. Djelotvornosti poslaničkih pitanja doprinose faktori kao što je mogućnost parlamenta da postavi pitanje ako im treba nešto pojasniti. Mogućnost poslanika da pokrene debatu o poslaničkim pitanjima spada, također u ovu nadležnost.

Članovi parlamenta imaju mogućnost da postavljaju pitanja. Javnost može prisustvovati sjednici gdje se postavljaju pitanja ili da dio sjednice prate putem medija. Parlamentarne komisije učestvuju u nadgledanju nad politikom vlade. Aktivnosti vlade prate se putem privremenih zadataka sa komisijom i na kraju se daje informativni izvještaj.

Na sudsko saslušanje se šalju pozivi. Prednosti istražne komisije su velike, i njihovo formiranje se tumači od strane javnosti kao pozitivan signal u politici. Istražne komisije mogu pružiti ocjenu vladine politike o pitanju sigurnosti. Za ishod istrage od velikog značaja je udio poslanika u parlamentu iz opozicije. Ovlaštenja se razlikuju od parlamenta do parlamenta i između komisija. Ključne ovlasti čine, između ostalog biranje teme i obim istrage u parlamentu, obilazak vojnih baza i drugih objekata, zatim, skupljanje povjerljivih informacija i dokumenata, ali i organizovanje javnih saslušanja.

3.4. Parlamentarne komisije za obranu ili sigurnost

Pravilno razrađena struktura od velikog je značaja i ima uticaj na izvršnu vlast. Parlamentarni nadzor nad sektorom sigurnosti obuhvata nekoliko komisija pod različitim nazivima a to su: komisija za odbranu i oružane snage, komisija za sigurnost, za vojne poslove, organizaciju osoblja. Komisija za vanjske poslove bavi se odlukama o masovnim misijama i učešću u njima, o međunarodnoj sigurnosti. Komisija za budžet ili fianansije ima glavnu riječ u vezi

budžeta, kad je u pitanju revizija javnih računa i pregled izvještaja za državni bužet. Komisija za obavještajne službe i pitanja koja se obavljaju iza zatvorenih vrata. Komisija za industriju i trgovinu kad je u pitanju nabavka naoružanja. Komisija za nauku i tehnologiju kad je u pitanju vojno istraživanje. Komisija za unutrašnje poslove bavi se policijom, i graničnom policijom.

Ovlasti za prikupljanje dokaza su različite. Neke stalne komisije nemaju pravo same prikupljati dokaze dok druge imaju neograničene ovlasti. Za izvršenje mandata veoma je bitan nivo stručnosti i raspoloživih sredstava. Posebno mjesto među akterima u institucijama zauzima Ombudsmen. U nekim zemljama ima opštu nadležnost i rješava sve probleme koji nastaju zbog lošeg rada admisitracije. Komesar komisije bavi se i raznim razmatranjem pritužbi građana. U nekim zemljama postoji posebni Ombudsmen kad su u pitanju oružane snage. Ombudsmen za odbranu javlja se pod raznim imenima u nekoliko zemalja. Ombudsmen za praćenje vojske u ime parlamenta- njegov je zadatak da istraži odluke koje su samovoljno donesene.

Parlament imenuje Ombudsmena za odbranu i podnosi izvještaj Parlamentu (Njemačka, Švedska) ili ministarstvu odbrane ga imenuje. Vojska na odsluženju vojnog roka ako bi bila maltretirana može pitati Ombudsmena da pokrene istragu zbog zlostavljanja. Ako on kaže da je žalba trebala postojati nadležna institucija preispituje ili mijenja odluku. Zbog državne sigurnosti masa informacija se ne daje u javnost. Posebnim uredbama se reguliše način i granica do koje je Ombudsmenu dozvoljeno da istražuje i pristupi vojnim bazama, ali Ombudsmen ne smije dati u javnost rezultate istrage. Evidencije o vojnom Ombudsmenu iznose da je institucija veoma jak instrument koja jača i unosi povjerenje u javnosti. Ombudsmen štiti i muški i ženski spol koji je u vojnoj službi od zloupotrebe kao i veću transparentnost u administraciji.

3.5. Značaj parlamentarnog nadzora

Nadzor se definiše kao praćenje i nadgledanje kako rade vladine organizacije i kako se provodi zakon. On pomaže da se unaprijedi kvalitet rada i daje legitimnost politici rada. Zakonodavstvo može spriječiti zloupotrebu nezakonitih radnji u javnim organizacijama. Određuje se opravdano trošenje javnog novca i provođenje politike rada.

Članice OSCE-a nalažu da javna vlast treba da poštuje Ustav i poštuje zakonske uredbe. Također, članice OSCE-a prihvataju oblik vlade koji je reprezantativan na pravi način. Izvršna vlast je odgovorna zakonodavnoj ili biračkom tijelu. Obaveze OSCE-a tiču se nadzora

parlamenta o pitanju vojnih i paravojnih snaga, obavještajnih službi i policijskih službi na nivou države. Poslovnici pružaju detaljniji okvir za pružanje nadzora.

3.6. Zakon o parlamentarnom nadzoru Bosne i Hercegovine

Bosna i Hercegovina je složeno ustrojena. Ovlasti su pobrojane u Ustavu Bosne i Hercegovine. Efektivan parlamentarni nadzor nad aktivnostima i politikama rada izvršnih vlasti suštinski je dio demokratskog upravljanja, vladavine prava i odgovornog rada predstavnika vlasti. U tom svjetlu, Zakon o parlamentarnom nadzoru može predstavljati pozitivan korak u razvoju i sazrijevanju političkog sistema Bosne i Hercegovine. Ovakvim zakonom bi se uspostavio sveobuhvatan i efektivan okvir za sve nadzorne aktivnosti Parlamenta Bosne i Hercegovine (Parlamentarna skupština) u smislu njenih institucija izvršne vlasti. Izvjesni elementi parlamentarnog nadzora se mogu naći u poslovnicima oba doma Parlamentarne skupštine jer se temelje na ravnoteži nadležnosti, regulativi utjelotvorenoj u Ustavu Bosne i Hercegovine.

U članu 1.[16] stoji da Zakon o parlamentarnom nadzoru reguliše parlamentarni nadzor nad institucijama i organima uprave Bosne i Hercegovine, te nad licima imenovanim, potvrđenim ili odobrenim od strane jednog ili oba doma Parlamentarne skupštine. Nije u potpunosti jasno da li je namjera ove odredbe samo opisati obim Nacrta zakona (tj., da li samo ukazuje na to da je zakon osmišljen da definiše način na koji se vrši parlamentarni nadzor kada Parlament ima nadležnost za nadzor) ili da, ustvari, uistinu definiše obim parlamentarnog nadzora kao takvog (tj., da propisuje da sva tijela i zvaničnici koji se pominju u zakonu podliježu parlamentarnom nadzoru prema ovom zakonu, bez obzira na to da li je nadležnost parlamenta za vršenje nadzora nad njima propisana drugim zakonom). Ako je namjera da se članom 1. utvrdi koje javne vlasti su predmetom parlamentarnog nadzora, pažnju treba posvetiti formulaciji teksta u tom smislu. Naprimjer, ako razumijemo da termini prevedeni na engleski jezik kao ‘institucije’ i ‘organi uprave’ imaju konkretnije značenje u izvornom jeziku gdje one podrazumijevaju izvršne vlasti, nejasno je da li obuhvataju i nedržavne subjekte s izvjesnim javnim funkcijama ili nezavisne regulatore koji su, strogo govoreći, izvan izvršne grane vlasti, kao što je Centralna banka. S druge strane, formulacija ‘lica’ koje imenuje, potvrđuje ili odobrava. Parlamentarna skuština je preširoka, ako se posmatra bukvalno, budući da ta lica mogu biti, naprimjer, sudije Ustavnog suda. Član 1. potrebno je izmijeniti kako bi se

[16] MIŠLJENJE O NACRTU ZAKONA O PARLAMENTARNOM NADZORU U BOSNI I HERCEGOVINI https://www.osce.org/files/f/documents/6/5/322431.pdf Pristup: 22.05.202

razjasnilo da li su navedene vlasti i zvaničnici predmetom parlamentarnog nadzora temeljem ovog zakona (neovisno o tome je li ovo pitanje regulisano nekim drugim zakonom) i, ako jesu, predmet parlamentarnog nadzora treba definirati na precizniji način. Član 2. propisuje da se parlamentarni nadzor „vrši putem stalnih ili ad hoc tijela“ utvrđenim od strane Parlamentarne skupštine. U mnogim parlamentima, stalne parlamentarne komisije obično vrše mnogo nadzornih aktivnosti. Član 2., iako ne isključuje ovakav pristup, može potaknuti uspostavu ad hoc nadzornih tijela koje mogu opteretiti resurse Parlamentarne skupštine, te fragmentirati i preusmjeriti stručno znanje koje je dostupno u sklopu njenih stalnih komisija. Zato je preporučljivo konkretno navesti u Nacrtu zakona da uobičajena funkcija nadzora leži, prvenstveno, na postojećim komisijama, a da nadzor ad hoc komisija predstavlja izuzetak. Ono što je važno jeste da, iako komisije imaju ključnu ulogu u nadzoru, nije tačno da se sav nadzor vrši kroz njih i slična tijela, kako to, izgleda, sugerira član 2. Zaista, neke vrste parlamentarnog nadzora se vrše od strane parlamenta u cjelini, putem plenarnih debata, vremena za postavljanje pitanja i glasanja o nepovjerenju. Nadzor mogu vršiti i pojedinačni članovi parlamenta ili grupe članova putem pisanih i usmenih pitanja upućenih vladi i podnošenjem interpelacija. Zbog toga, iako je korisno uvesti termin „nadzorna tijela“ kada se govori o svim stalnim i ad hoc komisijama i potkomisijama kojima je povjerena funkcija nadzora, član 2. treba izmijeniti kako bi se jasno naznačilo da nadzorna tijela nisu jedini kanal kroz koji se vrši nadzor.

IV GENEZA RAZVOJA CYBER RATOVANJA

4.1. Definiranje pojma Cyber prostora

Iako je uticaj informaciono-komunikacijskih tehnologija na cjelokupno čovječanstvo očigledan i revolucionaran, on je teško kvantitativno mjerljiv, posebno u opštem smislu. Razlog za to su kompleksnost i širina njihove specifične i opšte primjene. Jedan od mogućih posrednih pokazatelja rasta značaja informaciono-komunikacijskih tehnologija za savremeno čovječanstvo je analiza učestalosti svakodnevne upotrebe njihovih karakterističnih lingvističkih simbola (riječi). Ključni izraz u vezi sa primjenom informaciono-komunikacionih tehnologija koji prati cijeli njihov razvoj je izraz cyber. Navedeni izraz istovremeno ima svojstvo riječi, morfeme i lekseme i predstavlja ključni konceptualni simbol

savremene upotrebe informaciono-komunikacionih tehnologija u svim oblastima, uključujući i bezbjednost i odbranu.[17]

Izraz „cyber prostor“ je nastao i razvijao se u SAD, paralelno sa razvojem i primjenom računarskih nauka i informaciono-komunikacijskih tehnologija. Prvo javno upotrebljavano značenje izraza „cyber prostor“ razvili su književni, filmski i strip umjetnici, kao umjetnički i filozofski koncept, u okviru specifičnog, tehnološki orjentisanog, podžanra naučne fantastike, pod nazivom „cyber pank“ (eng. cyberpunk) u periodu od šezdesetih do kraja osamdesetih godina dvadesetog vijeka. Umjetničko-filozofska predstava cyber prostora je obuhvatala konceptualno „virtuelno“ okruženje, sačinjeno od digitalnih podataka. Međutim, bilo bi pogrešno smatrati da su umjetnici zaslužni za stvaranje i postojanje cyber prostora.

S obzirom da međunarodno pravo kreiraju države, u pogledu međunarodno-pravnog definisanja cyber ratovanja i cyber prostora, od najvećeg značaja su stavovi država, a zatim i relevantnih međunarodnih stručnih organizacija. Međutim, ne postoji jedinstvena definicija cyber prostora kao tehničkog, društvenog, vojnog ili prirodnog fenomena. U akademskoj i stručnoj javnosti postoji mnoštvo različitih definicija koje se razlikuju po kontekstu, sadržaju i namjeni. Većina država koje kreiraju vlastite strategije razvoja informacionog društva ili strategije nacionalne bezbijednosti i odbrane su usvojile sopstvene definicije cyber prostora. U određenom broju slučajeva, razlike u njihovim stavovima su značajne. Definicije se razlikuju zavisno od prihvaćenog kriterijuma. Također, zbog brzog razvoja računarskih nauka, inženjerstva i informaciono-komunikacijskih tehnologija, značenje pojma cyber prostor se mijenja u vremenu čak i u okviru istog konteksta, odnosno u okviru istih institucija. Zajednička temeljna svojstva svih definicija cyber prostora su:

- cyber prostor je rezultat primjene računarskih nauka i upotrebe informacionokomunikacijskih tehnologija;
- računarski informacioni sistemi imaju sposobnost međusobne interakcije,
- odnosno stalnog ili povremenog umrežavanja i sve informaciono-komunikacijske tehnologije funkcionišu kroz operacije sa podacima i informacijama.

Ostala svojstva koja se tiču postojanja, upotrebe i karakteristika cyber prostora su ili izvedena iz prethodno navedenih, ili zavise od njih. U te izvedene elemente se mogu svrstati, veličina, položaj/pozicija u prostorno-geografskom smislu, trajanje, gustina, vrijednost i druge. U pogledu osnove cyber prostora, opšti stav je da on predstavlja okruženje, prostor ili najčešće,

[17] Ali, Idrees and Andrea Shalal. „F-35 Chief Cites 'Good, Bad and Ugly' About No. 1 U.S. Arms Program.“ Reuters, March 24, 2016. str. 223.

sredinu, u kojoj postoje podaci elektromagnetne prirode i koji je nastao vještačkim putem. U svim definicijama cyber prostor ima nematerijalnu prirodu (najčešće da je „virtuelni prostor“), odnosno da je dio šireg informacionog okruženja ili prostora.

Cyber prostor je ljudska tvorevina stvorena primjenom informaciono-komunikacijskih tehnologija u elektromagnetnom okruženju u kome se podaci stvaraju, čuvaju, šalju, primaju, obrađuju i uništavaju, čiji su elementi podaci, sistemi, procesi i ljudi koji su umreženi ili mogu biti umreženi. Karakteristike cyber prostora su: cyber prostor je vještačka tvorevina ljudi, zasnovana na primjeni tehnologije; dio je informacionog prostora; te postoji na osnovu ili kao dio elektromagnetnog okruženja; u njemu se stvaraju, čuvaju, šalju, primaju, obrađuju i uništavaju podaci, odnosno– informacije; postoji i funkcioniše na osnovu primjene računarskih informacionih tehnologija; njegovi elementi su podaci/informacije (u digitalnom obliku), informacioni– sistemi i infrastruktura, procesi i ljudi kao kreatori, učesnici aktivnosti i procesa;. Karakteriše ga sposobnost ili mogućnost umreženosti i protoka podataka između dijelova sistema ili između odvojenih sistema; povezanost između njegovih dijelova se načelno ostvaruje na nivou podataka. Ali može biti ostvareno i na fizičkom nivou (fizičke infrastrukture i veze), nivou procesa (uspostavljene veze), nivou ljudi (kao kreatora cyber prostora, faktora koji omogućava njegovo postojanje, korisnika i obrađivača); osnova, procesi, efekti i korisnici cyber prostora mogu postojati na fizičkom, logičkom i kognitivnom nivou.

4.2. Cyber rat

Naravno i pojedinci utiču na mogućnost i način vođenja sukoba u cyber prostoru, i to ne samo kao pripadnici državnih i korporativnih institucija. Crno tržište ranjivosti, eksploita i kriminalnih hakerskih usluga je stvoreno od strane kriminalaca i namijenjeno je kriminalcima. Međutim, i ono ima značajan uticaj na vođenje cyber špijunaže i sukoba između država. Međunarodno pravo oružanih sukoba se odnosi na radnje, postupke i aktivnosti u međunarodnim sukobima između država i drugih subjekata međunarodnog prava. Međutim, ono se odnosi i na krivična djela pojedinaca, organizacija i grupa koja su se desila u tom međunarodnom okruženju tokom oružanih sukoba. Na osnovu međunarodnog prava moguće je utvrditi krivicu pojedinca za krivična djela učinjena tokom međunarodnih sukoba za koja ne postoji odgovornost država. Za sve druge odnose (koji se ne tiču oružanih sukoba) nadležne su druge vrste međunarodnog prava, poput međunarodnog krivičnog i ugovornog prava, ili su nadležna pak unutrašnja prava država u skladu sa njihovim suverenim nadležnostima i jurisdikcijom nacionalnih sudova. Imajući u vidu navedenu ulogu država,

cyber sukobi se moraju regulisati prije svega kao sukobi koji se odvijaju između država u cyber prostoru, i koji dostižu nivo, odnosno posljedice oružanih sukoba.

Cyber ratovanje predstavlja specifičnu formu vođenja sukoba koji se vodi u cyber prostoru putem primjene informaciono-komunikacijskih tehnologija. Tehnologija i rat oduvijek su ostvarivali uzajamnu vezu. Izraelski vojni historičar i teoretičar rata, Van Kreveld navodi: "Ukoliko je tačno da je svaki dio rata pod uticajem tehnologije, ništa manje nije tačno da na svaki dio tehnologije utiče rat". Cyber ratovanje predstavlja izrazit primjer navedene ideje. I druge forme ratovanja u odnosu na područje vojnih dejstava ili na vrstu primjenjenih sredstava, poput, naprimjer, pomorskog, kopnenog, vazdušnog, kosmičkog, oklopno-mehanizovanog, podmorničkog, informacionog ili psihološkog ratovanja su direktno ili posredno zavisne od specifičnih tehnologija. Međutim, rijetko koja vrsta tehnologije i odgovarajućeg ratovanja je u tolikoj mjeri tehnološki zasnovana i povezana sa svim aspektima društvenog života, kao što je to slučaj sa informaciono-komunikacijskim tehnologijama. U savremenom svijetu je teško naći čak i pojedinačnu djelatnosti u kojoj informaciono-komunikacijske tehnologije ne povećavaju efektivnost i efikasnost tehničkih, organizacionih i društvenih sistema ili ne omogućavaju nove sistemske funkcionalnosti. Iako je uzajamni uticaj ratovanja i tehnologije veliki, pomenuta dva fenomena funkcionišu po suprotstavljenim principima, te da se rat ne može dobiti vođenjem isključivo na osnovu tehnoloških principa, bez uticaja ljudske prirode.[18]

4.3. Cyber napadi

Cyber napad načelno predstavlja akte agresije unutar cyber prostora ili kroz cyber prostor na informacioni sistem drugog entiteta. On je oblik vojnog dejstva ekvivalentan primjeni oružane sile, pa se može preduzimati i u ofanzivnom i u defenzivnom smislu. Cyber napadi su vezani za cyber prostor. Ključni sadržaj cyber prostora su podaci i informacije u elektronskom obliku, a faktor koji ga omogućava jesu informaciono-komunikacijske tehnologije. U svakom slučaju, cyber napad je napad i stoga je potrebno analizirati šta oba pojma znače u kontekstu primjene IKT u cyber prostoru, u smislu informacione i cyber bezbjednosti, i u smislu vojno-političke i međunarodnopravne primjene. Cyber ratovanje se izvodi preduzimanjem cyber napada. Njih omogućava prisustvo ranjivosti u svim informacijskim sistemima, kao i sama priroda informacijskih tehnologija, koja omogućava beskonačno kopiranje elektronskih podataka i umrežavanje između sistema na nivou podataka. Pored toga, cyber prostor je

[18] Bertuglia, Cristoforo Sergio and Franco Vaio. Nonlinearity, Chaos & Complexity, the Dynamics of Natural and Social Systems. New York, NY: Oxford University Press, 2005 str. 156. -158.

tehnološki stvoreno okruženje, pa je stoga značaj tehničko-tehnološki orijentisanog pristupa razumijevanju njegovih fenomena od primarne važnosti. Od suštinske važnosti za razumijevanje prirode cyber napada je njihov tehnički i tehnološki kontekst, a ne pravni.

4.3.1. Cyber odbrana

Sigurnost cyber prostora danas predstavlja značajan izazov za nacionalnu sigurnost. Cyber sigurnost se odnosi na tehnologije, procese i prakse koji su dizajnirani da zaštite mreže, računare, programe i podatke od napada, od oštećenja ili od neovlašćenog pristupa. U kontekstu cyber sigurnosti, vlada treba da implementira određene mjere kao što su dizajniranje sigurnih i otpornih mreža, sigurni komunikacijski i informacijski sistemi, te korištenje sigurnosnih politika, standarda i održivih sigurnosnih mehanizama. Cyber prostor postaje prilično dinamično okruženje koje prelazi državne granice i uvijek stvara nove dimenzije nesigurnosti kao rezultat pojave višestrukih centara moći u cyber prostoru, vladinog ili nevladinog. U ovim okolnostima, gore pomenuti akteri će oblikovati događaje u cyber prostoru koji će biti višestruko ciljani i uticati na komunikacijske i informacijske sisteme sa katastrofalnim posljedicama. Cyber sigurnost ili sposobnost da se zaštiti i odbrani upotreba cyber prostora od cyber napada je osnova cyber odbrane. Obezbjeđivanje društva od cyber prijetnji postalo je jedan od najvećih prioriteta, i u tu svrhu vlade moraju energično braniti mreže i sisteme prijetnji unutrašnjim i spoljašnjim prijetnjama. U opsegu cyber odbrane su štetne radnje ili prijetnje (moguće ili stvarne). Cyber odbrana se fokusira na štetne radnje koje su izvorno izvedene iz cyber prostora. Svrha ove odbrane je da obezbijedi trajnost usluga prostora za korisnike. Cyber odbrana predstavlja sposobnost da zaštiti i zaštiti prostor od mogućih cyber napada. Cyber napad, je napad na istoimeni prostor u cilju ometanja, onemogućavanja, uništavanja i kontrole računarske infrastrukture ili uništavanja integriteta podataka i informacija ili njihove krađe. Cyber odbrana danas predstavlja veliki izazov za vlade i može se postići samo kroz međunarodnu saradnju i partnerstvo.

Vlade moraju podsticati koherentan odgovor na osiguranje cyber prostora, a na nacionalnom nivou to je zajednička odgovornost svih ministarstava i vladinih agencija, privatnog sektora i građana. Na regionalnom i međunarodnom nivou, ovo uključuje saradnju i koordinaciju sa svim relevantnim partnerima. Također zahtjeva izbor najbolje kvalifikovanog osoblja koje će voditi ove napore. Korišćenje, upravljanje i odbrana kritične informacione strukture je mnogo lakše kada se odgovornost dijeli i kada postoji međunarodna saradnja i partnerstvo. Sigurnost informacija ili kako i da nazovemo ovo područje koje se bavi sve većim poremećajima u povjerljivosti, dostupnosti i integritetu informacija, je glavni imperativ informacijske

sigurnosti (Information Security), osiguranja informacija (Information Assurance) i cyber odbrane (Cyber Defense). Svi navedeni termini imaju više sličnosti, nego li razlike u načinu na koji se percipiraju sigurnost informacija i sigurnost informacijskih sustava. Sve se one međusobno preklapaju i dijele zajednički izazov, sigurnost informacija. Međutim, postoje i pokušaji da se predstave kao odvojene discipline. Naime, informacijska sigurnost je predstavljena kao podskup informacijske bezbjednosti. Ali, i informaciona bezbjednost je predstavljena kao podskup cyber odbrane, tj. cyber sigurnosti i obratno. Mogućnost konfuzije proizlazi iz sličnosti i činjenice da je cyber sigurnost relativno nova disciplina. Stoga, ona želi da prihvati mišljenje da cyber odbrana pokriva samo cyber prostor, ili da je cyber odbrana u stvari sigurnost informacija plus bezbjednost mreža. Međutim, povećana opasnost od napada informacijske sigurnosti prisilila je vlade da uzmu u obzir i rizike takvih napada na njihove komunikacijsko-informacijske sustave i druge kritične infrastrukture. Pažnja je također posvećena uključivanju država u informacijski rat i mogućnost kolapsa komunikacione infrastrukture ako se ona ne brani.

4.3.2. Cyber obavještajni rad

Obaviještajni rad je jedan od ključnih elemenata u planiranju i provođenju. Kao i neki drugi pojmovi iz teorije informacijskih nauka, ni obaviještajni rad nema jedinstvenu i opšteprihvaćenu definiciju. Neke od postojećih definicija je, da se pod obavještajnim radom podrazumijeva obavještajno djelovanje usmjereno prikupljanje i obrada informacija o okruženju, sposobnostima i namjerama sudionika u području interesa, a u svrhu identificiranja prijetnji i prilika koje mogu iskoristiti donositelji odluka.[19]Zatim, svaka informacija, prerađena ili deformirana od strane državnih tijela kako bi se prikrio njezin stvarni autor, plasirana s ciljem utjecaja na djelovanje jedne ili više stranih vlada, međunarodnih organizacija, dužnosnika, osoba te javnih ili privatnih subjekata s ciljem da njezin autor dobije podršku za ispunjavanje svojih političkih i vojnih ciljeva. Također, u slučajevima postojanja dvostrukih agenata ili u ratnim operacijama obmanjivanja sve informacije (i istinite i lažne) kojima je cilj omogućiti neometano djelovanje dvostrukih agenata. Obavješatajni rad je također i brižljivo, od strane izvještajne službe pripremljena nazovi-obavijest s ciljem unošenja zablude, obmane, ometanja ili potkopavanja povjerenja u pojedince, institucije i vlade. Obavještajni rad je i stvaranje i širenje informacija etiketirajućeg i netačnog sadržaja s ciljem ocrnjivanja protivnika. Zatim, ciljana distribucija netačnih informacija.

[19] Tabain Nikola, Povijest protuobavještajnog djelovanja: Dvostruke igre u Drugom svjetskom ratu, Zagreb, 2020. str. 93.

Obavještajni rad je i svjesno širenje potpuno ili djelomično netačnih informacija riječima, pismom, slikom ili drugim oblicima djelovanja s ciljem zastrašivanja i slabljenja djelovanja i potencijala protivnika. Pojam protuobavijesti je nastao, i razvijen je, u sustavu sovjetskih izvještajno-sigurnosnih službi kao jedno od sredstava i metoda djelovanja uz pomoć koje su izvršavani postavljeni ciljevi i zadaće. Stoga je potrebno objašnjenje i određenje tog pojma početi korištenjem rječnika kojim se koriste izvještajno- sigurnosne službe. Protuobavijest (dezinformacija, eng. disinformation, njem. desinformation, rus. dezirfomacion, tal. disinformazione, fran. desinformation, španj. desinformacion) naziv je koji su prvo upotrijebili pripadnici sovjetskih sigurnosnih službi početkom 20. stoljeća. Protuobavijest su, kao sredstvo borbe protiv svojih protivnika, koristili sovjetski komunisti predvođeni Lenjinom.

U „službenu upotrebu" unutar sovjetskog izvještajno-sigurnosnog sistema ulazi 1923. godine kada I. S. Inshlikt, tadašnji zamjenik šefa GPU-a (preteče KGB-a, današnjeg FSB-a) predlaže osnivanje posebnog ureda za provođenje aktivnih izvještajnih operacija. Pod tim pojmom podrazumijevani su procesi i djelovanja upereni prema stranoj i domaćoj javnosti s ciljem manipuliranja osjećajima i percepcijama javnog mijenja u odnosu na pojedine teme. S ciljem učinkovitijeg planiranja i provođenja operacija protuobavještavanja (dezinformiranja), nametanja poželjnih stavova u januaru 1959. godine osnovan je odjel koji je takva traženja trebao provesti u praksi. Odjel je postao poznat po svom kasnijem nazivu Odjel A, po prvom slovu izraza „aktivne mjere“ koji su Sovjeti koristili kao prikriveni naziv za ovaj oblik djelovanja. Prvi načelnik Odjela bio je general Ivan Ivanovič Agajan koji je tečno govorio nekoliko stranih jezika. Smatra se da upravo Agajan stoji iza operacija kojima je poticano antisemitsko djelovanje njemačkih državljana u Njemačkoj i širom svijeta. Sovjeti su razlikovali nekoliko različitih vrsta djelovanja putem protuobavijesti. Sredinom prošlog stoljeća propagandom su nazivane sovjetske protuobavijesti usmjerene prema Zapadu, a koje su kao takve uspješno prepoznate. Protuobavijest (dezinformacija) je sredstvo, a protuobavještavanje (dezinformiranje) metoda koja se koristi na svim razinama zajednice i društva kao i u skoro svim područjima: poslovnim, socijalnim, političkim, vojnim, sigurnosnim. Može biti usmjerena prema vanjskom i unutarnjem javnom mnijenju, odnosno vanjskoj i unutarnjoj ciljanoj publici.

Dio je procesa provođenja psiholoških, odnosno informacijskih operacija. Cilj je svake protuobavijesti promjena, ili učvršćivanje, postojećeg načina i ili/mišljanja te navođenje protivničke strane (na razinama svjesnog i nesvjesnog odlučivanja) na donošenje odluka i

djelovanje u korist vlastite štete, a u korist onih koji upravljaju IO. Njome se pokušava razbiti kohezija i vezujuća sila koja drži na okupu (bilo da se radi o vjerskim, političkim, kulturnim, povijesnim, civilizacijskim vezama), potkopava se povjerenje u vladajuću strukturu, diskreditiraju se ili omalovažavaju pojedinci i interesne grupe/udruge. Istovremeno, naručitelj i prevoditelj protuobavještavanja se mora potruditi da i on sam, kao i „njegova" javnost, ne postane žrtva protivničkih protuobavijesti.

Cyber potpomognuti obavještajni rad koji se odnosi na prikupljanje podataka putem društvenih mreža i drugih online sajtova koji služe za postavljanje i mogućnost postavljanja podataka. Te podatke koji su korisni za određene obavještajne grupe bivaju preuzeti i provjereni te se njima može upravljati.

Protuobavještavanje je proces kojim se protuobavijest, nekim od mogućih informacijsko-komunikacijskih kanala, upućuje prema cip. Stvaranje učinkovite protuobavijesti zahtijeva znatna predznanja o ciljanoj publici, njezinoj prošlosti, sadašnjosti te očekivanoj budućnosti. Ta se predznanja moraju temeljiti na velikoj količini relevantnih obavijesti (podataka i informacija) prikupljenih na različite načine (javnim i prikrivenim djelovanjima). Tek na temelju izvršenoga temeljitog prikupljanja i obrade prikupljenih podataka može se pristupiti planiranju protuobavijesti na različitim razinama. Njome se može poticati promjena, ali i podržavati postojeći način razmišljanja, odlučivanja, djelovanja sustava vrijednosti kod ciljane publike. Ako je planer nezadovoljan s postojećim stanjem KJZ, nastojat će ga promijeniti (ili u smjeru smirivanja, ili u smjeru pogoršavanja trenutnog stanja). Ako je pak zadovoljan dostignutim stanjem KJZ, isto će pokušati održati nastavljajući svoje djelovanje. Stoga je neophodno stalno pratiti učinkovitost protuobavještavanja (odnosno psiholoških i informacijskih operacija u cjelini) kako bi se iste, na temelju prikupljenih podataka, informacija i raščlambi, mogle po potrebi redefinirati u skladu s novim potrebama i ciljevima te u skladu s mogućnostima novih (ili pak korištenjem postojećih) informacijsko-komunikacijskih sistema i sredstava.

4.3.3. Cyber ratovanje u 20. i 21. stoljeću

Zahvaljujući brojnim nedostacima, neki vid napada u cyber prostoru se uvijek može ostvariti dugim i upornim traženjem načina za neovlašćeni pristup sistemu. To se može učiniti primjenom pojedinačnih elemenata ili njihovom kombinacijom na fizičkom (preko ljudi, elektromagnetnih talasa, energije, hardvera, i u fizičkom prostoru), logičkom (putem logičkih instrukcija i podataka) i na kognitivnom nivou (u svijesti, volji, znanju, razumijevanju ljudi i inteligentnih sistema). U kontekstu informacione bezbjednosti to podrazumjeva uključivanje u

obzir tri ključna područja bezbjednosti: ljudi, procesa i tehnologija. Konceptualni okvir organizaciono-bezbjednosnog trojstva „ljudi, procesi i tehnologije“ je nastao početkom šezdesetih godina kao rezultat istraživanja u oblasti organizacionih nauka, posebno organizacione strategije, strukture i menadžmenta znanja, u uslovima pojave novih automatizovanih tehnologija. Unutrašnje sile organizacije, inherentnu tehnologiju, strategiju, procese, ljude i strukturu organizacija pokreću dvije najvažnije sile u životu svakog organizacionog sistema: spoljno socioekonomsko okruženje i tehnologija. Iz tog koncepta je izgrađen novi model socioekonomskog sistema, po kome svaka organizacija funkcioniše kao dinamički sistem četiri ključne promjenljive: ljudi, tehnologije, strukture i zadataka. Po Lavitovom modelu, promjene u jednom elementu impliciraju organizacione promjene koje ostvaruju efekte na jedan ili više drugih elemenata. Struktura i zadaci organizacije se jednostavnije mogu predstaviti najmanjim zajedničkim imeniteljem koji zadržava svojstvo oba elementa – organizacionim procesima. Cyber prostor je okruženje nastalo funkcionisanjem informaciono-komunikacionih tehnologija čiji su ključni sadržaji podaci, pri čemu ključni procesi potiču od manipulacije ljudi i sistema sa tim podacima. Pokretanje cyber napada predstavlja upotrebu IKT u cilju zlonamjerne manipulacije sa podacima u cyber prostoru. Cayber ratovanje predstavlja ratovanje četvrte generacije i ono ima svoje određene karakteristike od kojih je ključna asimetrija borbenih dejstava tokom sukoba. U toj formi sukoba po pravilu se sukobljavaju nedržavni pokreti sa državama. Cilj njihovog djelovanja u odnosu na jaču stranu je slom, dezorganizacija i delegitimizacija postojeće državne vlasti ili političke i vojne strukture i kampanje jače vojne sile i uspostavljanje vlastitog sistema vlasti. Uprkos tome što vojno razvijenija strana posjeduje očiglednu vojnu nadmoć, asimetrično vojno slabiji protivnik napada konstantno, prikriveno i iznenadno, neprekidno pokušavajući da drži protivnika u fazi vanredne situacije, dezorganizuje ga i prisiljava da troši resurse na vlastitu odbranu.[20]

4.3.4. Studije slučaja cyber napada

Cyber napadi postali su svakodnevnica, te se gotovo na dnevnoj bazi može čuti u raznim informativnim emisijama i pročitati na internet portalima o napadima na web stranice, napadima na korisničke profile na društvenim mrežama, krađu osobnih podataka, krađu intelektualnog vlasništva itd. Svi ovi slučajevi nerijetko se vežu kako uz firme tako i uz pojedince. Ali što je s napadima na kritičnu nacionalnu infrastrukturu (u daljnjem tekstu KNI), odnosno sve ono što ta infrastruktura obuhvaća. O toj temi nema baš puno domaće ili

[20] Lind, Nightengale, Schmitt, Sutton, Wilson, "Changing Face of War", str. 22-26.

strane literature. U interesu državnih službi, ali i velikih kompanija je da takve napade sakriju od javnosti kako bi građani zadržali povjerenje, bilo da se radi o poslovnom odnosu ili građanskoj lojalnosti Ako govorimo o cyber napadima na KNI moramo odmah razjasniti da takav napad dolazi s javnog interneta i bez ekspertnog tehničkog znanja stručnjaka ne možemo niti sa sigurnošću utvrditi tko stoji iza napada. Napadaču je svejedno koliko je udaljen od svoje mete, dok god ima dobro oružje, a u ovom slučaju internetsku mrežu i alate. Ne smijemo zanemariti insiderske prijetnje, gdje je akter osoba unutar sustava, kojima ne treba internetska mreža, nego LAN kao lokalna računalna mreža i softverski alati, ali kako govorimo o KNI uzet ćemo u obzir širi parametar napada, odnosno infrastrukturu koju pruža internet. U pravilu iza napada rijetko stoji jedna osoba nego skupina ili organizacija koja broji više članova, te svi oni međusobno komuniciraju također internetom. Navedena skupina može upravljati botnet infrastrukturom u kojoj se može nalaziti više stotina tisuća zaraženih računala kojima upravlja napadač koji je zarazio ta računala. Računala se mogu zaraziti malicioznim kodom, ili čak kupiti na underground sceni (deep web) za imaginarnu internetsku valutu BitCoin koja se prodaje i kupuje za prave valute, a jedna od najvećih burzi je Mt. Gox koja drži preko 80% svih BitCoin transakcija. Za razliku od glasovne komunikacije telefonom ili elektronskom poštom u prošlosti, današnja komunikacija se odvija putem servisa za koje se ne može osigurati presretanje u realnom vremenu, osim ako nismo prisutni na serveru pružatelja usluge (jedan od primjera je i Skype u vlasništvu Microsofta ili Google Talk u vlasništvu Googlea). Kao što se može pročitati na nekoliko internetskih izvora, FBI-a kao najveći prioritet za ovu godinu sebi postavio zadatak da dobije mogućnost presretanja i čitanja internetskih datotečnih (cloud based) i e-mail servisa u realnom vremenu, ali i drugih oblika internetske komunikacije. Kako proizlazi iz dostupne literature, to još uvijek nisu u stanju, barem ne legalno. Informacije koje dolaze iz FBI-a govore da će se već ove godine promijeniti zakonska regulativa i da će biti moguće u realnom vremenu nadzirati sve internetske servise i to od Dropboxa do internetskih igara u kojima je moguće komunicirati među korisnicima. Svaki od ovih tipova komunikacije može se potencijalno koristiti za kriminalne aktivnosti. Jedna od takvih aktivnosti su i napadi na kritičnu nacionalnu infrastrukturu.

Projekt Olympic Games nikad nije bio javno potvrđen od strane agencija iz SAD-a ili Izraela, za koje se sumnja da su u suradnji razvijali razne oblike cyber oružja koji su bili iznimno uspješni u izvršenju svojih zadataka protiv meta u Bliskom istoku. Projekt je započeo oko 2006. godine pod administracijom tadašnjeg predsjednika G. W. Busha, koji je prihvatio

mogućnost korištenja malicioznog koda da bi se onesposobio Iranski nuklearni program u postrojenju Natanz. Tačni detalji projekta nisu poznati, ali poznat je detalj da je u projekt bila umiješana Izraelska jedinica 8200. Kao rezultat projekta sumnja se da su bili razvijeni maliciozni kodovi: Stuxnet, Duqu i Flame. Maliciozni kod Flame je bio detektiran 2012-te godine od strane CrySiS laboratorija, Iranskog CERT-a i Kaspersky laboratorija. Prve infekcije od ovog malicioznog koda mogu se pratiti već od 2007. što znači da maliciozni kod nije bio detektiran 5 godina, gdje je većina infekcija bila vezana uz računalne sustave u Iranu, Izraelu, Saudijskoj Arabiji, Siriji, Egiptu i Libanonu. Primarna namjena Flamea je bila za špijunažu i prikupljanje informacija, gdje su napadači htjeli prikupiti veliki broj PDF dokumenata i Word dokumenata te nacrta koji su bili izrađeni u alatu AutoCad. Interesantna je velika fleksibilnost Flamea koji ima desetak modula koji služe za razne funkcije te njegova ogromna veličina od 20-ak megabajta. Neke od funkcionalnosti koje je imao je širenje putem mreže, USB stikova, modul za krađu podataka s uređaja koji imaju bluetooth povezanost s inficiranim računalom, prisluškivanje Skype razgovora, spremanje sadržaja koji korisnik unosi putem tipkovnice, spremanje slika koje korisnik vidi na ekranu i velika količina drugih modula. Cijela kompleksnost ovog malicioznog koda je zavidna, gdje se sumnja na povezanost s malicioznim kodom Stuxnet gdje je modul za širenjem malicioznog koda putem USB memorije skoro pa identičan na ta dva maliciozna koda. Drugi maliciozni kod za koji se sumnja da je iz iste porodice je Duqu.

Duqu je bio identificiran krajem 2011. godine, gdje je CrySyS laboratorij utvrdio da se radi o malicioznom kodu iz iste porodice kao Stuxnet. Duqu je bio namijenjen za skupljanje informacija i podataka s računala koje je zarazio i služio je za pripremanje terena za daljnje napade. Jedna od funkcionalnosti mu je bila krađa kriptografskih ključeva i certifikata što je omogućavalo veću razinu pristupa za napade koji su slijedili. Najzanimljiviji maliciozni kod iz skoro svih studija slučaja je Stuxnet. Stuxnet je bio poznat po svojem učinku protiv Iranskog nuklearnog programa. Stuxnet je inficirao računalnu mreže uz pomoć više mehanizama širenja, kao što je širenje putem USB memorija, putem ranjivih mrežnih servisa. Interesantno je bilo korištenje više 0day ranjivosti za koje nije postojala protumjera za zaštitu. Zadnje verzije Stuxneta su imale čak 6 takvih ranjivosti, koje je koristio za inficiranje kontrolera za upravljanje industrijskim postrojenjima gdje mu je primarna namjena bila uništavanje centrifuga za obogaćivanje urana. Prema nekim slobodnim procjenama Stuxnet je uništio oko 1 000 centrifuga u Natanzu povećavanjem brzine rada centrifuge i pokazivanjem operateru centrifuge da je odabrana brzina ona koju je operater unio u kontroler. Prema nekim

slobodnim procjenama, Natanz je u to vrijeme imao oko 3 000 centrifuga što bi značilo da je Stuxnet III. međunarodna znanstveno-stručna konferencija 294 imao značajni utjecaj na Iransku nuklearnu infrastrukturu. Postoje neke informacije prema kojima Stuxnet nije imao značajan utjecaj protiv Iranske infrastrukture jer su nakon 2010. Očito povećane zaštitne mjere i povećan broj centrifuga za obogaćivanje urana. Kao reakciju na taj napad, Iran je povećao svoje ofenzivne sposobnosti za cyber ratovanje i započeo napade na razne mete širom SAD-a.

V MEĐUNARODNOPRAVNE REGULATIVE CYBER RATOVANJA

5.1. Ratovanje u cyber prostoru predmet istraživanja međunarodnog prava

Od razvoja Interneta, početkom 90-tih godina sa svim njegovim prednostima i pozitivnim stranama svjedoci smo pojave i one negativne strane Interneta: cyber kriminala. Internet je postao kao jedno veliko selo, a dodatna otežavajuća činjenica jeste da se radi o internacionalnom prostoru kojim je upravljala samo SAD sa svojim zakonima, dok veliki broj drugih država nije znalo na koji način pravno reagovati na cyber kriminal. Prvi kaznenopravni okvir koji je pokušan sprovesti bio je u SAD kada je predložen savezni zakon o računalnom kriminalitetu. I pored toga što nije izglasan mnogo toga je pozitivnog donio budućnosti ovaj zakon. Evropa je u okviru svojih zakona imala vezu samo sa onim stvarima koje su "opipljive", dok se pojavom Interneta ukazala potreba i za pravnim regulativama vezanim za informacije i druge "beztjelesne vrijednosti". Međunarodna zajednica pokušava putem svojih velikih organizacija da kontroliše i uredi cyber prostor. Svoj doprinos tom uređenju su svakako prirodali i Ujedinjeni narodi čiji je cilj uspostavljanje međunarodnog pravnog okvira koji uređuje sigurnost ovog prostora. NATO isto tako daje doprinos i razvoj za upravljanje i kontrolu cyber prostora. Oni su na samitu u Pragu identificirali problem i potrebu za odbranom od cyber napada i utemeljili su Cyber Defense program.[21] Vijeće Evrope je na konferenciji u Budimpešti 2001. usvojilo Konvenciju o cyber kriminalu koju je potpisalo 38 zemalja svijeta. Ova konvencija prestavlja međunarodni ugovor i njene odredbe se ne primjenjuju direktno nego ih svaka država posebno mora primjeniti u okviru svog vlastitog

[21] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf Pristup: 22.06.2020.

zakonodavstva. Organizacija Američkih Država (OAS) usvojila „sveobuhvatnu Strategiju cyber sigurnosti američkih zemalja“ kojoj je cilj između ostalog usvojiti „politike i zakonodavstvo protiv cyber kriminala koji će štititi korisnike interneta i spriječiti kaznenu zloupotrebu računala i računalnih mreža uz poštovanje privatnosti i individualnih prava korisnika interneta“.[22] Šangajska Organizacija za Suradnju (SCO) Organizacija u svojoj deklaraciji iz Ekaterinburga od 2009. godine ističe da "značaj pitanja osiguravanja međunarodne informacijske sigurnosti kao jednog od ključnih elemenata zajedničkog sustava međunarodne sigurnosti". Ova Organizacija predstavlja potencijalno težište internacionalne pravne regulative u borbi protiv cyber napada.[23]

5.2. Primjena već postojećih uredbi međunarodnog prava na cyber ratovanje

Razne države svijeta su, tijekom druge polovice 20. vijeka, prošle četiri koraka u stvaranju kaznenopravnog okvira koji obuhvaća sve zabilježene oblike cyber kriminala:

- *Zaštita privatnosti*- zbog povećanih mogućnosti za sakupljanjem, pohranjivanjem i prenošenjem podataka putem računala nastaju kaznenopravni okviri o zaštiti podataka (Švedska 1973., SAD 1974., Njemačka 1978., Austrija, Danska, Francuska 1979.);
- *Računalni imovinski kriminalitet*- zbog neadekvatnosti postojećih zakona, koji štite materijalne stvari, nastaju zakoni koji se fokusiraju na zaštitu nematerijalnih stvari poput zakona o neovlaštenom pristupu (SAD 1978., Italija 1979., Australija 1981., UK 1984., Hrvatska 1997.);
- *Zaštita intelektualnog vlasništva*- zaštita autorskih prava za računalni softver, uključujući zakon o autorskim pravima te pravnu zaštitu topografija (Filipini 1972., SAD 1983., Mađarska 1984., Australija, Indija i Meksiko 1985.);
- *Štetan i ilegalan sadržaj*- zabrane širenja pornografije, govora mržnje i klevete (UK 1994., Njemačka 1997.).[24]
- *Talinski pripručnik*- je akademska studija kojom se prikazuje na koji način se međunarodno pravo primjenjuje na cyber kriminal. On nudi pravne smijernice i

[22] Organizacija Američkih Država, A comprehensive Inter – American Cybersecurity Strategy: A multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, Dodatak A, 2004 str. 226.-228.
[23] Hathaway, A. Oona, Crootof, Rebecca, Levitz Phillip, Nix Haley, Nowlan Aileen, Perdue, William, Spiegel, Julia. The Law of Cyber – Attack, SAD, 2012., str. 53.
[24] Chawki, M. A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy, 2008. str. 83.-85.

pokazatelje svima, te prikazuje kako napad putem računala se može računati kao oružani napad u pogledu međunarodnih zakona.

Pored navedenih dokumenata i sporazuma, međunarodna politika je donijela i druge dokumente i sporazume kako bi pokušala kontrolisati i regulirati cyber prostor. Međunarodni sporazumi koji mogu pomoći u stvaranju boljeg cyber prostora s

- *Ugovori neširenja nuklearnog oružja* – Napravljeni su kako bi spriječili širenje nuklearnog oružja u početnim fazama razvoja.
- *Antarktički ugovorni sistem i svemirsko pravo* – Kontrolira se korištenje svemira kao mjesta gdje se može koristiti nuklearno oružje i ako se nuklearno oružje postavlja na svemirsko tijelo.
- *Konvencija UN-a o pravu mora (UNCLOS)* – Kao i svemir i okeani nude nesagledliv prostor koji je sličan cyber prostoru. Ova konvencija je mogla biti primjenjivana dok određene svjetske sile nisu odobrile pristup zahtjva za prenos tehnologije UN-u.
- *Ugovor o uzajamnoj pravnoj pomoći (MALT)* - SAD trenutno prati ovaj pristup dok Rusija preferira analogiju tretiranja cyber oružja kao oružja masovnog uništenja i zabrane njegovog korištenja pod režimom odgovarajućeg sporazuma.
- *Povelja UN*-a – Na osnovu koje bi se najbolje mogao regulisati cyber prostor jeste upravo po ovoj povelji. Međutim problem predstavlja dio oko korištenja sile koja se u ovoj povelji ne dozvoljava. Može se koristiti uz odobrenje Vijeća sigurnosti ili eventualne samoodbrane. Cyber prostor nema „oružanog napada“ te je tu velika polemika vezano za ovu povelju.
- *Obveze među državama* - Države imaju dužnost koja se sastoji od nekolicine manjih kako bi spriječili cyber napade uključujući donošenje strogih kaznenih zakona, provođenje istraga, kaznenog progona napadača i tijekom trajanja istrage i kaznenog progona, sudjelovanje s državom-žrtvom. Jedini međunarodni sporazum koji se direktno bavi cyber napadima jer Europska konvencija o cyber kriminalu. Iako je sporazum samo regionalan, i dalje je jako utjecajan na međunarodno pravo zbog važnosti država koje su ga ratificirale. Nadalje, demonstrira kako su države svjesne da je potrebno kriminalizirati cyber napade i da je dužnost država da spriječe da na njihovom teritoriju nedržavni članovi provode cyber napade protiv drugih država.[25]

[25] Scott Shackleford, članak., „From nuclear War to Net War: Analogizing Cyber Attacks in International Law“, objavljeno u Berkeley Journal of International Law (BJIL), Vol 25 No 3. 2009. str. 51.

5.3. Primjena principa ratovanja na cyber prostor

Ratovanje u cyber prostoru odnosno cyber napadi su relativno novi oblik ratovanja i prijetnji. Država koja je doživjela napad mora znati napraviti razliku da li je doživjela oružani napad ili predstojeći oružani napad prije nego odgovore sa aktivnom odbranom. Znanstvenici su obavili istraživanja i utvrdili nekoliko principa i modela cyber napada. Postoje tri glavna modela:

- *Instrumentalni pristup* - koji provjerava je li učinjena šteta novog oblika napada mogla biti učinjena samo kroz cyber napad;
- *Pristup djelovanja* - zvan posljedični pristup, u kojem je sličnost napada s cyber nebitna već je bitno sveobuhvatno djelovanje na državu-žrtvu;
- *Pristup striktne odgovornosti* - u kojem cyber napadi protiv kritične infrastrukture automatski tretirani kao oružani napadi, s obzirom na ozbiljne posljedice koje mogu nastati zbog onesposobljenja takvih sistema.[26]

5.3.1. Tallinski priručni osvrt na međunarodna prava

Razvojem cyber prostora koji je, kako vrijeme odmiče, sve složeniji i rasprostranjeni došlo je do potrebe za razvojem i izradom međunarodnog pravnog dokumenta za cyber ratovanje i cyber napade. U ovom dokumentu je obuhvaćen ovaj prostor, norme i prava za vođenje napada i ratova putem cyber prostora te mogućnost djelovanja putem međunarodnog prava. 2009. godine skupina stručnjaka je radila oko tri godine na ovom dokumentu, da bi 2013. Godine ugledao svjetlo dana. 2017. je izašla i dorađena verzija. Glavni pokretač i zagovornik za izradu ovog dokumenta bio je NATO, te na kraju je izrađen dokument pod nazivom Tallinski priručnik.

Ovaj priručnik je akademska, neobavezujuća studija o tome kako bi se trebalo međunarodno pravo primjeniti u cyber prostoru. Tallinski priručnik nudi ekspertima iz oblasti međunarodnog prava, onima koji prave razne napade ali i onima koji su napadnuti u cyber prostoru, kako i kada ovi napadi mogu da se vode kao oružani napadi po međunarodnom pravu. Nisu svi računalni napadi, koliko god oni ozbiljni i opasni bili, na nivou oružanog napada. Pomoću ovog dokumenta se pokušava protmačiti i napraviti ta razlika ali zbog svakodnevnog razvoja i napretka ovog prostora to je prilično zahtjevan proces. Tallinski priručnik kao što i u samom nazivu kaže nije obavezujući dokument na međunarodnom nivou, nego samo „priručnik“ kojeg su izradili neovisni znanstvenici u određenom vremenskom

[26] CRS Report for Congress, Cyberwarfare, Steven A. Hildreth, http://www.fas.org/irp/crs/RL30735.pdf Pristup: 21.06.2020.

periodu. Cyber prostor, napadi unutar njega su danas svakodnevni i postepeno se sve više pojavljuju i razvijaju. Velika je razlika između savremenih napada i tradicionalnih istrojiskih napada i ratova. Zbog toga je veoma važno da postoji dokument koji sadrži sve potrebne smijernice za države koje se nalaze u problemu sa cyber prostorom. Pomoću ovog priručnika se može utvrditi i odrediti mogućnosti i sankcije na međunarodnom pravnom nivou ali i na nivou pravne države u kojoj se potencijalno ti napadi i problemi dešavaju.

5.3.2. Legalnost cyber ratovanja

Kroz historiju mnoge države, carstva i kraljevstva su osvajana i formirana na osnovu ratova. U bližoj historiji i kod nas su bili strašni ratni periodi koji nikome ništa dobro nisu donijeli. Kako se tehnološki države razvijaju, velika razlika između velikih i malih država, odnosno onih koji su važni na svjetskoj mapi. Svi ratovi koji se vode imaju određene upute šta je dozvoljeno, a šta nije dozvoljeno zavađenim stranama. Te upute i pravila treba da poštuju, jer međunarodna zajednica ima svoje sudove putem kojih mogu da dokažu ukoliko je neko od strana kriv i prekršio pravila ratovanja. Jedan poznat primjer jeste međunarodni sud u Haagu koji ima svrhu da prikaže i dokaže sve zločine koji su se desili za vrijeme rata na Balkanu. Legalnost ratovanja pa tako i cyber ratovanja se najbolje objašnjava time šta se smije raditi odnosno koje se radnje smiju poduzimati. Kroz međunarodno humanitarno pravo je sve objašnjeno i prikazano šta je legalno, a šta nije prilikom sagledavanja ratova. Cyber prostor je relativno novi pojam, ali se sve više i brže razvija i širi, a samim tim se pojavljuju i cyber ratovi koji se vode.

- *Prijetnja i napad na civile* – cyber napadima ili akcijama se mogu ugroziti veliki broj života nevinih ljudi. Kontrola ili napad na nuklearna postrojenja, hemijska postrojenja ili brana, mogu se desiti i tkz. Kolateralne žrtve.
- *Pravo na samoodbranu* – Jasno je da svi moraju poštovati Međunarodno humanitarno pravo odnosno svi se moraju pridržavati pravila i običaja rata. Ako se putem digitalnog napada desi fizička šteta, svakako legalno izvšiti samoodbranu. Međutim ukoliko se desi cyber napad bez fizičke štete treba se urediti da isto tako može napadnuta strana da ima legalno pravo na samoodbranu.

Da bi cyber napadi mogli da se karakterišu kao napadi za pravno oružane sukobe moraju da uzrokuju štetu i biti tako opasni kao što su i napadi nekim drugim oružjem npr. biološko, konvencionalno, hemijsko ili nuklearno. Na cyber napade se primjenjuju postojeći pravni izvori: međunarodni ugovori, međunarodni običaji i opća pravna načela. Cyber napad ili

ozbiljna prijetnja cyber napadom od strane jedne države usmjeren protiv cyber infrastrukture druge države predstavlja povredu njene suverenosti što povlači odgovornost države za međunarodne protivpravne akte.[27]

5.4. Savremeni izazovi međunarodnog prava

Međunarodno pravo predstavlja skup pravila koja su zadužena za regulisanje pravila i odnose između država na međunarodnom prostoru. Ono ne reguliše samo odnose između država, nego i odnose između međunarodnih organizacija i država, odnose između naroda. Ovo pravo se primjenjuje na sve države dok regionalno pravo reguliše samo odnose između država određene regije.

Međunarodno pravo uređuje odnose između država na međunarodnoj sceni i to se znatno razlikuje od onoga što se dešava unutar država. Značenje pojma međunarodne zajednice nije jednako kao što je nekad bilo. Savremeni međunarodni tokovi donijeli su množenje odnosa, kao i posebnih sposobnosti različitih subjekata koji stupaju u te odnose, ali su omogućili i dekompoziciju u pogledu priznanja i samog značenja pojma međunarodne zajednice.[28]

Savremeni izazovi su svakako usložnjeni iz razloga velikih međunarodnih dešavanja, ratova na pojedinim dijelovima, velikih migracija, pojave različitih bolesti i zaraza, nesuglasica vodećih svjetskih sila. Isto tako razvoj „digitalnog prostora“, velike mogućnosti koji taj prostor pruža, konflikti i kontrola tog prostora je jedan veliki izazov za međunarodnu zajednicu i međunarodno pravo.

5.5. Principi Međunarodnog humanitarnog prava

Međunarodno humanitarno pravo se primjenjuje prilikom oružanih sukoba, i primjenjuje se od početka sukoba ravnopravno za sve učesnike bez obzira ko je od njih započeo sukob. Osnovni zadatak ovog prava jeste da štiti sve one koji više ne sudjeluju ili nisu ni sudjelovali u ratu, i ograničavanje određenih sredstava i načina ratovanja. Isto tako medicinsko osoblje, vjerski službenici, ranjenici, bolesnici, civili i sve one koji ne sudjeluju u borbi, ovo pravo čuva pod svojom zaštitom. Osnovna pravila ili principi Međunarodnog humanitarnog prava su:

[27] S. Softić .Međunarodno pravo i cyber sigurnost. Pregledni naučni rad (Zbornik radova), godina XX broj 5. Univerzitet u Sarajevu, FKKSS, 2019. str. 95.
[28] Kazazić, V., Savić, M. Aktualna pitanja međunarodnopravnog subjektiviteta. Zbornik radova Pravnog fakulteta Sveučilišta u Mostaru br. XXVI., 2018., str. 92. – 110

- Vojnici koji nisu sposobni za borbu kao i osobe koje ne sudjeluju u sukobima trebaju biti zaštićeni i prema njima se treba humano odnositi.
- Zabranjeno je ubiti ili povrijediti vojnika ili osobu sa suprotne strane koja se predala ili je neosposobljena za borbu;
- Sukobljene strane moraju pružiti svu moguću medicinsku pomoć i njegu onima koji se nađu pod njihovim nadzorom. Moraju poštivati sve principe Crvenog križa ili polumjesaca;
- Zarobljnici bilo da se radi o civilima ili vojnicima treba da se zaštite od nasilja i osvete;
- Niko ne smije biti mučen, tjelesni kažnjavan ili nasilno ispitivan;
- Strane koje su u sukobu te svi učesnici sukoba nemaju neograničene načine ratovanja kao i sredstva ratovanja;
- Strane koje su u sukobu konstantno moraju da paze na civilno stanovništo, te praviti znatnu razliku između civila i vojnika. Napadati se smiju smamo vojni ciljevi.[29]

5.6. Primjena Međunarodnog humanitarnog prava na cyber ratovanje

Konstantan razvoj i povećanje cyber prostora je više nego primjetan. Svjedoci smo intenzivnog razoja ovog prostora, dok određeni segmenti se ne mogu tako brzo i u korak pratiti. Međunarodno humanitarno pravo na cyber ratovanje djeluje kroz Tallinski priručnik koji je pobliže objašnjen u prethodnim dijelovima ovog rada. Ovim priručnikom se na nekin način uredio do tada izuzetno veliki i nepoznati prostor. Međunarodno humanitarno pravo i njegova primjena na cyber prostor je dalje u tekstu.

Nijedna država ne može tvrditi da ima punu suverenost nad cyber prostorom, dok mogu izvršavati suverene ovlasti nad infrastrukturom i opremom koja se nalazi na njihovom području. Države imaju pravo na osnovu principa suvereniteta da ugase potpuno ili djelomično internet, te ima pravo na kontrolu svih ugovora, opreme ili infrastrukture koji su na njihovom teritoriju. Isto tako nijedna država ne može da zahtjeva suverenost nad cyber prostorom. Država uživa suverenu vlast u pogledu cyber infrastrukture, osobe i cyber aktivnosti smještene na njenoj teritoriji, predmet svojim međunarodnim pravnim obvezama. Država je slobodna provoditi cyber aktivnosti u svojim međunarodnim odnosima, podložno bilo kojem suprotnom pravilu međunarodnog prava koje ga obvezuje. Država ne smije provoditi cyber operacije koje krše suverenitet druge države. Svako uplitanje države u cyber

[29] International Committee of the Red Cross (ICRC). War and international humanitarian law. URL: https://www.icrc.org/eng/war-and-law/overview-war-and-law.htm Pristup: 05.07.2020.

infrastrukturu na brodu oblik, bez obzira gdje se nalazi, koji uživa suvereni imunitet predstavlja: povreda suvereniteta. Država mora vršiti dužnu revnost da ne dozvoli svoju teritoriju, ili teritoriju ili cyber infrastrukturu pod njenom vladinom kontrolom, da se koristi za cyber operacije koje utiču na prava i proizvode ozbiljnih štetnih posljedica za druge države. Načelo dužne revnosti zahtijeva da država preduzme sve mjere koje su izvodljive u okolnostima da se stane na kraj cyber operacijama koje utiču na pravo i proizvode ozbiljne štetne posledice za, druge države U skladu s ograničenjima utvrđenim u međunarodnom pravu, država može vrše teritorijalnu i ekstrateritorijalnu nadležnost nad cyber aktivnosti.

Država može vršiti ekstrateritorijalnu propisanu nadležnost sa vezano za cyber aktivnosti:
(a) sprovode ga njeni državljani;
(b) počinjeni na plovilima i zrakoplovima koji ih posjeduju državljanstvo;
(c) koje provode strani državljani i osmišljena je da ozbiljno potkrada suštinske državne interese;
(d) koje sprovode strani državljani protiv svojih državljana, sa izvesnim ograničenja; ili
(e) koja predstavljaju krivična djela prema međunarodnom pravu koja podliježu međunarodnom pravu princip univerzalnosti .
Država može vršiti samo vanteritorijalnu nadležnost za izvršenje u odnos prema osobama, predmetima i cyber aktivnostima na osnovu:
(a) specifičnu raspodjelu vlasti prema međunarodnom pravu; ili
(b) valjana saglasnost strane vlade za vršenje nadležnosti nad svoju teritoriju. [30]

[30] Tallinn Manual on the international law applicable to cyber warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre od Excellence. General Editor: Michael N. Schmitt Cambridge University Press. 2013. str. 123.- 158.

VI DEMOKRATSKI NADZOR I KONTROLA NAD CYBER RATOVANJEM

6.1. Ratovanje u modernom društvu

Ratovi su vođeni uvijek kroz historiju, od onih malih do razornih. Svaki od velikih je obilježio poglavlje historije čovječanstva, i uticao je na određene promjene na svjetskom nivou. Razvoj ratovanja i ratova se dešavao razvojem društva i cjelokupne civilizacije. To možemo pojasniti jednostavno da se nekada ratovalo lukom i strijelom te najzad dostignuto je ratovanje putem virtuelnog prostora. Kao i u svemu velike sile u svijetu su mnogo više usmjerene u razvoju naoružanja i pripremom vojske zbog raznih ratova koje vode. Tako je i kroz cjelokupnu historiju bilo, jer su sile kao što su (SAD, Njemačka, Francuska, Velika Britanija, Rusija, Kina itd.) pretežno bile te koje su vodile ratove i u većini slučajeva dominirale u tim ratovima. Za ratovanje u modernom društvu se može reći da je karatkeristično to što se povećavaju resursi i sredstva koji se u ratu upotrebljavaju u svrhu komunikacije, vojnog naoružanja, razne prateće mehanizacije, profesionalne specijalizacije vojske itd. Ratovanje odnosno ratovi su dobili drugu dimenziju pojavom Industrijske revolucije koja je dovela do toga da se poveća proizvodnja oružja i njegova primjena.

To se može vidjeti u Prvom svjetskom ratu gdje su ratovale velike industrijske sile protiv Austro-Ugarskog carstva. Svakim novim razvojem određenog društva u bilo kojem smislu, tehnološkom, ekonomskom, industrijskom dolazi do superiornosti u odnosu na nerazvijena društva koja postaju na neki način „zavisna“ od ovih razvijenih. Danas kada je tehnologija i mnogi tehnološki izumi izuztno ubrzali cijelu civilizaciju i sve procese, imaju svoj udio i u modernom ratovanju. To se odnosi prije svega na nuklearno naoružanje ali i virtuelni– cyber prostor. Nova tehnologija se uveliko koristi u procesu ratovanja te je to svakako glavni pokretač modernog ratovanja. Nuklearno naoružanje ili naoružanje koje se koristi putem cyber prostora je skoro nemoguće kontrolisati i regulisati. Može se reći da za ove oblike ratovanja nema niti je moguće postaviti bilo koju vrstu granica, a mogu izazvati ogromne žrtve i posljedice.

6.2. Međunarodna sigurnost

Kada se govori o međunarodnoj sigurnosti ili sigurnosti uopšte, prije toga trebamo znati šta svakom društvu daje sigurnost. Prema riječima mnogih autora, kroz historiju ali i danas sigurnost za društvo je država. Suverenitet i samostalnost svake države je osnova sigurnosti zajednica i ljudi koji se nalaze u toj državi. Najznačajniji događaj za nastanak suverenih država je Westphalski mir iz 1648. godine, kojim je prekinut Tridesetogodišnji rat, vanjska politika postala je sekularizirana, a glavne jedinice međunarodnih odnosa postale su države (još uvijek ne nacionalne države). Te jedinice su bile legalno jednake u međusobnim odnosima.[31]

Sigurnost svake države počinje od njene unutrašnjosti odnosno javne sigurnosti, legitimiteta države i vlasti, ostvarivanja javnih ciljeva, kao i vanjskih faktora vojna odbrana države od eventualnih napada, te podržavanje stanovništva drugim sredstvima kako bi ostvarili egzistenciju. Glavni cilj svake države jeste primarna sigurnost što bi u prevodu značilo što kvalitetnije i duže trajanje političkog sistema (ustavnog poretka u državi). Ljudi koji vode državu i stanovništvo koje je dio te države moraju da imaju isti interes vezano za dobrobit te države. Ukoliko se ta mišljenja razilaze, pitanje je da li ljudi koji vode državu rade u njenom interesu. Nacionalna sigurnost kao pojam označava očuvanje teritorijalnog integriteta same države i njenih granica, odbranu od eventualnih agresija na državu, nezavisnosti države u političkom ili bilo kojem drugom smislu. Kada je riječ o regionalnoj sigurnosti predstavlja jednu od osnovnih interesa svih država regije ali i međunarodne zajednice. Sve je veći broj povezivanja država u zajednice, posebno se to odnosi na zemlje koje se nalaze prema geografiji jako blizu. To ne predstavlja samo skup nacionalnih sigurnosti te regije, nego održava odnose između država, pazi na eventualne sukobe u cijeloj regiji i značajno utiče na nacionalne sigurnosti svake države u regiji.

Kada govorimo o međunarodnoj sigurnosti, međunarodna sigurnost nije samo zbir strategijskih nacionalnih bezbjednosti jer je i nacionalna bezbjednost shvaćena šire (ravnopravnost, nezavisnost, samostalnost, slobodan razvitak), već i opredjeljivanje za odgovarajuće vrijednosti u međunarodnim odnosima pa i u odnosima unutar država (demokratija). [32] Jasno je da međunarodna sigurnost ne predstavlja samo skup nacionalnih sigurnosti i jednoj zajednici, nego je njen prvenstveni zadatak sprečavanje eventualnih masovnih razaranja i uništenja zemlje raznim sukobima i ratovima. Isto tako međunarodna

[31] Cvrtila, V., Države i međunarodna sigurnost, Polit. misao, Vol XXXIV, 1997. str. 31.-43.
[32] Dimitrijević, V. Pojam sigurnosti u međunarodnim odnosima. Beograd, Rad. 1973. str. 83.- 85.

sigurnost dokazuje kvalitetnu suradnju i odnos međunarodnih odnosa, globalnog razvoja i sigurnosti u zajednici. Sigurnost je sve manje nacionalni problem, danas je to problem koji se rješava unutar jedne regije, jačanjem i razvojem međunarodne zajednice. Što je veći broj zemalja povezana kroz jednu zajednicu, to je bolje i pozitivnije utiče na međunarodnu sigurnost.

6.2.1. Ujedinjeni narodi

UN predstavlja najveću svjetsku međunarodnu organizaciju, a čije su članovi suverene države. Zadatak Ujedinjenih naroda jeste prvenstveno da očuvaju i osiguraju mir, kvalitetne međunarodne odnose i suradnju, međunarodnu saradnju na svim poljima između različitih država. Sjedište Ujedinjenih naroda je u New Yorku, a pored toga imaju i niz svojih odjeljenja širom svijeta. UN ima šest glavnih dijelova od kojih se sastoji, a to su: Opća skupština, Vijeće sigurnosti, Gospodarsko i socijalno vijeće, Starateljsko vijeće, Tajništvo i Međunarodni sud pravde. Glavni ciljevi UN-a su: Očuvanje međunarodnog mira i sigurnosti, Razvoj kvalitetnih i prijateljskih odnosa između država, međunarodna suradnja između država prilikom rješavanja različitih međunarodnih problema u ekonomiji, socijalne ili bilo koje druge prirode, biti središte pomoći za narode kako bi ostvarili zajedničke ciljeve. Osnovni i primarni zadatak je svakako održavanje međunarodnog mira i sigurnosti. Članovi Ujedinjenih naroda mogu biti isključivo države koje poštivaju Povelju, i koje Organizacija procjeni da mogu izvršavati obaveze koje su potrebne. [33]

Kada govorimo o međunarodnoj sigurnosti i Ujedinjenim narodima, veza je ta da je UN ogranizacija koja prije svega i primarno ima zadatak za održavanje mira i sigurnosti zbog toga je od početka Vijeće sigurnosti glavni dio same organizacije. Vijeće mora biti sposobno da djeluje jako brzo kada se pojavi slučaj ugrožavanja mira i sigurnosti, zbog toga je svaka članica obavezna da osigura svog predstavnika koji će biti uvijek dostupan u sjedištu organizacije. Posebno važno jeste da UN ima međunarodni sud koji je zadužen za sve međunarodne sporove, pored toga ima i savjetodavnu funkciju na zahtjev UN-a i drugih organizacija. Sjedište ovog suda se nalazi u Haag-u u Nizozemskoj.

Djelovanje Ujedinjenih naroda na održavanje i očuvanje mira i sigurnosti ogleda se i kroz mirovne misije. Svrha mirovnih misija jeste da uz odsustvo upotrebe oružja postignu zacrtane ciljeve a to je postizanje mira između država ili unutar jedne države. Mirovne misije predstavljaju koncept koji je razvijen kako bi se pomoglo državama koje su pogođene sukobima kako bi osigurale mir i sigurnost. Djelovanje ovog sektora Ujedinjenih naroda nema

[33] Oficijalna stranica Ujedinjenih nacija www.un.org Pristup: 25.08.2020.

zadatak da oružano napadne određenu stranu u sukobu ili određenu države. Kroz historiju niz je prilika gdje je UN slao svoje grupe u žarište sukoba kako bi napravili i osigurali potreban mir u tim državama.

6.2.2. NATO

NATO ili Organizacija Sjevernoatlanskog sporazuma predstavlja savez država iz Sjeverne Amerike i Evrope koje poštivaju sporazum potpisan u Washingtonu. Predstavlja međunarodnu organizaciju čiji je pravni temelj pravo na samostalnu ili zajedničku vojnu odbranu svake države. Sve države članice bez obzira na veličinu, politički uticaj, vojnu silu ima jednako pravo odlučivanja unutar saveza. Ono što je specifično za ovu organizaciju jeste da nema svoju vojsku nego se ustupaju vojnici država članica kako bi se pomoglo ili upravljalo određenom krizom u jednoj državi koja samostalno nije u mogućnosti. Primarni zadaci ovog saveza jesu: odbrana i sigurnost, upravljanje krizom i kriznim situacijama i kooperativna sigurnost. Glavni zadatak NATO-a jeste očuvanje mira i sigurnosti, političkim i vojnim putem u zemljama koje su članice ovog saveza. Situacije koje zahtjevaju reakciju saveza se rješavaju prije svega mirnim i diplomatskim putem, ukoliko od toga nema koristi koristi se vojna pomoć u osiguravanju mira i sigurnosti. Oružani napad na jednu ili više država članica saveza znači napad na sve članice NATO saveza. [34]

Kada govorimo o međunarodnoj sigurnosti i NATO saveza, jasan je uticaj ove organizacije koja je sačinjena od niza članica koje se međusobno slažu i osiguravaju sigurnost i mir. Pored toga poštiva se značaj i suverenitet svake od članica ovog saveza bez obzira na njenu veličinu, ekonomsku ili bilo koju drugu moć. To daje dodatnu sigurnost međunarodnom prostoru i dodatno osigurava mir i stabilnost.

6.2.3. Vijeće Evrope

Vijeće Evrope predstavlja najveću razinu i tačku koja je zadužena za razvoj političkih odluka i sigurnosti u Evropskoj uniji. Prema svojoj poziciji i važnosti predstavlja najvažnije političko tijelo Evropske unije. Osnovni zadatak ovog vijeća jeste da se osigura sloboda, sigurnosti i pravda u Evropskoj uniji. Samit kako se nazivaju sastanci čelnika u Vijeću Evrope, je mjesto gdje se vode ključni razgovori na najvišem nivou Evropske unije ali se tu ne donose konačne odluke. U suštini to predstavlja određenu strukturu konačnih odluka vezano za Evropsku uniju. Jedan od glavnih zadataka ovog vijeća jeste utvrditi smijernice i puteve, zajedničkih interesa i politika Evropske unije, sa akcentom na zajedničku vanjsku i sigurnosnu politiku. Tu se rješavaju problemi vanjskih poslova, sporova između država koje su članice Evropske

[34] Oficijalna stranica NATO-a www.nato.int Pristup: 26.08.2020.

unije itd. Ovo vijeće čine svi šefovi država ili vlada članica Evropske unije zajedno sa predsjednikom Evropskog vijeća i predsjednikom Evropske komisije. Cilj Evropske unije jeste da se osnaži ideja slobode i sigurnosti uz poštivanje svih ljudskih prava i sloboda, vladavine prava, i državnih institucija. Sve je usmjereno u povećanja slobode i sigurnosti unutar unije i pružanja pomoći onima kojima je to potrebno. Ono što se radi putem Vijeća Evrope jeste da se štite prava i sigurnost svih građana unije ali i trećih zemelja kojima je pomoć potrebna u vidu osiguranja državnih granica, jačanje policijskih kadrova, opremanje i školovanje kadrova itd. Jačanje sigurnosti je jedan od ključnih dijelova plana koji ima Evropska unija za naredni period. Suzbijanje terorizma, očuvanje sigurnosti svih članica unije ali i Evropske unije u cijelini. Bitno je naglasiti da sve članice unije osim nacionalnih sigurnosti trebaju biti na pomoći ostalim zemljama članicama kojima je pomoć potrebna. Važan dio plana jeste suzbijanje terorizma, njegovog finansiranja, razmjene podataka među zemljama članicama te jačanje policijske saradnje. Cilj Vijeća Evrope i Evropske unije jeste da se uvežu sve nacionalne sigurnosne politike tako što daju određene instrukcije i upute nadležnim institucijama. Zbog toga je tlo Evropske unije područje pravde, slobode svih njenih članica. [35]

6.2.4. Organizacija Sjedinjenih Američkih Država

Sjedinjene Američke Države (SAD) predstavljaju vodeću svjetsku političku, ekonomsku, ali i vojnu silu u Svijetu. Organizacija ove države na svim razinama političkog djelovanja je izuzetno kvalitetna i moćna, da pored svoje nacionalne brige i sigurnosti, djeluju i pomažu drugim državama i međunarodnim organizacijama. Kada govorimo o međunarodnoj sigurnosti i SAD-u, možemo vidjeti kako je ova država članica tri od četiri ključne međunarodne organizacije za sigurnost i međunarodnu saradnju. To jasno pokazuje važnost i veličinu značaja ove države, njene organizacije i političkog djelovanja. Evropska politika je povezana sa SAD-om putem NATO-a. Nijedna država u međunarodnim organizacijama nema vodeću ulogu sve su ravnopravne, ali SAD uvijek imaju jednu od vodećih uloga. Euroatlanski prostor sve se više spominje i koristi kao bliskost SAD-a i Evropske unije koje su povezane prije svega zbog privrede i vojne suradnje. Ova suradnja i povezanost kao rezultat donose svjetski mir i globalnog razvoja u privrednom svijetu. Spajanje ove dvije privrede imamo polovinu privrede u cijelom svijetu i zbog toga je izuzetna važna saradnja ovih institucija. Ova suradnja isto tako pozitivno djeluje na trajanje ali i napredak sigurnosnih sistema, mira i pravde ali i političkih odnosa u cjelini. Nijedna država na svijetu nije toliko sposobna

[35] Oficijalna stranica Evropske Unije www.coe.int/en/web/portal Pristup: 27.08.2020.

organizacijski, vojno, ekonomski ili na bilo koji drugi način, pa tako ni Sjedinjene Američke Države, da nema potrebu pravljenja međunarodne saradnje radi poboljšanja sigurnosti, mira i stabilnosti određene regije ali i cijelog svijeta.

6.2.5. Organizacija za sigurnost i saradnju u Evropi (OSCE-OESS)

Ova organizacije je prvobitno nastala kao Konferencija o Evropskoj sigurnosti i suradnji. Bavi se mnoštvom sigurnosnih pitanja i najveća je regionalna sigurnosna organizacija na svijetu. Članice ove organizacije čine države iz Evrope, Azije, Sjeverne Amerike. Glavni cilj ove organizacije jeste vladavina prava, odnosno ima jako važnu ulogu u rješavanju sukoba u područima kojima je pomoć potrebna. Misije OESS-a jeste da se sukobi riješe i donesu političke odluke kao dogovor, te jačanju kvalitete života i civilnog društva. Zadatak koji rješava ova organizacije jeste saradnja država članica po pitanju pravnog i ekonomskog prostora, demokratije, ljudskih prava i medijskog prostora. Pored toga još su usmjerene u suzbijanju i borbi protiv terorizma. Za Evropske zemlje članice OESS nije primarna organizacija vezana za aspekt sigurnosti, prva je NATO nakon toga dolazi OESS. Ova organizacija ima zadatak da kordinira dogovor Evropskih država po pitanju sigurnosti sa akcentom na rješavanju i prevenciju sukoba. [36]

Specifičnost OESS-a je činjenica da ta organizacija nije osnovana međunarodnim ugovorom nego se zasniva na političkom dogovoru država članica izraženom u praksi i u političkim dokumentima. Obveze država temeljem dokumenata OESS-a su političke obveze, a ne međunarodnopravne (mogu imati međunarodnu obvezatnost iz drugih razloga, primjerice zato što odražavaju međunarodno običajno pravo). [37]

Ova organizacija ima brojne ogranke u zemljama jugoistočne i istočne Evrope te preko svojiih predstavnika utiču i djeluju na razvoj demokratizacije. Oni kroz razna djelovanja npr. Nadgledanjem izbora,, obukom policijskih službenika, podržavaju rad medija, pravodusnih organa itd. Mnogi zvaničnici smatraju da će i dalje ova organizacija imati jako velik značaj. Smatraju da je jedinstvena i nezamjenjiva bez obizira na rast broja članica Evropske unije i njenog razvoja.

[36] Oficijalna stranica OSCE-a www.osce.org Pristup: 28.08.2020.
[37] Vojin Dimitrijević, Obrad Račić, Vladimir Đerić, Tatjana Papić, Vesna Petrović, Saša Obradović, Osnovi međunarodnog javnog prava, Beograd 2005., str. 137–138.

6.3. Osnovni principi demokratskog nadzora i kontrole u sektoru sigurnosti u međunarodnim organizacijama

Sigurnost je jedna od osnovnih ljudskih prava na koje polažu svi ljudi koji žive na određenoj teritoriji. Kroz historiju dešavali su se veliki sukobi i vodili ratovi, i u bliskoj prošlosti smo svjedoci užasnih dešavanja na našim prostorima. Zbog toga su formirane i organizovane organizacije na međunarodnom nivou, kod kojih je jedan od ključnih i primarnih zadataka sigurnost, mir i vladavina prava.

Pored toga je važno i poštivanje suvereniteta države i njenih institucija ali je pomoć međunarodnih organizacija više nego potrebna. U nekim dijelovima ovog rada su već spomenute skoro sve međunarodne organizacije koje se bave održavanjem i uspostavljanjem mira na određenoj teritoriji, gdje pokušavaju putem političkih pregovora da uspostave željene odnose između dvije strane. Ukoliko nije moguće da se to uspostavi diplomacijom, ove organizacije imaju i svoje mirovne misije gdje putem vojne intervencije uspostavljaju mir i stabilnost određenog teritorija. Primjeri ovih organizacija su NATO, Ujedinjeni narodi (UN), OESS itd.

Jasno je da sigurnost i odbranu granica i suvereniteta jedne države održava i ostvaruje svaka država za sebe ali u slučaju da ona nije sposobna to da uradi međunarodne organizacije djeluju i pomažu. Zbog toga na međunarodnom nivou nema dogovorenih standarda u oblasti demokratskog i međunarodnog nadzora sigurnosti. Postoje određeni principi kojima se regulišu civilno-vojni odnos, a to su:

- Država je jedini akter u društvu koji ima legitiman monopol nad upotrebom sile; sigurnosne službe su odgovorne legitimnim demokratskim organima vlast;
- Parlament je suveren i njemu je izvršna vlast odgovorna za utvrđivanje, primjenu i pregled sigurnosne i odbrambene politike;
- Parlament ima jedinstvenu ustavnu ulogu u smislu odobrenja i revizije troškova odbrane i sigurnosti;
- Parlament ima osnovnu ulogu u smislu proglašenja i ukidanja vanrednog stanja ili ratnog stanja;
- Principi dobre uprave i vladavina prava se odnose na sve grane vlasti, te time i na sigurnosni sektor;

- Osoblje sigurnosnog sektora ima pojedinačnu odgovornost pred sudovima za kršenje domaćih i međunarodnih zakona (u vezi sa nesavjesnim postupanjem koje se sankcionira u građanskopravnim ili krivičnopravnim postupcima);
- Organizacije sigurnosnog sektora su politički neutralne.[38]

6.3.1. Ujedinjeni narodi

Kako je već u prethodnom dijelu rada objašnjeno Ujedinjeni narodi (UN) predstavlja najveću svjetsku međunarodnu organizaciju, a čije su članovi suverene države. Zadatak Ujedinjenih naroda jeste prvenstveno da očuvaju i osiguraju mir, kvalitetne međunarodne odnose i suradnju, međunarodnu saradnju na svim poljima između različitih država. Kako je Evropa, ali i ostatak svijeta doživio ogromne probleme i sukobe koji su donijeli velike štete za cijelo društvo, formirane su organizacije za rješavanje sporova mirnim putem, diplomacijom i razgovorom. Jedna od tih međunarodnih organizacija jesu i Ujedinjeni narodi. U cilju sprječavanja historije svjetskih ratova te osnivanja Ujedinjenih naroda kao organizacije čiji je temeljni cilj uspostava i održanje mira. Dolazi do formiranja sustava kolektivne sigurnosti kao „institucionaliziranog sistema, postupka ili mehanizma osiguranja mira u kojem su se države članice Ujedinjenih naroda sporazumjele da se zajednički postave naspram svakog čina agresije ili drugog zabranjenog oblika upotrebe sile prema jednoj od država članica.

Osnovna načela koja imaju Ujedinjeni narodi (UN) i kojih se pridržavaju i poštuju su:

- Organizacija se temelji na načelu suverene jednakosti svih svojih članova;
- Da bi se svim članovima osigurala prava i blagodati koje proistječu iz članstva, članovi moraju u dobroj vjeri ispunjavati obveze koje su preuzeli u skladu s ovom Poveljom;
- Članovi rješavaju svoje međunarodne sporove mirnim sredstvima na takav način da ne ugroze međunarodni mir i sigurnost, te pravdu;
- Članovi se u svojim međunarodnim odnosima suzdržavaju od prijetnje silom ili upotrebe sile koje su uperene protiv teritorijalne cjelovitosti ili političke nezavisnosti bilo koje države, ili su na bilo koji način nespojive s ciljevima Ujedinjenih naroda;
- Članovi daju Organizaciji punu pomoć u svakoj akciji koju ona poduzima u skladu s ovom Poveljom i suzdržavaju se od pomaganja države protiv koje Ujedinjeni narodi poduzimaju preventivnu ili prisilnu akciju;

[38] Fluri, P., Johnsson, A. Parlamentarni nadzor nad sektorom sigurnosti: principi, mehanizmi i prakse. Interparlamentarna unija Centar za demokratsku kontrolu nad oru`anim snagama Verzija izdata u Sarajevu: Misija OSCE-a u Bosni i Hercegovini. 2003. str. 184.-187.

- Organizacija osigurava da države koje nisu članice Ujedinjenih naroda postupaju u skladu s ovim načelima koliko je to potrebno za održavanje međunarodnog mira i sigurnosti;
- Ništa u ovoj Povelji ne ovlašćuje Ujedinjene narode da se miješaju u poslove koji po svojoj biti spadaju u unutrašnju nadležnost države, niti ne obvezuje članove da takve poslove podnose na rješavanje prema ovoj Povelji.[39]

6.3.2. NATO

Sjeveroantlanski savez ili organizacija sjeveroatlanskog ugovora (NATO) kao što je prethodno objašnjeno predstavlja međunarodnu organizaciju koja za cilj ima odbrana svojih članica od potencijalnih vojnih napada. Primarni cilj je održati i osigurati mir, sigurnost i suverenitet svake države članice.

Kako bi NATO ostvario svoje primarne ciljeve, ima svoje zadatke koje se odnose na sigurnost država članica, a to su:

- Osigurava nezamjenjiv temelj stabilnosti i sigurnosti u Europi s naglaskom na razvoj demokratskih institucija i mirnog rješavanja nesuglasica. Teži stvaranju okružja u kojem nijedna država neće moći ugroziti nijednu evropsku naciju niti joj nametnuti hegemoniju prijetnjama ili upotrebom sile;
- U skladu s člankom 4. Sjeverno-atlantskog sporazuma, služi kao preko atlantski forum za razmatranje bilo kojih pitanja koja su od ključne važnosti državama članicama, što uključuje i situacije čiji bi razvoj mogao ugroziti njihovu sigurnost. Omogućava zajedničko usmjeravanje napora na poljima koja su od zajedničkog interesa;
- Brani države članice od bilo kojeg oblika agresije na njihov teritorij, te ga pokušava spriječiti;
- Promiče sigurnost i stabilnost održavajući trajnu suradnju sa svim partnerima kroz Partnerstvo za mir, Evroatlantsko partnersko vijeće, te savjetovanje, suradnju i partnerstvo s Rusijom i Ukrajinom;
- Pridonosi razumijevanju čimbenika ključnih za međunarodnu sigurnost i ciljeva suradnje na tom području, putem programa informiranja u zemljama članicama NATO-a i zemljama partnerima te putem inicijativa kao što je Mediteranski dijalog.[40]

[39] Šalić, B .Ujedinjeni narodi. Šibenik: Veleučilište u Šibeniku, Upravni studij., Završni rad 2016. str. 53.
[40] Čukljaš, M. (2015.) .Organizacija sjevernoatlanskog ugovora NATO. Šibenik: Veleučilište u Šibeniku, Upravni studij, Završni rad 2015. str. 28.

6.3.3. OSCE

Organizacija za Evropsku sigurnost i suradnju (OSCE ili OESS) predstavlja panaevropsku sigurnosnu organizaciju u čijem su sastavu zemlje članice iz Evrope, Azije i Sjeverne Amerike. Ono što je primarni zadatak ove organizacije jeste da rano upozore i sprečavaju sukobe, kontrolišu eventualne sukobe i upravljaju tim kriznim situacijama, te pomažu u oporavku nakon sukoba koji su se desili. Veliki je spektar zanimanja i dijelovanja ove organizacije, pa u to možemo navesti upravljanje granicama, kontrolu oružja, borbu protiv terorizma, ilegalnom trgovinom (ljudima, drogom), ljudskim pravima itd. OSCE djeluje na tri glavna segmenta: vojno-politički, ekonomsko-ekološki i ljudski. Radi kvalitetnije i bolje suradnje članica ove međunarodne organizacije na polju sigurnosti usvojile su Kodeks ponašanja u vojnopolitičkim aspektima sigurnosti. Principe Kodeksa je teško nabrojati jer ih ima 42 pa ćemo objasniti samo nekoliko njih:

- Države članice naglašavaju da je puno poštivanje svih načela Konferencije za sigurnost i suradnju u Evropi, koji su uključeni u Helsinškom završnom aktu, te provedba, u dobroj vjeri, svih obaveza preuzetih u sklopu Konferencije za sigurnost i suradnju u Evropi, od temeljne važnosti za stabilnost i sigurnost, te, shodno tome, sačinjava predmet direktne i zakonske brige za svaku od njih;
- Države članice potvrđuju da su sva načela Helsinškog završnog akta od prvenstvene važnosti, i prema tome će ona biti jednako i bezrezervno primjenjiva, a svako od njih bit će tumačeno u kontekstu s drugima;
- Države članice imaju suvereno pravo biti, odnosno ne biti, članice međunarodnih organizacija, kao i biti, odnosno ne biti, strana u bilateralnim ili multilateralnim ugovorima, uključujući ugovore o savezima; one isto tako imaju pravo promijeniti svoj status u ovom pogledu, što podliježe relevantnim sporazumima i procedurama. Svaka država članica poštivat će prava svih ostalih u ovom pogledu;
- Svaka država članica uzdržavat će samo onoliko vojnih kapaciteta koji su u srazmjeru s njihovim individualnim ili kolektivnim legitimnim potrebama sigurnosti, uzevši u obzir svoje obaveze u skladu s međunarodnim pravom;
- Država članica može postaviti svoje oružane snage na teritorij druge države članice u skladu s njihovim međusobno, slobodnom voljom dogovorenim spora zumom, kao i u skladu s međunarodnim pravom.[41]

[41] OSCE Misija u Bosni i Hercegovini, Odjel za sigurnosnu saradnju. Sarajevo, 2007. godine

Kao što smo i rekli imamo oko 42 principa odnosno pravila u ovom Kodeksu koji jasno i koncizno objašnjava mogućnosti i djelovanje članica u samoj organizaciji ali i njihovoj individualnoj ulozi.

6.3.4. EU

Evropska unija (EU) je skup demokratkih zemalja okupljenih sa ciljem zajedničkog razvoja mira, prosperiteta i napretka. Članice EU su formirale zajedničke institucije po pitanju određenih interesa te su u tom dijelu podredile dio svog suvereniteta, a sve kako bi se donijele kvalitetne odluke na Evropskoj razini. Ugovorom o Evropskoj uniji koji je potpisan od članica odnosi se na tri glavna segmenta djelovanja i saradnje i to: prvi obuhvata tri zajednice – Evropska zajednica za ugalj i čelik, Evropska ekonomska zajednica i Evropska zajednica za atomsku energiju.[42]

Drugi obuhvata zajednička vanjska i sigurnosna politika dok je treći skup saradnja u pravosuđu i unutarnjim poslovima. U okviru Mehanizma za civilnu zaštitu Evropska unija i nekoliko drugih evropskih zemalja imaju važnu ulogu u koordinaciji odgovora na krizne situacije u Evropi i svijetu. Postojeće i potencijalne krizne situacije neprestano se prate, a zemlje sudionice surađuju i u procjeni rizika, sprečavanju katastrofa, pripravnosti i planiranju. Hitna pomoć pruža se u fizičkom obliku, poput hrane, smještaja ili opreme, raspoređivanjem posebno opremljenih timova ili slanjem stručnjaka na teren radi procjene i koordinacije. Timovi, stručnjaci i oprema zemalja sudionica drže se u pripravnosti za pružanje brze pomoći EU-a diljem svijeta. [43]

Evropska unija je u 2016. godini donijela globalnu strategiju na vanjsku i sigurnosnu politiku, u cilju bolje sigurnosti, povećala stabilnost cijele regije oko Evropske unije, odbrane, i riješila određena pitanja energetske sigurnosti, migracija koje su nezakonite, terorizma. Ovom strategijom postavljeno je pet osnovnih principa za područje EU:

- Sigurnost Evropske unije;
- Otpornost država i unija;
- Integriran pristup sukobima i krizama;
- Zajednički regionalni poreci;

---

http://www.mfa.gov.ba/HTML/Bos/Multilaterala/OSCE-Kodeks-Ponasanja.pdf Pristup: 28.04.2020.

[42] Oficijalna stranica Evropske unije www.europa.eu Pristup: 25.05.2020.

[43] Oficijalna stranica Evropske unije https://europa.eu/european-union/topics/humanitarian-aid-civil-protection_hr Pristup: 30.04.2020.

- Globalno upravljanje za 21. vijek. [44]

6.3.5. Vijeće sigurnosti

Vijeće sigurnosti predstavlja jedno od glavnih tijela Ujedinjenih naroda (UN) i primarni zadatak ovog vijeća jeste održavanje međunarodnog mira i sigurnosti. Vijeće sigurnosti ima 15 članica od kojih je pet stalnih to su: Kina, Rusija, SAD, Francuska i Ujedinjeno Kraljevstvo te pored toga deset članica koje nisu stalne biraju se na period od dvije godine. Kao što smo i naveli cilj ovog vijeća jeste održavanje međunarodnog mira i sigurnosti, kako članica tako i cijele regije i svijeta. Međutim kada se pojavi eventualna prijetnja međunarodnom miru, vijeće prvo traži mogućnost mirnog djelovanja i rješavanje eventualnog sukoba diplomacijom i razgovorima. Predlaže prijedloge i principe kako bi se riješila kriza i osigurao mir. Ukoliko je došlo do oružanog sukoba primarni zadatak vijeća jeste da se zaustavi vatra. Vijeće ima mogućnost da šalje svoje vojnike u mirovnu misiju kako bi držao razdvojene zavađene strane ili zabraniti uvoz oružja, na kraju može jednostavno silom nametnuti svoje odluke. [45]

Funkcije i ovlasti Vijeća sigurnosti se nalaze u članu 24. Povelje:

- Da bi se osigurala brza i djelotvorna akcija Ujedinjenih naroda, njihovi članovi povjeravaju Vijeću sigurnosti prvenstvenu odgovornost za održavanje međunarodnog mira i sigurnosti, i pristaju da Vijeće sigurnosti radi u njihovo ime kad obavlja svoje dužnosti na temelju te odgovornosti.

- U obavljanju tih dužnosti Vijeće sigurnosti djeluje u skladu s ciljevima i načelima Ujedinjenih naroda. Posebne ovlasti koje su Vijeću sigurnosti date za obavljanje tih dužnosti izložene su u glavama VI., VII., VIII. i XII.

- Vijeće sigurnosti podnosi Općoj skupštini na razmatranje godišnje, a po potrebi i posebne izvještaje. [46]

6.4. Parlamentarni nadzor nad sistemom nacionalne sigurnosti

Svaki sukob ne predstavlja prijetnju određenoj državi ili nacionalnoj sigurnosti i mir. Danas u savremenom životnom okruženju mnogo je više sukoba na nivou država zbog stavova pojedinih državnih službenika koji imaju međusobno različite stavove po pitanju određenih

[44]Oficijalna stranica Evropske unije, Ured za publikacije https://op.europa.eu/webpub/com/eu-what-it-is/hr/#chapter2_17 Pristup: 30.04.2020.
[45]Oficijalna stranica Evropske unije www.op.europa.eu Pristup: 22.05.2020.
[46]Oficijalna stranica Ujedinjenih naroda https://hr.wikisource.org/wiki/Povelja_Ujedinjenih_naroda Pristup: 22.05.2020.

segmenata. Nacionalna sigurnost odnosno zaštita države je jedna od osnovnih stvari koje svaki građanin želi, a to u suštini znači u prvom redu zaštita i sigurnost građana i zajednice. Državna sigurnost se sve manje može ostvariti samo na osnovu same države, sve veća je potreba i ideja za udruživanje i međusobnu pomoć između različitih država. Tako da danas imamo veliki broj međunarodnih organizacija upravo za uspostavljanje sigurnosti i mira kao što su NATO, UN, OSCE itd. Države se sve češće udružuju i u drugim poljima kao što su ekonomski, obrazovni, privredni ili bilo koji drugi sektor i segmenat primjer Evropska unija.

Kada govorimo o parlamentarnom nadzoru za sigurnost države, po mnogima je to jedini i pravi način, jer Parlament jedne države je izabran od građana i ima svu vrhovnu vlast pod kontorolom. Sigurnost i mir jedne države je izuzetno važna te zbog toga je važna i vlast koja može da kontroliše i donosi odluke najbolje za samu državu. Pored toga izvršna vlast mora kontrolisati cjelokupnu sigurnost jer je cijeli segment sigurnosti na budžetu i važno je da parlament kontroliše i nadzire korištenje javnih sredstava iz budžeta koji bi se trebali koristiti na kvalitetan i transparentan način. Parlament kao izvršna vlast u praksi ima mogućnost utvrđivati zakone koji se direktno tiču sigurnosti. Osim toga mogu da kontrolišu da li se određeni zakoni koji su donešeni direktno primjenjuju ili ne.

Državna sigurnosna politika utvrđuje vladin pristup sigurnosti i kako se očekuje postizanje takve sigurnosti. Državna sigurnosna politika obuhvata osnovne odluke u vezi sa sigurnosnim sektorom koje utječu na vanjsku i unutarnju sigurnost države i društva. Temelji se na datom pristupu sigurnosti, daje smjernice za vojnu doktrinu i utvrđuje se unutar okvira međunarodnih i regionalnih regulativa kojima je država pristupila. Stoga, ona se ne temelji samo na percepciji potreba i prioriteta državne sigurnosti, nego na nju utječu razni vanjski faktori, pritisci i obaveze. U svim slučajevima ona treba ispuniti vrijednosti i principe koji su zajamčeni državnim ustavom ili poveljom.[47]

Parlament čine pojedinci koji su izabrani demokratskim putem od strane građana i oni su u službi i interesu građana. Ima nekoliko razloga zbog kojih je potrebno da parlament djeluju u utvrđivanju sigurnosne politike te odobrenje od strane parlamenta na transparentan način a to su:

- Državna sigurnosna politika utječe na život, vrijednosti i dobrobit ljudi i ne bi trebala biti prepuštena prosudbi izvršnih organa i same vojske;

[47] Fluri, P., Johnsson, A. Parlamentarni nadzor nad sektorom sigurnosti: principi, mehanizmi i prakse. Interparlamentarna unija Centar za demokratsku kontrolu nad oru`anim snagama Verzija izdata u Sarajevu: Misija OSCE-a u Bosni i Hercegovini. 2003.

- Državna sigurnosna politika ostavlja velike posljedice po budućnost vojske, njenih pripadnika, i muškaraca i žena;
- Državna sigurnosna politika ima velike finansijske posljedice i tiče se novca poreskih obveznika;
- Osim finansijskih izdataka, sigurnosne mjere mogu ograničiti slobodu i prava građana i utječu na demokraciju;
- Stoga je bitno da parlament osigura da su takve mjere u svako doba konzistentne sa postojećim međunarodnim humanitarnim pravom, posebno sa četiri Ženevske konvencije i dva Protokola i sa instrumentima kojima se garantiraju ljudska prava, posebno sa Univerzalnom deklaracijom o ljudskim pravima i Međunarodnom poveljom o građanskim i političkim pravima. U Povelji se kaže da određena prava ni pod kojim okolnostima ne mogu biti ograničena.[48]

6.5. Uloga demokratskog društva u ratovanju

Demokratija predstavlja oblik vlasti gdje većina građana određene države biraju svoje predstavnike koji zastupaju njihove interese. Demokratija je sve ono što se u ljudskoj zajednici oduvijek željelo a to je jednakost, sloboda, sigurnost, pravo na mišljenje. Sve to imamo u demokratiji koja nam to omogućuje i pruža. Danas je prisutno mnogo društava i država gdje preovladava ovaj oblik vlasti, ali sve više građani postaju nezadovoljni djelovanjem vlasti koju biraju. Pa je sve češće pojava demokratije samo kao idealnog oblika vlasti u teoretskom smislu dok je u praksi daleko od idealnog. Demokratija se odnosi i na izbor svih predstavnika i u međunarodnim organizacijama, ljudima koji zasjedaju i predstavljaju određenu državu i naciju. Ono što je jedna od ključni stavki demokratije jeste mogućnost izbora te na određeni način sigurnost, što je veoma važno za život zajednice. Ono što je danas jasno jeste da demokratija ne garantira sigurnost i mir te je veliki broj ratova koji su nastali u bliskoj prošlosti upravo dolaskom demokratije i demokratskog društva. Jedan od glavnih zastupnika demokratskog društva i slobode izbora jesu Sjedinjene Američke Države (SAD). Kroz bližu historiju se možemo uvjeriti kako je upravo ova država imala dio svog uticaja na uspostavljanje demokratskog društva i nastanak rata sa oogromnim društvenim nemirima i siromaštvom. To možemo vidjeti na primjeru "Bliskog Istoka" i država poput Iraka, Libije, Afganistana itd.

[48] Fluri, P., Johnsson, A. Parlamentarni nadzor nad sektorom sigurnosti: principi, mehanizmi i prakse. Interparlamentarna unija Centar za demokratsku kontrolu nad oru`anim snagama Verzija izdata u Sarajevu: Misija OSCE-a u Bosni i Hercegovini, 2003.

Kao najbolji primjer možemo prikazati Irak, zemlju koja je imala enormna prirodna bogatstva prvenstveno se to odnosi na naftu. Država je bila uređena da je jedan čovjek bio na čelu kao diktator. SAD je imala više ciljeva pokretanjem rata u Iraku, prvi je bio da se sama država razoruža od oružja prvenstveno nuklearnog, ali samo razoružavanje Iraka. Drugi cilj je bio borba protiv terorizma, kasnije uspostavljanje demokratije, slobode i slobodno tržište. Kada je riječ o terorizmu, tadašnjem vodstvu države Irak na određeni način nije odgovarao bilo koji režim koji je imao doticaj sa terorizmom te su sve mogućnosti bile daleko od Iraka što je drugi od ciljeva koji nisu imali temelj nastanka rata u Iraku. Kada govorimo o uspostavljanju demokratije i slobode glavni cilj je bio svrgnuti sa vlasti Sadama Huseina koji se smatrao diktatorom. Na taj način SAD su napravile veliki problem, dolazi do podjele društva na Šite, Sunite, Kurde itd. Na vrhuncu, u Iraku je otpočeo građanski rat. Uvođenjem slobodnog tržištva ekonomija ove države je postala puna korupcije i malverzacija te je bila daleko od one koju je naslijedila. Ovo je samo jedan primjer uloge demokratskog društva u ratovanju, za primjer također možemo uzeti i sukob devedesetih godina na prostoru Balkana.

6.6. Izazovi demokracije u ratovanju

Danas društvo teži demokratskom načinu života i vladanja. Većina država svijeta imaju demokratski način vlasti koja se bira na osnovu volje većine, koja bira svoje predstavnike koji ih zastupaju u vlasti. Sve je manje drugih oblika vladavine, kao što je komunizam (npr. Kina) ili diktatura (npr. Sjeverna Koreja). I pored demokratske vlasti i dalje velike sile i države imaju svoje interese, te zbog njih koriste svoju moć kako bi ostvarili željene ciljeve. Isto tako kada su određeni resursi u pitanju, posebno se to odnosi na bliski istok sa velikim izvorima nafte, koje su u budućnosti od velikog značaja ili određenog prostora koji je važan sve se radi kako bi kroz demokraciju ostvarili svoje ciljeve.

Zbog toga danas demokratsko društvo pruža sigurnost, slobodu, mogućnost izbora i glasa. Ljudima sve manje odgovara sama vlast koju izaberu i njihov rad. Svakodnevno smo svjedoci ratova na raznim frontovima bilo da je se radi za određenu teritoriju, prirodno bogatsvo ili bilo koji drugi razlog. Uprkos demokratiji međunarodna zajednica i njene članice imaju zadnju riječ i oni su ti koji kontroliraju i određuju cjelokupnu situaciju. Pitanje demokratije istodobno i pitanje međunarodne zajednice i njenog udjela u izgrađivanju odnosa među narodima i državama. Dakle, demokratija je univerzalna vrijednost, a njeno stanje i problemi razvitka su problemi od međunarodnog značenja. [49]

[49] Hadžić Izet Demokratija, ljudska prava i slobode kao osnovne vrijednosti političkog sistema. Stručni rad ISSN 1512-5785 broj 35. 2015. str. 83.

Vodeće zapadne nacije već neko vrijeme djeluju na način da je demokratija rješenje političkih sukoba i kako je krajnji cilj vanjske politike treba da bude poticanje demokratije u državama u kojima ona još ne postoji. I dalje se drže te pretpostavke bez obzira na sukobe i razaranja koja se događaju iz tih razloga na Bliskom istoku. Jasno da to žele iz razloga što u pravilu demokratske države međusobno ne ratuju, a niti se unutar njihovih granica dešavaju građanski ratovi jer kad narod u demokratiji bira svoje predstavnike postoji mogućnost da se problem riješi bez velikih sukoba i problema, te nepopularnu vlast smjene bez nasilja. Zbog toga je demokratija veoma važna za Zapadnu politiku. Na taj način su demokratija i rat povezani. Demokratija na Bliskom istoku, sa druge strane doprinese velikim sukobima i razaranjima koja traju dugi niz godina. Te države poslije imaju velike ekonomske probleme, žrtve tih sukoba su siromašne kao i sama država, ostaju bez prirodnih resursa na osvnovu kojih su egzistiraliitd.

6.7. Demokratski nadzor i kontrola nad cyber ratovanjem

Virtuelni prostor koji ne postoji ni u kom fizičkom obliku, koji je mnogo složen i rasprostranjen, i to sve kao produkt razvoja i mogućnosti interneta i novih tehnologija, tako još možemo opisati cyber prostor. U tom prostoru se u savremenom svijetu sve više vrše, po ljude i planetu, loše stvari. Često smo svjedoci raznih hakerskih napada na određene državne službe i agencije, hakerske napade na nuklearna postrojenja, rat između država putem cyber prostora. Sve to je jako teško pratiti i staviti pod kontrolu, zbog toga sve velike sile pokušavaju da zaštite prostor kojim oni djeluju. Kada govorimo o cyber prostoru mnogima je to još uvijek velika nepoznanica i još uvijek je ta oblast jako mlada, ali ona enormnim koracima napreduje i pitanje je da li će se ikada moći zaštititi i izučiti taj prostor. Države kao cjeline koje su zadužene za osiguravanje mira i sigurnosti svojih građana moraju putem svoje vlasti da osiguraju nadzor i kontrolu nad tim prostorom kako bi zaštitili svoj integritet, sigurnost i mir.

Globalna kultura cyber sigurnosti zahtijeva da svi sudionici adresiraju sljedećih devet komplementarnih elementa:

1. *Svijest* - Sudionici bi trebali biti svjesni potrebe za sigurnošću informacijskih sistema i mreža i šta oni mogu učiniti kako bi se poboljšala sigurnost;
2. *Odgovornost* - Sudionici su odgovorni za sigurnost informacijskih sistema i mreža na način koji odgovara njihovim individualnim ulogama. Oni bi trebali redovito razmatrati svoje politike, prakse, mjere i postupke, te procijeniti jesu li oni prikladni za njihova okruženja;

3. *Odgovor* - Sudionici bi trebali djelovati pravovremeno i na kooperativan način kako bi spriječili, otkrili i reagirali na sigurnosne incidente. Oni bi trebali, po potrebi, dijeliti informacije o prijetnjama i ranjivostima, te implementirati procedure za brzu i učinkovitu suradnju kako bi se spriječilo, prepoznalo i reagiralo na sigurnosne incidente. To može podrazumijevati prekograničnu razmjenu informacija i suradnju;
4. *Etika* - S obzirom na sveprisutnost informacijskih sistema i mreža u modernim društvima, sudionici moraju poštivati legitimne interese drugih ljudi, prepoznajući da njihovo djelovanje ili nedjelovanje može naškoditi drugima;
5. *Demokracija* - Sigurnost treba provoditi u skladu s vrijednostima priznatim u demokratskim društvima, uključujući slobodu razmjene misli i ideja, slobodan protok informacija, povjerljivost informacija i komunikacija, odgovarajuću zaštitu osobnih podataka, otvorenost i transparentnost;
6. *Procjena rizika* - Svi sudionici trebaju provoditi periodične procjene rizika kojima se identifciraju prijetnje i ranjivosti. Procjene rizika trebaju biti dovoljno široko usmjerene kako bi obuhvatile ključne unutarnje i vanjske faktore, kao što su tehnologije, fzički i ljudski faktori, politike i treća strana pružanja usluga. Procjene rizika trebaju omogućiti određivanje prihvatljive razine rizika, te pomoći u odabiru odgovarajućih kontrola za upravljanje rizikom od potencijalne štete informacijskim sistemima i mrežama u svjetlu prirode i važnosti informacija koje trebaju biti zaštićene;
7. *Sigurnosni dizajn i provedba* - Sudionici trebaju inkorporirati sigurnost kao neophodan element prilikom planiranja i dizajniranja, upravljanja i korištenja informacijskih sistema i mreža;
8. *Upravljanje sigurnošću* - Sudionici trebaju usvojiti sveobuhvatan pristup upravljanju sigurnošću temeljem procjene rizika koja je dinamična, te koja obuhvaća sve razine aktivnosti sudionika i sve aspekte njihovog poslovanja;
9. *Ponovna procjena* - Sudionici bi trebali redovito pregledati i ponovno procjenjivati sigurnost informacijskih sistema i mreža, te poduzeti odgovarajuće izmjene u sigurnosnim politikama, praksama, mjerama i postupcima koji uključuju adresiranje novih i promjenu postojećih prijetnji i ranjivosti. [50]

Sigurnost u cyber prostoru i njena kontrola predstavlja novi problem za sve države i vlasti. Još uvijek je mnogo stvari koje nisu poznate u tom dijelu i jako teško i sporo, vlade i državne

[50] UN General Assembly "A/RES/57/239, Creation of a global culture of cybersecurity", 2003.

službe rješavaju te probleme. Niz je problema koji utiču na demokratski nadzor cyber sigurnosti:

- Prvo, problemi nadzora pogoršani su zbog kompleksnosti mreže. U cyber sigurnost uključen je veliki i raznovrsni broj državnih, privatnih, međunarodnih i drugih nedržavnih aktera. Slično tome, veoma raznoliki akteri participiraju i u onom što bi se u širem smislu moglo nazvati kao cyber napad. Kompleksnost mreže nadzornim tijelima, kao što su parlamentarni odbori (često s ograničenim ovlaštenjima), otežava da prate relevantne aktere, stječu saznanja o njihovom posto-janju i aktivnostima ili čak i pravni mandat da to čine;
- Drugo, probleme nadzora pogoršava tehnička kompleksnost. Zbog izrazito tehničke prirode izazova cyber sigurnosti i odgovora na nju nadzorna tijela često nemaju neophodnu stručnost da ih razumiju i adekvatno nadziru. Javno-privatna suradnja dodatno pogoršava problem stvarajući razdor između visoko plaćenih i sofisticiranih tehničkih eksperata koji su uključeni u provođenje direktive i (često) slabo plaćenih i slabije informiranih državnih aktera koji su zaduženi za njihov nadzor;
- Treće, probleme nadzora pogoršava pravna kompleksnost. Cyber sigurnost nas suočava s kompleksnim pravnim pitanjima koja se odnose (između ostalog) na pravo privatnosti i slobodu izražavanja. Ova kompleksnost se dalje uvećava kroz javno-privatnu suradnju i povezana pravna pitanja u pogledu odgovornosti i kontrole. Dodatan razlog za zabrinutost predstavlja i činjenica da postoji suštinska tenzija između zaštite privatnosti i poboljšane identifikacije i provjere identiteta korisnika. Činjenica je da države i firme često bez adekvatnog demokratskog nadzora skupljaju i obrađuju veliku količinu ličnih i privatnih podataka radi vlastite sigurnosti (kao i sigurnosti svojih klijenata);
- Četvrto, probleme nadzora pogoršava heterogenost aktera. U većini slučajeva institucije nadzora su organizirane kao agencije ili funkcionalno slična tijela. Naprimjer, parlamentarni odbor može da nadgleda obavještajne službe i aktivnosti, oružane snage i pravosuđe. Međutim, javno-privatna suradnja koju podrazumijeva cyber sigurnost seže preko agencijskih ovlaštenja pa i izvan njihovog mandata. To rezultira velikim brojem područja u kojima nadzora ili nema ili je on neadekvatan.
- Peto, probleme nadzora pogoršavaju percepcije mandata. Generalno, državna nadzorna tijela se staraju o državnim agencijama za čiji rad su direktno odgovorna.

Ovo ostavlja privatne partnere takvih agencija izvan dometa nadzora, čak i u slučajevima kada ih takve agencije direktno finansiraju ili s njima blisko surađuju;

- Šesto, problem nadzora pogoršava narušavanje odnosa principal-agent. Postupci svakog državnog agenta povezani su lancem odgovornosti od principala ka agentu. Tako postoji lanac odgovornosti i nadzora između demokratskih institucija (poput parlamenta) i pojedinaca ili agencija koje provode državne direktive. Ove veze prekinute su uvođenjem privatnih aktera i stvaranjem javno-privatnih mehanizama suradnje. Iako se javna IT preduzeća naizgled ponašaju kao puki agenti države, taj odnos je generalno mnogo složeniji i zamagljeniji zbog mnogobrojnih asimetričnih informacija koje smanjuju transparentnost i sprečavaju efikasno djelovanje nadzornih mehanizama.[51]

6.7.1. Unutrašnji akteri demokratskog nadzora i kontrole

Svaka državna vlast ima zadatak osigurati sigurnost i mir svojih građana koji žive u toj državi. To postiže djelovanjem državnih agencija kao što su policija, vojska, razna ministarstva, agencije itd. Kao što smo već naglasili cyber prostor je izuzetno veliki, prostor koji nije proučen i koji se svakodnevno razvija zahvaljujući razvoju interneta i novih tehnologija. Zbog toga države putem svoje vlasti prave nacionalne planove putem kojih će u periodu od par godina da se posebno fokusiraju na to područje. Imamo primjer susjedne Hrvatske kako putem unutrašnjih aktera nadzire i kontroliše ovaj prostor. Oni kroz taj plan definiraju područja koja koriste ili će koristiti cyber prostor, a koja će dodatno educirati i pripremiti za korištenje. Isto tako utvrdili su zakone i prava osoba koja se ne mogu i ne smiju narušiti tokom korištenja cyber prostora i njegovih dijelova. Svi društveni dijelovi koji u svom poslovanju i djelovanju koriste cyber prostor međusobno su povezani, dok sve zajedno MUP Republike Hrvatske kontroliše i nadzire. Osnovni ciljevi ove strategije koje ima država Hrvatska su:

- "sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira",
- "provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti cyber prostora",
- "uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima",
- "jačanje svijesti o sigurnosti cyber prostora",
- "poticanje razvoja usklađenih obrazovnih programa",

[51] Hamidović, H.Mjesto i uloga cayber sigurnosti u razvoju modernih društava. Sarajevo: Sarajevski žurnal za društvena pitanja, Vol. 4. Broj 1-2. 2015.

- "poticanje razvoja e-usluga",
- "poticanje istraživanja i razvoja rada akademskog, gospodarskog i javnog sektora",
- "sustavni pristup međunarodnoj suradnji". [52]

Glavno tijelo za informacijsku sigurnost je Ured vijeća za nacionalnu sigurnost u RH, pored tog tijela ima i Zavod za sigurnost informacijskih sustava. Njihov primarni zadatak jeste zaštita i kontrola cyber prostora koji se direktno tiče ove države. Na kraju tu je i policija odnosno školovanje kadrova koji će moći u budućnosti da kvalitetno odgovore zadatku i zaštite ovo područje. Kroz ovaj primjer možemo vidjeti djelovanje unutrašnjih snaga za kontrolu i sigurnost cyber prostora. Sve države se moraju usmjeriti zaštiti i kontroli ovog prostora jer se danas gotovo sve vrši „online“ i zbog toga svi trebaju da naprave određene korake kako bi se što kvalitetnije i sigurnije moglo koristiti.

6.7.2. Vanjski akteri demokratskog nadzora i kontrole

Vanjski akteri su agencije i organizacije koje su „van“ države odnosi se na međunarodni nivo. Mnoge razvijene države puno brže i više napreduju u istraživanju ovog prostora i samim tim putem saradnje sa njima druge države mogu da koriste njihova znanja i spoznaje. Ujedinjeni narodi (UN), Interpol, Europol, Europski centar za cyber kriminal - EC3, ENISA - agencija Europske unije za mrežnu i informacijsku sigurnost, CEPOL - "Agencija Europske unije za osposobljavanje u području izvršavanja zakonodavstva" samo su od nekih organizacija i agencija koje pomažu državama u otkrivanju, istraživanju, praćenju i kontroli cyber prostora.

Primjer agencija Evropske unije za mrežnu i informacijsku sigurnost (ENISA), pomaže državama EU da se bolje opreme i pripreme za sprječavanje, otkrivanje i odgovor na probleme informacijske sigurnosti. To uključuje organizaciju vježbi za slučajeve cyber krize u cijeloj Evropi, pomoć u razvoju nacionalnih strategija informatičke sigurnosti, promicanje suradnje među timovima za hitne računalne intervencije i izgradnju kapaciteta. [53]

6.8. Uticaj privatnih kompanija na demokratski nadzor i kontrolu

Velike privatne kompanije svih zemalja su uvijek jako blizu vladajućim strukturama odnosno vlasti. Vlasnici tih kompanija su u velikoj mjeri veoma važni ljudi koji djeluju na politiku i vlast na određeni način iz „sjene“. Većina velikih privatnih kompanija imaju enorman broj zaposlenih, velike prihode i velike poreze koje plaćaju državi. Pored toga svi zaposleni i njihove porodice na neki način su zbrinuti radom u tim kopmanijama te se za njih država ne

[52] Protrka, N. .Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru. Doktorski rad, Zadar: Sveučilište u Zadru, 2018.
[53] ENISA - European Network and Information Security Agency https://europa.eu/european-union/about-eu/agencies/enisa_hr Pristup: 28.09.2020.

mora zanimati na određeni način. Zbog toga vlasnici tih kompanija imaju određeni pristup političkoj sceni i odlukama koje donose ili treba da donesu državne službe. Naravno putem svoje moći na određeni način djeluju na pojedine odluke ukoliko oni ili njihova kompanija može imati neku korist ili povlasticu. To je svakako jedan problem u današnjoj demokratiji ali je jako prisutan, u velikoj mjeri kod malih zemalja i zemalja u tranziciji. Kompanije koje svojim radom i funkcionisanjem interesuju državu svakako bivaju u nešto komfornijoj situaciji u odnosu na druge kompanije. Možemo vidjeti primjer tih kompanija svugdje u svijetu: Bingo, Hifa - Bosna i Hercegovina, Ina, Agrokor – RH, Apple – SAD.

Velike kompanije imaju posebnu ulogu u ekonomskom i političkom životu. Analizirajući njihovu ulogu i unutarnju strukturu, gigantske kompanije i "javna ili socijalna poduzeća", sa širokim socijalnim posljedicama, ali i "politički sustavi", jer ostvaruju vlast nad mnogim osobama. No, iako "bitno javne ili socijalne, ne privatne organizacije", sustav upravljanja u njima jest ili prosvijećeno skrbništvo ili čak grubi despotizam, što se opravdava njihovim navodnim privatnim karakterom. Slijedi da je demokratizacija kompanija uvjet ne samo većeg stupnja organizacijskog pluralizma u društvu već i potpunije političke jednakosti građana. Pretvaranje velikih kompanija u socijalne i političke sustave povezano je s promjenom odnosa vlasništva i kontrole u korporacijskom kapitalizmu. Dok je u prošlosti vlasništvo značilo kontrolu, u korporacijskom kapitalizmu taj je odnos promijenjen, jer velike kompanije kontroliraju menedžeri, a ne njihovi vlasnici (dioničari). Menedžeri imaju, dok vlasnici nemaju moć, a moć je jedino bitna. Promjena odnosa moći između vlasnika i menedžera zaoštrava problem tko i na koji način treba upravljati velikim kompanijama. Ako su velike kompanije po svojoj naravi i utjecaju socijalna i politička poduzeća, a moć vlasnika (dioničara) nad kompanijom toliko mala u usporedbi s menedžerima, te kompanije treba shvatiti kao javne, a ne kao privatne entitete. Budući da ih ne kontroliraju vlasnici, pitanje kontrole nad velikim korporacijama teorijski prethodi pitanju vlasništva. [54]

6.9. Uticaj medija

Jedan od ključnih elemenata interakcije i učinkovitog funkcioniranja svake biološke skupine je sposobnost komunikacije, odnosno prijenosa i dijeljenja određenih relevantnih informacija među članovima skupine ili među različitim skupinama. U suštini, komunikacija osigurava opstanak skupine jer omogućuje distribuciju informacija o potrebama skupine i izvoru njihovog zadovoljenja (položaj izvora hrane), zatim informacija o stanju pojedinca u skupini (plač ili cvilež u slučaju boli), upozoravanje na opasnost (lavež pasa) te iskazivanje prijetnje

[54] Ravlić, S., Pluralizam i participacija..., Polit. misao, Vol XXXVII, 2000. br. 1, str. 84.—98.

(režanje). Komunikacija je uvjetovala razvoj medijskih tehnologija u ljudskom društvu te je, s vremenom, nadišla ulogu isključivo biološkog sredstva za opstanak ili razvoja socijalnih odnosa i postala primarni faktor u širenju informacija relevantnih za razvoj i primjenu ideja, znanja i praksi u svim sferama djelovanja.[55]

U zemljama u kojima mediji nisu neovisni o vladinim institucijama, vrlo je lako moguće da vladari medije zloupotrijebe u svrhu propagande. U takvim slučajevima, mediji sigurno ne mogu pojačati transparentnost i demokratski nadzor nad sektorom sigurnosti. Sa pojavom Interneta, potencijal za pristup javnosti zvaničnim informacijama je postao ogroman. Postoji opći trend u zadnjem desetljeću ka većoj transparentnosti, odgovornosti prema javnosti i pristupačnosti zvaničnih informacija. Ovaj trend bi se trebao podsticati s obzirom da doprinosi informiranosti građanstva, većem kvalitetu javne debate u vezi sa važnim političkim pitanjima i na kraju boljoj upravi. A nedostatak interneta je taj što ga mogu koristiti ekstremne grupe za širenje, naprimjer, rasizma i antisemitizma. U nekim nedavnim sukobima drugi informacioni mediji, kao što su radio stanice, pružili su platformu ekstremnim grupama i pomogle stvaranju mržnje među raznim društvenim grupama.

Internet, infrastrukture, uređaji, softveri, hardveri i aplikacije najbolje su kombinacije kako promijeniti ljudski život i stvoriti novo bojno polje. Ratovi na kakve smo navikli postali su irelevantni za budućnost, ali i sadašnjost, a dobrim dijelom zamijenilo ih je informacijsko ratovanje. Informacijski rat događa se svugdje u svijetu s varijacijama u svrhama kao što su političke, nacionalne, špijunaža, obavještajne jedinice te uključujući i uništavanje druge rase bez upotrebe oružja. Prema američkoj službenoj doktrini četiri su instrumenta i izvora nacionalne moći: javna diplomacija, informacija, vojska i gospodarstvo. Informacijski rat definiran je kao napad ili obrana u svrhu razaranja, iskorištavanja, odbijanja korištenja informacijskog sistema te digitalne/računalne mreže u svrhu zaštite vlastite. Novi mediji kao što su društvene mreže najbolji su način za informacijsko ratovanje. Društvene mreže mogu se definirati kao platforma za interaktivnu komunikaciju individue ili grupe za dijeljenje, razmjenu, diskusiju i komentiranje sadržaja u različite svrhe. Virtualna komunikacija dovodi do toga da svaka osoba može biti vojnik u informacijskom ratu koji se vodi putem novih medija. [56]

[55] Rufferty, I., 2017., How Communication Has Evolved With The New Technologies. https://medium.com/bsg-sms/how-communication-has-evolved-with-the-new-technologies-52ee1ca114f Pristup:28.09.2020.
[56] Lukač, I. Uloga novih medija u informacijskom ratovanju. Osijek: Sveučilište Josipa Jurja Strossmayera. Diplomski rad. 2019.

Mediji tako mogu pomoći vladi i parlamentu da građanima objasne svoje odluke i politike, koji imaju pravo da budu informirani i da sudjeluju u političkom procesu na temelju informacija koje su im poznate. Naprimjer, mediji mogu doprinijeti ostvarenju prava javnosti na informiranost putem distribuiranja informacija o onima koji obavljaju javne funkcije u oblasti sigurnosti, vrsti sigurnosne politike koja je usvojena, raspoređivanju trupa u inozemstvu, vojnoj doktrini, nabavci i ugovorima i drugim sporazumima na kojima se temelje, akterima koji u tome sudjeluju, izazovima pred sigurnošću ubuduće i relevantnim debatama. Međutim, oni također mogu biti podvrgnuti nametnutoj ili samonametnutoj cenzuri kada se radi o povjerljivim informacijama. [57]

VII DEMOKRATISKI NADZOR I KONTROLA STUDIJA SLUČAJA BOSNA I HERCEGOVINA

7.1. Organizaciona struktura u Bosni i Hercegovini

Savremena država Bosna i Hercegovina sa današnjom strukturom je nastala nakon potpisivanja mirovnog sporazuma u Daytonu 1995. Godine. Osnovni razlog potpisivanja ovog sporazuma je svakako zaustavljanje rata koji se u to vrijeme dešavao na ovim prostorima. Potpisom ovog mirovnog sporazuma Bosna i Hercegovina kao država je sačinjena od dva entiteta Federacije Bosne i Hercegovine i Republike Srpske te od Distrikta Brčko. Svaka od ovih jedinica odnosno entiteta ima zasebnu vladu i vlast, isto tako i distrikt ima svoju vlast. Pored toga i jedan i drugi entitet imaju svoju policiju, ministarstva, administracije. Naravno sve to je podređeno državnoj vlasti koja je najviši po hijerarhijskoj strukturi. Na nivou države imamo vlast, parlament, vladu, policiju, vojsku i ostale institucije koje ima državna ovlaštenja. U skladu sa Dejtonskim sporazumom, Visoki predstavnik pod mandatom Ujedinjenih nacija postavljen je da bi podržao provedbu mira.

Dok je Dejtonski mirovni sporazum imao neprocjenjiv značaj za zaustavljanje rata i donošenje mira i stabilnosti Bosni i Hercegovini, često se postavlja pitanje adekvatnosti Dejtonskog ustavnog sistema u sadašnjim okolnostima, kako u zemlji tako i van nje. Uveliko se smatra da su strukture koje su proizašle iz Dejtonskog mirovnog sporazuma previše kompleksne i fizikalno neodržive. Također se smatra da se uloga i ovlasti date međunarodnoj zajednici trebaju progresivno smanjivati kako država bude postizala normalizaciju. Bosna i Hercegovina ima direktno birano tročlano Predsjedništvo, koje se rotira na osmomjesečnoj

[57] Fluri, P., Johnsson, A. Parlamentarni nadzor nad sektorom sigurnosti: principi, mehanizmi i prakse. Interparlamentarna unija Centar za demokratsku kontrolu nad oru`anim snagama Verzija izdata u Sarajevu: Misija OSCE-a u Bosni i Hercegovini. 2003.

osnovi. Predsjedništvo je odgovorno, između ostalog, za vođenje vanjske politike, predlaganje godišnjeg budžeta i za zastupanje Bosne i Hercegovine u međunarodnim organizacijama. U entitetima također postoje predsjedništva. Bosna i Hercegovina ima dvodijelni Parlament na nivou države, parlamente entiteta, Brčko Distrikta te parlamente na kantonalnom nivou. [58]

Politički konsenzus je rijetka roba u BiH. Nedostatak političke volje ima puno veći uticaj na upravljanje u njoj nego u drugim zemljama, jer da bi sistem funkcionirao, potrebno je ostvariti visok stupanj saglasnosti.

I odlučivanje na državnom nivou kao i podijeljene nadležnosti koje je država dobila nakon Dejtona ostavljaju dosta prostora za lake i djelotvorne političke i administrativne opstrukcije. Kao što smo vidjeli, ako se predstavnici koji su imenovani ili izabrani u jednom entitetu jednostavno ne pojave u dovoljnom broju, oni na taj način paraliziraju rad državnih institucija. Dobro je poznato i dokumentirano da predstavnici RS-a u državnim institucijama kao i vlada tog entiteta opstruiraju državne poslove. Predstavnici RS-a su češće nego svi drugi konstitutivni narodi zajedno bojkotirali rad državnih institucija. Prenošenje nadležnosti s RS-a na državni nivo teče veoma sporo, i nevoljko, a uspješno samo pod značajnijim međunarodnim pritiskom. Premda je država formalno preuzela nadležnosti, RS je odgovorna za neprovođenje državnih direktiva na svojoj teritoriji, a njeni predstavnici na državnom nivou i dalje čine sve da onemoguće rad državne vlade. Opstrukcije RS-a su relativno očigledne i jasne. Međutim, manje se zna o načinima na koje Federacija BiH potkopava državne institucije. Opstrukcije u Federaciji su obično rezultat administrativne nesposobnosti, previda ili jednostavno loše komunikacije, a ne toliko političke opstrukcije. Međutim, u Federaciji je evidentna i nešto eksplicitnija politička opstrukcija izgradnje države. Uprkos značajnoj retoričkoj podršci izgradnji države, u stvarnosti, FBiH, njena vlada, parlament i dominantne političke stranke iskazuju veliko nepoštivanje autoriteta i integriteta države.

Uprkos značajnim izazovima s kojima se država BiH suočava, učinjeni su izvjesni pozitivni pomaci u pogledu "normalizacije" državnih funkcija od Dejtona do danas. Općenito, uspjehu ovih reformi doprinijela su tri faktora: (a) jasna podjela nadležnosti, (b) djelotvorni državni kapaciteti za provedbu i (c) djelotvorna međunarodna pomoć. Ukratko, državne institucije su najdjelotvornije tamo gdje država ima isključive nadležnosti i gdje je potreba za saradnjom s entitetima minimalizirana i gdje su međunarodni napori usredotočeni ne samo na usvajanje legislative već i na institucionalni razvoj s ciljanom međunarodnom podrškom. To ukazuje da uprava na državnom nivou u BiH ne podrazumijeva ništa što je samo po sebi neodrživo.

[58] Evropska komisija – Bosna i Hercegovina izvještaj o napretku u 2005. godini. Brisel: SEC 2005. br izdanja 1422

Ratno naslijeđe ne znači da su zajedničke međuentitetske strukture na državnom nivou osuđene na nedostatak legitimiteta kod javnosti. Državne institucije ipak mogu funkcionirati vrlo djelotvorno ukoliko su zadovoljeni određeni uvjeti. [59]

7.2. Pravni okvir za demokratski nadzor

Parlamentarni nadzor nad sektorom sigurnosti u Bosni i Hercegovini regulisan je odredbama Ustava BiH, ustavima entiteta i kantona te velikim brojem zakona, podzakonskih akata i pravilnika. Na državnom nivou BiH, 2004. godine je uspostavljena Zajednička komisija za odbranu i sigurnost (ZKOS BiH) kao parlamentarno tijelo koje u skladu s Poslovnicima oba doma Parlamentarne Skupštine BiH, ima široka ovlaštenja za provođenje nadzora u ovoj oblasti. U skladu s nadležnostima, ZKOS inicira donošenje zakona ili zakonskih izmjena na nivou BIH, učestvuje u izradi i usvajanju strateških dokumenata, raspravlja o izvještajima o radu institucija sektora odbrane i sigurnosti, i po potrebi obavlja saslušanja predstavnika odbrane, policijskih i sigurnosnih agencija.

Druga parlamentarna komisija na državnom nivou je Komisija za nadzor nad radom Obavještajno-sigurnosne agencije BiH. Poslovnicima oba doma Parlamentarne Skupštine BiH je utvrđeno da je Zajednička komisija za nadzor nad radom OSA-e zadužena da nadzire zakonitost rada Obavještajno-sigurnosne agencije Bosne i Hercegovine, da vrši budžetsku kontrolu i analizira načine trošenja budžetskih sredstava ove agencije. Na nivou Federacije BiH, vanjski nadzor nad radom sigurnosnog sektora obezbijeđen je kroz radna tijela oba doma Federalnog parlamenta, koja su odgovorna za pitanja sigurnosti. To su Komisija za bezbjednost Predstavničkog doma i Komisija za bezbjednost Doma naroda.

Parlamentarni nadzor može biti definisan kao „revizija, praćenje i nadgledanje rada vladinih i javnih organizacija, te provedbe politika rada i zakona“. Ovakav nadzor ima krucijalnu ulogu u demokratskom upravljanju jer pomaže da se unaprijedi kvalitet politika rada, programa i praksi izvršnih tijela, te daje veću legitimnost takvim politikama rada. Prilikom vršenja funkcije nadzora, zakonodavstvo može otkriti i spriječiti zloupotrebu nadležnosti i nezakonite radnje u redovima vladinih i javnih organizacija, te, istovremeno, osigurati efikasno i transparentno trošenje javnog novca od strane izvršnih vlasti i pravilno provođenje politika rada. [60]

---

[59] Strukture upravljanja državom Bosnom i Hercegovinom, Izdavač: Vanjskopolitička inicijativa BH http://vpi.ba/wp-content/uploads/2016/05/Struktura_upravljanja_drzavom_u_BiH.pdf Pristup: 10.10.2020.

[60] Mišljenje o nacrtu zakona o parlamentarnom nadzoru u Bosni i Hercegovini, na osnovu nezvaničnog engleskog prevoda Nacrta zakona koji je osigurala Misija OSCE-a u Bosni i Hercegovini (2017.) Ured OSCE-a za demokratske institucije i ljudska prava. https://www.osce.org/files/f/documents/6/5/322431.pdf Pristup: 25.10.2020.

Komisije su uspostavljene u skladu s poslovnicima oba doma Federalnog parlamenta i imaju širok spektar nadležnosti. Ove komisije razmatraju pitanja sistema i politike u oblasti bezbjednosti u okviru prava i dužnosti doma pri kojem djeluju, predlažu mjere za organizovanje, vođenje i razvoj bezbjednosti Federacije, a veliki značaj komisija leži u tome što one mogu provoditi i istrage i u tu svrhu zahtijevati svjedočenja, dokaze i dokumente. U Republici Srpskoj, nadzor nad radom sigurnosnog sektora realizuje se kroz Odbor za bezbjednost koji se nalazi u okviru Narodne skupštine RS. Odbor za bezbjednost između ostalog, razmatra pitanja iz domena rada organa i institucija sigurnosti, daje mišljenje, stavove i preporuke te predlaže Narodnoj skupštini preduzimanje odgovarajućih mjera. Nadležnost Odbora je da učestvuje i u raspravi u donošenju budžeta sigurnosti u Republici Srpskoj, prati ostvarivanje budžeta u ovoj oblasti i razmatra izvještaje revizije o kontroli finansijskog poslovanja institucija nadzora.[61]

Odbrambena politika Bosne i Hercegovine je važan dio unutrašnje i vanjske politike. Izgrađena je na strateškim principima koja odgovaraju vanjskoj i sigurnosnoj politici i rezultat je razmatranja šireg sigurnosnog okruženja. Odbrambena politika definiše glavne elemente odbrambenog sistema Bosne i Hercegovine i načine na koji oni funkcioniraju, uključujući Oružane snage kao najbitniji dio sistema. Odbrambena politika Bosne i Hercegovine se zasniva na sljedećim principima:

- demokratskoj, civilnoj kontroli vojske, uz parlamentarni nadzor;
- transparentnosti aktivnosti u oblasti odbrane, uključujući planiranje i budžetiranje odbrane;
- uravnoteženosti snaga i mogućnosti unutar Bosne i Hercegovine, podregija i jugoistočne Evrope;
- modernizaciji snaga, uključujući razvoj interoperabilnosti Oružanih snaga Bosne i Hercegovine s NATO-om;
- integraciji u Evroatlantske kolektivne sigurnosne strukture;
- saradnji u oblasti kontrole naoružanja i mjerama izgradnje sigurnosti i povjerenja, uključujući učešće u sigurnosnim strukturama i protokolima jugoistočne Evrope;
- Izgradnji sistema odbrane, zasnovanog na navedenim principima, čime će Bosna i Hercegovina realizovati ciljeve odbrambenih reformi na putu od individualne ka kolektivnoj sigurnosti.

[61] Hadžović, D. Podnesak za Alternativno mišljenje i izvještaj za 2017. Parlamentarni nadzor nad sigurnosnim sektorom u Bosni i Hercegovini. Centar za sigurnosne studije. 2017.

Parlamentarni demokratski nadzor nad oružanim snagama i svim institucijama odbrane ostvaruje se preko Parlamentarne skupštine Bosne i Hercegovine. Za ostvarivanje parlamentarnog nadzora Parlamentarna skupština BiH formira odgovarajuća radna tijela – komisije, koje se neposredno bave navedenim pitanjem.[62]

7.3. Zakonski i podzakonski akti

Postoji rasprostranjeno mišljenje da sigurnosna politika predstavlja 'prirodni' zadatak izvršne vlasti s obzirom da ona posjeduje neoophodno znanje i može brzo djelovati. Na parlament se gleda kao na manje adekvatnu instituciju za bavljenje pitanjima sigurnosti, posebno s obzirom na njegove često vremenski duge procedure i nedostatak potpunog uvida u neohodnu stručnost i informacije. Međutim, kao što je to slučaj i sa bilo kojom drugom političkom sferom, parlamentu su dati u nadležnost revizija i praćenje rada izvršnih organa vlasti. S obzirom da se sektor sigurnosti bavi jednim od ključnih zadataka države, potreban je sistem provjera i balansa kao protuteža moći izvršne vlasti. Parlamentarni nadzor nad sektorom sigurnosti stoga predstavlja osnovni element raspodjele vlasti na državnom nivou, i ukoliko je djelotovoran, on ograničava moć izvršne vlasti ili predsjednika. Izvršna vlast utvrđuje zakone kojim se reguliraju pitanja sigurnosti. Bez obzira na to, članovi parlamenta igraju važnu ulogu u razmatranju nacrta zakona. Oni mogu, ukoliko je potrebno, predložiti amandmane kojim osiguravaju da predložene zakonske odredbe adekvatno odražavaju nov način razmišljanja o sigurnosti. Osim toga, na parlamentu je da vodi računa o tome da zakon ne ostane mrtvo slovo na papiru, nego da bude u potpunosti primijenjen. [63]

U Bosni i Hercegovini imamo formiranu Obavještajno – sigurnosnu agenciju BiH koja je osnovana 2004. godine kada je usvojen zakon o Obavještajno-sigurnosnoj agenciji Bosne i Hercegovine. Njen glavni zadatak jeste da prikuplja, analizira i distribuira obavještajne podatke u cilju zaštite sigurnosti , uključujući suverenitet, teritorijalni integritet i ustavni poredak Bosne i Hercegovine. Prema zakonu Agencija je civilna obavještajno sigurnosna institucija koja ima status nezavnisne administrativne organizacije Bosne i Hercegovine te ima status pravnog lica. Agencija je odgovorna za analiziranje prikupljenih podataka i njihovo prenošenje ovlaštenim dužnosnicima i tijelima (najvši organi vlasti i njihovi predstavnici), kao i za prikupljanje i analiziranje i prenošenje obavještajnih podataka sa svrhom pružanja pomoći ovlaštenim službenim licima, kako je definirano zakonima o krivičnom postupku u Bosni i Hercegovini, te ostalim mjerodavnim tijelima u BiH, kada je to potrebno radi

[62] Sigurnosna politika Bosne i Hercegovine, Predsjedništvo Bosne i Hercegovine, Sarajevo 2006.
[63] Born, H. Parlamentarni nadzor nad sektorom sigurnosti, DCAF Fojnica: Svjetlost.2003.

suzbijanja prijetnji po sigurnost Bosne i Hercegovine. Zakonom su jasno definirane "prijetnje po sigurnost Bosne i Hercegovine", a to su:

- Prijetnje sa aspekta terorizma uključujući i međunarodni terorizam;
- Prijetnja sa aspekta špijunaže usmjerena protiv BiH ili štete po sigurnos BiH na bilo koji drugi način;
- Prijetnja sa aspekta sabotaža usmjerenih protivi vitalne nacionalne infrastrukture BiH ili na drugi način usmjerene prema BiH;
- Prijetnja sa aspekta organizovanog kriminala usmjerenog prema BiH ili štete po sigurnost na bilo koji drugi način;
- Prijetnjama sa aspekta nezakonite međunarodne proizvodnje oružja za masovno uništenje, ili njihovih komponenti, kao i materijala i uređaja koji su potrebni za njihovu proizvodnju;
- Prijetnjama sa aspekta nezakonite trgovine proizvodima i tehnologijama koje su pod međunarodnom kontrolom;
- Prijetnjama sa aspekta radnji kažnjivih po međunarodnom humanitarnom pravu i prijetnjama sa aspekta djela organiziranog nasilja ili zastrašivanja nacionalnih ili vjerskih grupa u Bosni i Hercegovini.[64]

U Zakonu o Obavještajno-sigurnosnoj agenciji Bosne i Hercegovine imamo akte u kojima su detaljno prikazani svi zadaci, norme i obaveze ove agencije.

Pored toga imamo i Zajedničku komisiju za odbranu i sigurnost BiH koja je osnovana 2003. godine, a potreba za formiranjem ove komisije je bila za formiranje jedinstvenih Oružanih snaga Bosne i Hercegovine ali i drugih zajedničkih institucija iz sigurnosnog sektora. Demokratski i parlamentarni nadzor nad odbrambenim i sigurnosnim sektorom je bio neophodan za procese koji su uslijedili i koji se odvijaju radi priključenja Bosne i Hercegovine NATO savezu i Evropskoj uniji. Komisija sarađuje sa svim institucijama iz odbrambeno-sigurnosnog sektora u BiH, kao i međunarodnim organizacijama i institucijama, a posebno s NATO-om, Misijom OSCE-a, UNDP-a, EUPM-a, DCAF-a i dr.

Nadležnosti Komisije definirane su poslovnicima domova PSBiH, kao i određenim zakonskim odredbama u oblasti odbrane i sigurnosti. U skladu s navedenim propisima,

Komisija je nadležna za:

- Razmatranje i praćenje provođenja odbrambene i sigurnosne politike BiH;
- Razmatranje zakona iz oblasti odbrane i sigurnosti BiH;

[64] Obavještajno-sigurnosna agencija Bosne i Hercegovine http://www.osa-oba.gov.ba/nadlb.html Pristup: 25.10.2020.

- Razmatranje izvještaja, informacija i drugih akata Ministarstva odbrane BiH, Ministarstva sigurnosti BiH i drugih izvršnih tijela koja se bave pitanjima odbrane i sigurnosti, kao što su: Državna agencija za istrage i zaštitu (SIPA), Granična policija BiH, NCB Interpol BiH, Služba za poslove sa strancima, Centar za uklanjanje mina (BHMAC), s posebnim osvrtom na planove vezane za strukturu i statusna pitanja Oružanih snaga BiH, uvoz-izvoz oružja i vojne opreme, borbenu gotovost, vojne vježbe te međunarodne operacije podrške miru. Nakon razmatranja ovih akata, Komisija izvještava domove PSBiH;
- Razmatranje budžeta institucija odbrane i sigurnosti BiH i njihovog izvršenja, kao i revizijskih izvještaja o finansijskom poslovanju ovih institucija;
- Razmatranje pitanja saradnje BiH sa UN-om, Misijom OSCE-a i drugim organizacijama iz odbrambeno-sigurnosnog sektora;
- Ostvarivanje saradnje s nadležnim parlamentarnim komisijama bh. entiteta, drugih država, kao i međunarodnim organizacijama i tijelima iz odbrambeno-sigurnosnog sektora;
- Razmatranje svih drugih pitanja iz oblasti sigurnosnog sektora BiH.[65]

Kada govorimo o zakonskim i podzakonskim aktima vezano za sigurnost države Bosne i Hercegovine možemo naći i u Zakonu o Odbrani Bosne i Hercegovine. Kada govorimo o ovom zakonu samo dio se odnosi na demokratki nadzor i kontrole sigurnosti Bosne i Hercegovine. Kada govorimo o uvodnom dijelu Zakona Opće odredbe – član 4. zadaci oružanih snaga. Drugi dio zakona Prava i nadležnosti institucija Bosne i Hercegovine imamo član 6. – ciljevi, član 9. – vojnoobavještajni poslovi, član 10. – Nadležnost Parlamentarne skupštine Bosne i Hercegovine, član 12. – Nadležnost Predsjedništva, član 13. – Nadležnost Ministarstva odbrane BiH, član 15. – Organizacione i administrativne nadležnosti, član 16. – Komandne nadležnosti, član 17. kontrola i inspekcija, član 29. - Nadležnosti komandanta Komande za podršku Oružanih snaga. U poglavlju 4. Zakona o odbrani BiH, Proglašenje ratnog ili vanrednog stanja direktno vezano je nekoliko članova i to Član 40. – Zahtjev za proglašenje ratnog stanja, Član 41. - Zahtjev za proglašenje vanrednog stanja, Član 42. – Proglašenje ratnog i vanrednog stanja.[66]

[65] Parlamentarna skupština BiH - zajednička komisija za odbranu i sigurnost BiH https://www.parlament.ba/Publication/Read/3602?title=zajednicka-komisija-za-odbranu-i-sigurnost-bih&pageId=239 Pristup:25.10.2020.

[66] Zakon o odbrani Bosne i Hercegovine (2005.) (http://www.mod.gov.ba/files/file/zakoni/Zakon-o-odbrani-bs.pdf)

7.4. Vanjska kontrola demokratskog nadzora i kontrole

Kontrola u raznim službama od strane vlasti ima jako veliki značaj kako bi se osiguralo zakonito djelovanje ovih službi. Značaj kontrole obavještajnih službi od strane vlasti jeste zbog toga što ove agencije imaju ovlaštenja koji na određeni način mogu ograničiti ljudska prava i sloboda ukoliko se ne kontrolišu. Isto tako agencije su u sjeni odnosno rade u tajnosti te postoji mogućnost da to koriste kako bi izbjegli određenu kontrolu. Cilj kontrole je da se osigura da djelovanje obavještajnih službi bude opravdano i u skladu sa zakonom, kako bi ljudska prava i slobode bile maksimalno zaštićene. Posebno se to odnosi na Bosnu i Hercegovinu i ostale zemlje regiona koje su u razvoju, što ima veliki uticaj i na obavještajne agencije koje su postavljene kao jedan od uslova za pristup Evropskim integracijama.

Tomić smatra da vanjska kontrola ima četiri sektora i to:

- Parlamentarna kontrola;
- Vladina kontrola;
- Sudska kontrola;
- Specijalni oblici vanjske pravne kontrole.

Važnost vanjske kontrole jeste objektivnost i nepristrasnost, te povećanoj zaštiti zakonodavnosti kod svih oružanih državnih službi – voditi računa o vanjskoj i unutrašnjoj bezbjednosti.[67]

Nosioci demokratske civilne kontrole su:

- Izvršna vlast;
- Zakonodavna vlast;
- Sudska vlast;
- Javnost i civilno društvo.

Izvšna vlast – predstavlja vrh vlasti u političkom sistemu na kojem se kreira politika i kroz koji se ta politika provodi. Glavna funkcija ove vlasti jeste izvršavanje zakona, koji donosi zakonodavna vlast. Ovu vlast čini vlada i ona neprestano nadzire organe uprave posebno organe unutrašnjih poslova koji odgovaraju za svoj rad u granicama utvrđenih nadležnosti.

Zakonodavna vlast – donosi zakone za sve pa tako i za vlast kako bi se osigurala vladavina prava. U modernoj politici ova vlast nalazi se pod kontrolom predstavničkog tijela odnosno parlamenta. Prema demokratskim izborima građani biraju svoje predstavnike u parlamentu i

[67] Tomić, R.Normativna polazišta za civilnu kontrolu vojske i policije. Beograd - Centar za civilno - vojne odnose, 2001.

oni kao njihovi predstavnici glasaju za zakone u njihovo ime. Zakonodavna vlast vrši parlamentarni nadzor nad sektorom sigurnosti putem donošenja raznih zakona kojima se definiraju i reguliraju sigurnosne službe i njihove ovlasti. Parlamentarne nadležnosti za kontrolu službi su:

- Zakonom osniva službe bezbjednosti i druge ovlašćene državne organe;
- Definiše misije, ciljeve i zadatke;
- Dodjeljuje opšta i posebna ovlaštenja i utvrđuje postupke za njihovu primjenu;
- Utvrđuje obavezu izvještavanja parlamenta i obavještavanja javnosti;
- Utvrđuje procedudre, aktere i nadležnosti za parlamentarni nadzor;
- Nadzire poštovanje načela ustavnosti i zakonitosti u njihovom djelovanju;
- Uređuje procedure za unutrašnju kontrolu;
- Usvaja budžet i nadzire njegovo trošenje;
- Daje saglasnost na ili dostalja mišljenje za postavljanje rukovodilaca službi.

Parlamentarni mehanizmi primjenjeni na sektor sigurnosti su: parlamentarne debate o pitanjima sigurnosti, parlamentarna pitanja i upiti vladinim dužnosnicima i parlamentarna istraživanja u vezi sa sigurnošću. [68]

Sudska vlast – njen posao jeste da interpretira zakone koje je donijela zakonodavna vlast. U Bosni i Hercegovini primjer je Ustavni sud Bosne i Hercegovine koji je u odnosu na druge organe u vlasti Bosne i Hercegovine samostalan i neovisan. U Federaciji Bosne i Hercegovine postoje opštinski sudovi, kantonalni i Vrhovni sud Federacije Bosne i Hercegovine kao redovni sudovi. Sudska kontrola uprave je u većini država najvažnija i najrazvijenija vanjska kontrola. Ima tri glavna modela:

- Kontrola od strane redovnog sudstva (opšte nadležnosti);
- Kontrola od strane specijalnog sudstva, upravnog sudstva;
- Kontrola od strane upravnog sudstva, koji se po pravilu tiče opštih pravnih akata organa uprave.

Specijalne kontrole uprave spoljnog odnosno civilnog karaktera kada je riječ o kontroli policije i vojske. Među značajnima ubrajamo kontrolu koju vrši Ombudsmen, koji se bavi pritužbama građana u vezi sa mjerama i odlukama ili propustima javne uprave.[69]

[68] Born, H. Parlamentarni nadzor nad sektorom sigurnosti, DCAF Fojnica: Svjetlost. 2003. str. 83.
[69] Tomić, R. Normativna polazišta za civilnu kontrolu vojske i policije. Beograd - Centar za civilno - vojne odnose.2001

Civilno građansko društvo – uslov za postojanje ovog društva zasnovano je na vladavini prava, socijalnoj pokretljivosti, komunikacijama, društvu tolerancije i slobode kretanja ljudi. Angažman ovog društva treba da bude usmjeren na javnost provociranje rasprava o određenoj temi, uvjeravanje za opštu vrijednost cilja za koje se zalažu itd.[70]

Nevladina organizacija NVO – organizacija ili udruženje civilnog društva koja nije pod nadležnošću vlade i čiji osnivač nije država. Nevladine organizacije i društva mogu jačati demokratski i parlamentarni nadzor na više načina:

- Putem distribucije neovisnih analiza i informacija o sektoru sigurnosti, vojnim pitanjima parlamentu, medijima i javnosti;
- Praćenje i podsticanje poštivanja vladavine prava i ljudskih prava unutar sektora sigurnosti, uvrštavanjem u politički program pitanja sigurnosti koja su bitna za cjelokupno društvo;
- Doprinositi parlamentarnoj kompetentnosti i izgradnji kapaciteta putem kurseva, obuke i seminara, alternativnim stručnim mišljenjima o vladinoj sigurnosnoj politici, vojnim budžetima, nabavci, opcijama resursa podsticanjem javne debate i formuliranjem mogućih strateških opcija;
- Pružanjem povratnih informacija o odlukama u vezi sa državnom sigurnosnom politikom i načinom njihova realiziranja;
- Educiranje javnosti i omogućavanjem alternativnih debata u javnom domenu.[71]

7.5. Unutarnja kontrola demokratskog nadzora i kontrole

Pored vanjske kontrole imamo i unutrašnju kontrolu demokratskog nadzora svih državnih institucija, ljudi koji tamo rade, kao i sigurnosti države i njenih građana. Svrha je unutarnjeg nadzora sprečavanje i otkrivanje svih oblika nezakonitih, nepropisnih ili neetičnih postupanja ili ponašanja zaposlenika u svim institucijama tako i sigurnosti, ali i pomoć prilikom organizacije rada, rukovođenja i upravljanja ljudskim potencijalima. [72]

Rukovođenje i kontrola rada Obavještajno-sigurnosne agencije BiH od strane izvršne vlasti povjerena je Vijeću ministara BiH i predsjedavajućem Vijeća ministara BiH. U cilju izvršavanja svih zakonom definisanih dužnosti, predsjedavajućem Vijeća ministara BiH pomaže Sigurnosno-savjetodavni ured, čije članove imenuje predsjedavajući u konsultaciji sa

[70] Dmitrović, T.. Izazovi civilnog društva u BiH, Analize i preporuke za politike. Sarajevo 2017. http://www.sif.ba/dok/1386600343.pdf Pristup: 25.10.2020.
[71] Born, H.Parlamentarni nadzor nad sektorom sigurnosti, DCAF Fojnica: Svjetlost. 2003.
[72] Kralj, Ž .Unutarnja kontrola i nadzor policije. Stručni članak (Zagreb), godina 23. 2014, broj 1., str. 73.- 81.

generalnim direktorom, u skladu sa Zakonom o državnoj službi u institucijama BiH i na osnovu sigurnosnih provjera koje izrađuje Obavještajnosigurnosna agencija BiH. Pored toga, u cilju realizacije efikasne koordinacije svih obavještajno-sigurnosnih pitanja koja se odnose na ukupan rad Obavještajno-sigurnosne agencije BiH, postoji i Izvršni obavještajni odbor, kojeg takođe osniva predsjedavajući Vijeća ministara BiH.[73] Barem tri aspekta sektora sigurnosti predstavljaju pravi izazov za parlamentarni nadzor: Zakoni o tajnosti mogu onemogućiti nastojanja u pravcu povećanja transparentnosti u sektoru sigurnosti. Zakoni o tajnosti, posebno u zemljama u kojima se demokratski sistem vlasti razvija, kao i u zemljama koje su razorene ratom, mogu ograničiti ili ugroziti parlamentarni nadzor nad sektorom sigurnosti - razlog za to je i nepostojanje zakonskih propisa kojim se regulira sloboda informiranja.

Sektor sigurnosti predstavlja izrazito kompleksnu oblast u kojoj parlamenti trebaju vršiti nadzor nad pitanjima kao što su nabavka naoružanja, kontrola naoružanja i spremnost vojnih jedinica.

Kontrola obavještajno-sigurnosnih agencija ima izuzetnu važnost u svim demokratskim sistemima. Pored toga što je neophodna za demokratiju, izvršna kontrola obavještajno-sigurnosnih službi ima i svoje nedostatke. Može doći do zloupotrebe obavještajno-sigurnosnih službi u političke svrhe, u smislu da se službe koriste za pribavljanje informacija i podataka o političkim protivnicima ili podataka koji mogu narušiti ugled tih osoba, te iste, raznim ucjenama, prisiljavati na određene političke i druge poteze. Vrlo je tanka granica koja razgraničava vršenje pravilne kontrole obavještajno-sigurnosnog sektora od političke manipulacije i zloupotrebe, te je od posebnog značaja postojanje zaštitnih mjera i mehanizama, koji bi osigurali da službe ne budu zloupotrijebljene, odnosno mjere koje garantuju nepristrasnost i profesionalizam službi. U tom smislu potrebne su mjere koje pružaju zaštitu rukovodiocima agencija od navedenih utjecaja od strane izvršne vlasti. To se može učiniti u obliku garantovanja sigurnosti njihovog položaja, postavljanja zakonskih granica u smislu određivanja šta se od agencija može tražiti da naprave, te osnivanja nezavisnih mehanizama kojima se može izraziti zabrinutost zbog moguće zloupotrebe. Prava izvršne vlasti trebaju imati protivtežu kako bi se spriječilo da izvršna vlast zloupotrijebi agenciju. [74] Kada je riječ o našoj državi zakon o Obavještajno-sigurnosnoj agenciji BiH

[73] Musić, E. (2011.) .Opšti okviri kontrole obavještajno – sigurnosnih službi od strane izvršne vlasti. Zenica: Pravni fakultet Univerziteta u Zenici, Vol. 8 Issue 4, str. 287.-307.
[74] Born, H. i Johnson, L. Balancing operational efficiency and democratic legitimacy. Potomac Books, Inc 2005 str. 225.-239.

naleže jasne odredbe u smislu da Obavještajno-sigurnosna agencija BiH ne smije biti podložna nikakvim pokušajima potkopavanja njene nepristrasnosti, bilo promocijom interesa nekih političkih stranaka ili potkopavanjem vjerodostojnosti zakonitih političkih pokreta unutar zemlje. Važno je istaći zakonsku zabranu da zaposleni Agencije ne mogu biti članovi političkih stranaka, primati instrukcije od političkih stranaka, niti obavljati bilo kakvu dodatnu aktivnost za koju se plaća naknada ili drugu javnu ili profesionalnu dužnost koja je nespojiva s radom u Agenciji.[75]

Kontrola i njen značaj je jako važan faktor u funkcionisanju države i svih njenih institucija po zakonima koji su doneseni. Za ispravno vršenje kontrole neophodna je efikasna dvosmjerna komunikacija između obavještajnih službi i izvršne vlasti, u okviru koje bi izvršna vlast bila odgovorna za uobličavanje politike sigurnosnog i obavještajnog djelovanja, bez miješanja u pojedinačni operativni rad obavještajnih službi.

ZAKLJUČNA RAZMATRANJA

U ovom dijelu rada rezimirat ćemo sve dijelove ovog rada, pojasnit ćemo još jednom određene dijelove i hipoteze koje su postavljene na samom početku pisanja ovog rada. Ono što je veoma važno reći za temu ovog rada jeste da je veoma mali broj izvora pomoću kojih bi se detaljno sagledala situacija cyber prostora na nivou Bosne i Hercegovine ali i drugih država i prostora. Zbog toga je veoma važno bilo skupiti sve informacije, radove i zapise koji govore o ovoj oblasti pročitati i obraditi informacije kako bi se napravio kvalitetan rad koji može bar malo približiti cyber prostor i sve njegove pojavne oblike. Jasno je kako ova oblast još nije jasno definirana, istražena i izučena zbog toga što se radi o jako kompleksnom i velikom prostoru koji se svakodnevno razvija i povećava. S tim u vezi je jasna namjera svih velikih nevladinih organizacija koje su direktno uključene u istraživanje i praćenje ovog prostora, da što je jasnije moguće donesu određene okvire kako zakonske tako i sve druge kako bi se ova oblast jasnije i na najbolji mogući način pratila i kontrolisala. Svakako veliki problem predstavlja brz razvoj samog cyber prostora i cjelokupne tehnologije koja je ključ za ovaj prostor. Isto tako problem predstavlja i to što rijetko koja država, a posebno države koje ne spadaju u sami svjetski vrh razvoja, ima zakonske okvire i pravila koja pojednostavljuju kontrolu djelovanja u cyber prostoru. Otežavajuća okolnost isto tako je i ta što ovu oblast nije moguće fizički pratiti odnosno sve se dešava viralno. Interesantno je sagledati demokratski nadzor i odnos država prema cyber prostoru, ali i cyber ratovima koji su kroz bližu prošlost

[75] Musić, E. Opšti okviri kontrole obavještajno – sigurnosnih službi od strane izvršne vlasti. Zenica: Pravni fakultet Univerziteta u Zenici, Vol. 8 Issue 4,2005 str. 287.-307.

kao i sadašnjost sve prisutniji i češći. To je još jedan razlog zašto je bitno dodatno da se prouči ova oblast i zakonski reguliše na nivou država ali i globalnom nivou.

Kada govorimo o ovom radu konkretno pisan je po svim metodološkim principima i pravilima. Problem ovog rada je *uočavanje samog pristupa demokratskog nadzora kad je riječ o cyber ratovanju u svijetu*. U prvom dijelu je opisan cyber prostor i cyber ratovanje, da bi se kroz nastavak rada odnosno, druge dijelove razradio problem ovog rada. Pojašnjeno je na koji način se najjače svjetske nevladine organizacije, ali i konkretno državne institucije pojedinih država bore sa ovim problemom. Predmet rada je *utvrditi načine na koji parlamentarni nadzor djeluje kad je riječ o cyber ratovanju.* Kao što smo već ranije rekli sve češći su cyber ratovi, kada tome pridodamo evidentan i intenzivan tehnološki razvoj onda nam je jasno kako vodeće svjetske sile razvijaju ovaj prostor u svrhu „nacionalne odbrane" što dovodi kasnije do određenih napada i na kraju ratova.

U četvrtom dijelu ovog istraživanja je detaljno obrađen predmet ovog rada, tu je jasno objašnjen nadzor pojedinih organizacija i institucija na cyber ratovanje. Kada je riječ o ciljevima ovog istraživanja podjeljeni su na *ciljeve naučnog i društvenog smijera*. Naučni ciljevi ovog istraživanja su svakako da na temelju dosadašnjih spoznaja ali i novih saznanja i informacija budu objedinjene u jedan rad koji će moći poslužiti u razumjevanju i daljnjen istraživanju cyber ratovanja i prostora. Kada je riječ o društvenim ciljevima govorimo o tome kako je ne tako veliki broj populacije upoznat konkretno sa cyber napadima i ratovima koji su sve prisutniji i češći te zbog toga ovo istraživanje može koristiti u razumjevanju i prihvatanju tih činjenica. Hipoteze u ovom istraživanju imamo kao generalnu ali i dvije posebne odnosno parcijalne hipoteze. Generalna hipoteza ovog istaživanja glasi „*demokratski nadzor i kontrola nad cyber ratovanjem nije dovoljno i jasno definisan kako u domaćem, tako i u međunarodnom opravnom okviru*". Ovim radom smo putem svih prikupljenih informacija smo pokušali definisati prije svega na međunarodnom nivou ali i u samoj Bosni i Hercegovini. Kada je riječ o parcijalnim hipotezama imamo dvije i to su „*pravo oružanih sukoba se primjenjuje na sve aktivnosti poduzete tokom trajanja oružanog sukoba, i na sve posljedice nastale na teritoriji država koje su uključene u oružani sukob ne ograničavajući se samo na prostor gdje se vrše vojne operacije*". *Kao i „cyber napadi podliježu primjeni pravila jus ad bellum koja se odnose na pravo države na upotrebu sile u cilju realizacije svoje nacionalne politike*". Potvrđene su dvije parcijalne hipoteze koje su postavljene, a suština je objašnjena isčitavanjem Tallinskog priručnika koji je u suštini jedini dokument koji u velikoj mjeri objašnjava i detaljno prikazuje cyber prostor i sve njegove prednosti i nedostatke, te

uticaj i djelovanje država u okviru tog prostora. Sistem indikatora koji je korišten u ovom istraživanju jeste *sistem deskriptivnih indikatora.*

Kada govorimo o načinu istraživanja ono je sprovedeno u tri faze i to *prikupljanjem adekvatnih izvora koji se tiču zadane tematike, nakon toga analizu i interpretaciju datih izvora i na kraju prikazivanje rezultata izvora te davanja mišljenja o istim.* U ovom radu imamo naučnu i društvenu opravdanost, kada je riječ o naučnoj ona je bitna je zbog *spoznaje temelja sukoba u cyber prostoru te njihovim inkorporiranjem u današnju literaturnu tematiku*. Društvena opravdanost je *razumjeti samu suštinu prirode agresije u cyber prostoru i karakter cyber sukoba i rata kao i uloge parlamentarnog nadzora*.

Ovim radom je cjelokupni cyber prostor objedinjen u jednu cjelinu kako bi drugi studenti, profesori, naučnici i svi zainteresovani imali veliki broj informacija na jednom mjestu. Jasno zbog kompleksnosti i veličine ovog prostora ovo je samo dio koji može koristiti za daljnje istraživanje i objašnjenje cyber ratovanja ali i cyber prostora u cjelini.

PREPORUKE

Kada smo istražili i skupili veliki broj informacija potom ih obradili dobili smo bolji uvid i jasniju sliku o cjelokupnoj tematici. Sada nam je jasnije koliko je zapravo ovo područje kompleksno i rasprostranjeno. Isčitavanje i istraživanjem smo stekli određena saznanja i možemo dati određene preporuke svima onima koji će u budućnosti da istraživaju ovu oblast ili koji će se dodatno interesovati. Preporučujemo sledeće:

- Formiranje posebne agencije za cyber prostor u Bosni i Hercegovini, čiji će isključivi zadatak biti praćenje, otkrivanje, suzbijanje svih cyber kriminala ali i eventualnih napada kako unutar države tako i na samu državu i njen integritet;
- Formiranje posebne organizacije na nivou Evrope koja će moći pratiti radnje svih zemalja kod kojih je cyber prostor posebno razvijen i korišten;
- Omogućiti nepolitičko djelovanje organizacije i uvid u eventualne nezakonite radnje u cyber prostoru za svaku državu;
- Zakonski obavezati da se uokviri cyber prostor unutar svake države zasebno ili na nivou određene regije ili cjelokupnog kontinenta;
- Zakonski i podzakonski akti moraju biti mnogo izraženi i oštriji u svim državama u cyber prostoru;

- Pored Tallinskog priručnika treba se dodatno napraviti istraživanje kako bi se napisao vodič koji bi se mogao koristiti kao objašnjenje cyber ratovanja, cyber prostora, cyber napada itd.;
- Dodatno obučiti i edukovati stručnjake koji će se baviti ovim prostorom uz rad u nepolitičkim uvjetima;

Bosna i Hercegovina treba donijeti adekvatne zakonske i podzakonske akte kako bi zaštitila svakog pojedinca, instituciju ili državu u cjelini od bilo kakvih cayber napada ili eventualnog rata.

SKRAĆENICE

NATO – (North Atlantic Treaty Organisation) Sjeveroatlanski savez

OSCE – (Organization for Security and Co-operation in Europe) Organizacija za sigurnost i saradnju Evrope

EU – Evropska Unija

SAD – Sjedinjene Američke Države

NCIRC - Computer Incident Response Capability

UN – Ujedinjeni narodi

KNI – Kritična nacionalna infrastruktura

FBI – (Federal Bureau of Investigation) Savezni istražni ured

CERT – (Computer Emergency Response Team)

OAD - Organizacija Američkih Država

SCO - Šangajska Organizacija za Suradnju

RS – Republika Srpska

RH – Republika Hrvatska

FBIH – Federacija Bosne i Hercegovine

EC3 - Europski centar za kibernetički kriminal

ENISA - agencija Europske unije za mrežnu i informacijsku sigurnost

CEPOL - agencija Europske unije za osposobljavanje u području izvršavanja zakonodavstva

ZKOS – Zajednička komisija za odbranu i sigurnost

NVO – Nevladine organizacije

BIBLIOGRAFIJA

1. Beridan, Izet Politika i sigurnost, Fakultet političkih nauka, Sarajevo, 2008.
2. Robić, T. *Cyber ratovanje,* Prirodno-matematički fakultet, Zagreb.2016.
3. Mario Nobilo, Pojam sigurnosti u terminologiji međunarodnih odnosa, Pol. Misao, Vol. XXV Zagreb 1988. str. 69.-80.
4. Direkcija za evropske integracije, Pojmovnik evropskih integracija Sarajevo,2010. str. 73.-74
5. Beridan I., Tomić I., Kreso M., Leksikon sigurnosti – Drugo izmjenjeno i dopunjeno izdanje, Sarajevo. 2001.
6. Carter, Trimble, Bradley International Law, forth edition. New York: Aspen Publisher. Dinstein, Y.: War, Agression and Self -Defence, Cambridge University Press, 1994. Str. 433.
7. Brownlie, J: International Law and the use Force by States, Oxford University Press 1963.
8. Ali, Idrees and Andrea Shalal. „F-35 Chief Cites 'Good, Bad and Ugly' About No. 1 U.S. Arms Program.“ Reuters, March 24, 2016.
9. Bertuglia, Cristoforo Sergio and Franco Vaio. Nonlinearity, Chaos & Complexity, the Dynamics of Natural and Social Systems. New York, NY: Oxford University Press, 2005.
10. Lind, Nightengale, Schmitt, Sutton, Wilson, "Changing Face of War",2001. str. 22.-26.
11. Organizacija Američkih Država, A comprehensive Inter – American Cybersecurity Strategy: A multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, Dodatak A, 2004

12. Hathaway, A. Oona, Crootof, Rebecca, Levitz Phillip, Nix Haley, Nowlan Aileen, Perdue, William, Spiegel, Julia. The Law of Cyber – Attack, SAD, 2012., str. 53.
13. Chawki, M. A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy. 2005
14. Scott Shackleford, članak iz 2009., „From nuclear War to Net War: Analogizing Cyber Attacks in International Law“, objavljeno u Berkeley Journal of International Law (BJIL), Vol 25 No 3. 2009.
15. S. Softić .Međunarodno pravo i cyber sigurnost. Pregledni naučni rad (Zbornik radova), godina XX broj 5. Univerzitet u Sarajevu, FKKSS. 2019.
16. Kazazić, V., Savić, M. Aktualna pitanja međunarodnopravnog subjektiviteta. Zbornik radova Pravnog fakulteta Sveučilišta u Mostaru br. XXVI., 2018., str. 92. – 110
17. Tallinn Manual on the international law applicable to cyber warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre od Excellence. General Editor: Michael N. Schmitt Cambridge University Press,2013.
18. Cvrtila, V., Države i međunarodna sigurnost, Polit. misao, Vol XXXIV, 1997., br. 3, str. 31.—43.
19. Dimitrijević, V. Pojam sigurnosti u međunarodnim odnosima. Beograd, Rad.
20. Vojin Dimitrijević, Obrad Račić, Vladimir Đerić, Tatjana Papić, Vesna Petrović, Saša Obradović, Osnovi međunarodnog javnog prava, Beograd 2005., str. 137–138.
21. Fluri, P., Johnsson, A. Parlamentarni nadzor nad sektorom sigurnosti: principi, mehanizmi i prakse. Interparlamentarna unija Centar za demokratsku kontrolu nad oru`anim snagama Verzija izdata u Sarajevu: Misija OSCE-a u Bosni i Hercegovini, 2003.
22. Šalić, B. Ujedinjeni narodi. Šibenik: Veleučilište u Šibeniku, Upravni studij. Završni rad, 2016.
23. Čukljaš, M. Organizacija sjevernoatlanskog ugovora NATO. Šibenik: Veleučilište u Šibeniku, Upravni studij. Završni rad, 2015
24. Hadžić Izet Demokratija, ljudska prava i slobode kao osnovne vrijednosti političkog sistema. Stručni rad ISSN 1512-5785 broj 35, 2015.
25. UN General Assembly. “A/RES/57/239, Creation of a global culture of cybersecurity”. 2003
26. Hamidović, H. Mjesto i uloga cayber sigurnosti u razvoju modernih društava. Sarajevo: Sarajevski žurnal za društvena pitanja, Vol. 4. Broj 1-2, 2015

27. Protrka, N. Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru. Doktorski rad, Zadar: Sveučilište u Zadru, 2008
28. Ravlić, S., Pluralizam i participacija..., Polit. misao, Vol XXXVII, 2000., br. 1, str. 84.—98.
29. Lukač, I. Uloga novih medija u informacijskom ratovanju. Osijek: Sveučilište Josipa Jurja Strossmayera. Diplomski rad, 2019.
30. Evropska komisija – Bosna i Hercegovina izvještaj o napretku u 2005. godini. Brisel: SEC, 2005.
31. Hadžović, D. Podnesak za Alternativno mišljenje i izvještaj za 2017. Parlamentarni nadzor nad sigurnosnim sektorom u Bosni i Hercegovini. Centar za sigurnosne studije, 2017.
32. Born, H. Parlamentarni nadzor nad sektorom sigurnosti, DCAF Fojnica: Svjetlost, 2003.
33. Tomić, R. Normativna polazišta za civilnu kontrolu vojske i policije. Beograd - Centar za civilno - vojne odnose. 2001
34. Dmitrović, T.. Izazovi civilnog društva u BiH, Analize i preporuke za politike. Sarajevo, 2010. http://www.sif.ba/dok/1386600343.pdf.
35. Kralj, Ž. Unutarnja kontrola i nadzor policije. Stručni članak (Zagreb), godina 23. 2014, broj 1., str. 73.-81.
36. Musić, E. Opšti okviri kontrole obavještajno – sigurnosnih službi od strane izvršne vlasti. Zenica: Pravni fakultet Univerziteta u Zenici, Vol. 8 Issue 4, p287-307. 21p, 2011.
37. Sigurnosna politika Bosne i Hercegovine, Predsjedništvo Bosne i Hercegovine, Sarajevo 2006.

Normativno – pravni dokumenti

1. Krivični zakon Federacije Bosne i Hercegovine Službene novine Federacije BiH, br. 36/2003, 21/2004. ispr. 69/2004. 18/2015. gl. XXXII
2. Zakon o odbrani Bosne i Hercegovine (2005.) (http://www.mod.gov.ba/files/file/zakoni/Zakon-o-odbrani-bs.pdf)

Internetski izvori

1. Oficijalna stranica NATO-a Cyber Defence https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

2. Parlamentarna skupština BiH https://www.parlament.ba/Content/Read/25?title=FunkcijeParlamentarneskup%20tine BiH
3. OSCE (Sarajevo 2019.) https://www.osce.org/bs/mission-to-bosnia-and-herzegovina
4. MIŠLJENJE O NACRTU ZAKONA O PARLAMENTARNOM NADZORU U BOSNI I HERCEGOVINI https://www.osce.org/files/f/documents/6/5/322431.pdf
5. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf
6. CRS Report for Congress, Cyberwarfare, Steven A. Hildreth, http://www.fas.org/irp/crs/RL30735.pdf
7. International Committee of the Red Cross (ICRC). War and international humanitarian law. URL: https://www.icrc.org/eng/war-and-law/overview-war-and-law.htm
8. Oficijalna stranica UN-a www.un.org
9. Oficijalna stranica NATO-a www.nato.int
10. Oficijalna stranica Web portala www.coe.int/en/web/portal
11. Oficijalna stranica OSCE-a www.osce.org
12. Misija u Bosni i Hercegovini, Odjel za sigurnosnu saradnju. Sarajevo, 2007. godine. http://www.mfa.gov.ba/HTML/Bos/Multilaterala/OSCE-Kodeks-Ponasanja.pdf OSCE
13. Oficijalna stranica EU www.europa.eu
14. Oficijalna stranica EU https://europa.eu/european-union/topics/humanitarian-aid-civil-protection_hr
15. Oficijalna stranica EU https://op.europa.eu/webpub/com/eu-what-it-is/hr/#chapter2_17
16. Oficijelna stranica EU https://hr.wikisource.org/wiki/Povelja_Ujedinjenih_naroda
17. ENISA - European Network and Information Security Agency europa.eu. (https://europa.eu/european-union/about-eu/agencies/enisa_hr)
18. Rufferty, I., 2017., How Communication Has Evolved With The New Technologies. (https://medium.com/bsg-sms/how-communication-has-evolved-with-the-new-technologies-52ee1ca114f)
19. Strukture upravljanja državom Bosnom i Hercegovinom, Izdavač: Vanjskopolitička inicijativa BH (http://vpi.ba/wp-content/uploads/2016/05/Struktura_upravljanja_drzavom_u_BiH.pdf)
20. Mišljenje o nacrtu zakona o parlamentarnom nadzoru u Bosni i Hercegovini, na osnovu nezvaničnog engleskog prevoda Nacrta zakona koji je osigurala Misija OSCE-

a u Bosni i Hercegovini (2017.) Ured OSCE-a za demokratske institucije i ljudska prava. https://www.osce.org/files/f/documents/6/5/322431.pdf

21. Obavještajno-sigurnosna agencija Bosne i Hercegovine (http://www.osa-oba.gov.ba/nadlb.html)
22. Parlamentarna skupština BiH - zajednička komisija za odbranu i sigurnost BiH (https://www.parlament.ba/Publication/Read/3602?title=zajednicka-komisija-za-odbranu-i-sigurnost-bih&pageId=239)

Naziv odsjeka i/ili katedre: _____
Predmet: _____

IZJAVA O AUTENTIČNOSTI RADOVA

Ime i prezime: _____
Naslov rada: _____
Vrsta rada: _____
Broj stranica: _____

Potvrđujem:

- da sam pročitao/la dokumente koji se odnose na plagijarizam, kako je to definirano Statutom Univerziteta u Sarajevu, Etičkim kodeksom Univerziteta u Sarajevu i pravilima studiranja koja se odnose na I i II ciklus studija, integrirani studijski program I i II ciklusa i III ciklus studija na Univerzitetu u Sarajevu, kao i uputama o plagijarizmu navedenim na web stranici Univerziteta u Sarajevu;
- da sam svjestan/na univerzitetskih disciplinskih pravila koja se tiču plagijarizma;
- da je rad koji predajem potpuno moj, samostalni rad, osim u dijelovima gdje je to naznačeno;
- da rad nije predat, u cjelini ili djelimično, za stjecanje zvanja na Univerzitetu u Sarajevu ili nekoj drugoj visokoškolskoj ustanovi;
- da sam jasno naznačio/la prisustvo citiranog ili parafraziranog materijala i da sam se referirao/la na sve izvore;
- da sam dosljedno naveo/la korištene i citirane izvore ili bibliografiju po nekom od preporučenih stilova citiranja, sa navođenjem potpune reference koja obuhvata potpuni bibliografski opis korištenog i citiranog izvora;
- da sam odgovarajuće naznačio/la svaku pomoć koju sam dobio/la pored pomoći mentora/ice i akademskih tutora/ica.

Mjesto, datum **Potpis**

_____ _____