UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Jaka Zabukovec

Slovenija in zagotavljanje globalnega javnega dobra

Diplomsko delo

Ljubljana, 2015

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Jaka Zabukovec

Mentor: izr. prof. dr. Iztok Prezelj

Somentor: doc. dr. Erik Kopač

Slovenija in zagotavljanje globalnega javnega dobra

Diplomsko delo

Ljubljana, 2015

Slovenija in zagotavljanje globalnega javnega dobra

Zveza Nato je vse od nastanka leta 1949 do danes ohranila poglavitno nalogo kolektivne obrambe. Po koncu hladne vojne je področje svoje dejavnosti razširila še na področje kriznega upravljanja in sodelovanja. Te temeljne naloge bodo ostale nespremenjene tudi v prihodnosti, a hkrati se je pred leti zveza Nato začela ozirati na področje, ki je vse bolj aktualno za doseganje njenih ciljev. Gre za zagotavljanje uporabe in dostopa do globalnega javnega dobra. Globalna javna dobra so področja morij, zraka, vesolja in kibernetskega prostora, ki niso v nikogaršnji lasti in so dostopna vsem. Dostop in uporaba teh področij je ključnega pomena za delovanje zveze Nato, zato je zveza Nato že začela raziskovati svojo vlogo na tem področju in sprejemati ukrepe za zagotavljanje nemotene uporabe in dostopa do teh območij. Slovenija kot polnopravna članica zveze Nato je kot taka vpeta v dejavnosti zveze Nato in ima tako tudi sama določeno vlogo pri zagotavljanju dostopa in uporabe globalnih javnih dober, izvaja pa tudi dejavnosti na tem področju izven zveze Nato.

KLJUČNE BESEDE: Nato, globalna javna dobra.

Slovenia and assured access to global commons

Nato has kept its core task of collective security as its main objective since its establishment in 1949. After the end of the Cold war period, Nato has extended its objectives to crisis management and cooperation. These core tasks of the alliance will remain unchanged in the future, though Nato has started to build up interest in the area closely related to its ability to perform those tasks. We are talking about assured access to global commons. Global commons comprise of seas, air, space and cyberspace, which are owned by no one and are available for use to everyone. Assured access to these areas is of vital significance to the activities of Nato, therefore the alliance has already started to examine its role and started taking first measures to provide this assured access. Slovenia as a fulltime member of Nato is also a part of its activities and therefore plays a certain role, while also conducting activities to provide assured access to global commons on its own.

KEY WORDS: Nato, Global commons.

KAZALO

1 UVOD

Zveza Nato je bila ustanovljena z namenom zagotavljanja kolektivne varnosti članic v luči ogrožanja s strani Sovjetske zveze in ostalih članic Varšavskega sporazuma. S koncem bipolarne delitve na začetku 90. let prejšnjega stoletja je izginila tudi glavna nevarnost zaradi katere je bila zveza Nato ustanovljena. Mnogi so že takrat pričakovali postopno zmanjševanje vloge zveze Nato in njen postopni razpad. V tistem času je zveza Nato s preoblikovanjem strateških konceptov našla razširjeno vlogo v novem mednarodnem okolju s poudarjanjem sodelovanja z bivšimi nasprotniki, nadaljnjim zagotavljanjem vojaške zaščite državam članicam in vlogo krepitve varnosti in stabilnosti v Evropi (Yost 1998, 270). Nato je sledilo obdobje širitve zavezništva s svojo politiko odprtosti za nove članice. Na prelomu tisočletja je zveza Nato sprejela nov strateški koncept (leta 1999 v Washingtonu), ki je dodal dve novi nalogi zavezništva: krizno upravljanje in partnerstvo. Tako je zveza Nato razširila spekter svojega delovanja tudi na operacije, ki so bile izven določil 5. člena Severnoatlantske pogodbe. Po letu 2001 in terorističnemu napadu na Združene države Amerike je zavezništvo sprejelo tudi vrsto ukrepov za boj proti terorizmu. Zveza Nato deluje na globalni ravni s svojimi mirovnimi operacijami in kriznim upravljanjem. Po hladni vojni je zveza Nato posredovala na Balkanu in še danes pomaga pri reševanju kompleksnega problema varnosti na območju nekdanje Jugoslavije, po letu 2001 in terorističnem napadu na ZDA pa se je območje interesov in dejavnosti zveze Nato na območjih izven meja članic močno razširilo. Leta 2003 je zveza Nato začela z delovanjem v Afganistanu, kar je predstavljalo prvi poseg zavezništva izven območja Evrope (Vegič 2005, 181–196). Zveza Nato že dalj časa aktivno deluje tudi na območju Sredozemskega morja (operacija Active Endeavour) in na območju Indijskega oceana (operacija Ocean Shield). Pri svojih dejavnostih sodeluje tako z mednarodnimi organizacijami kot tudi z državami nečlanicami. V zadnjih letih je zelo pomemben vidik delovanja sodelovanje z Evropsko unijo (EU). Z najnovejšim strateškim konceptom iz leta 2010, sprejemom kasnejših področnih politik in na zasedanjih vrha zveze Nato od leta 2010 naprej (Lizbona, Chicago, Wales), pa je zveza Nato usmerila svojo pozornost k nekoliko širšemu konceptu, in sicer zagotavljanju dostopa in uporabe globalnega javnega dobra. Osrednje naloge ostajajo enake, vendar pa se veča zavedanje, da je za zagotavljanje varnosti in blaginje danes pomemben nemoten dostop in uporaba teh področij.

Globalna javna dobra so področja, ki so namenjena vsem državama na svetu, niso v nikogaršnji lasti in niso pod oblastjo nobene države. Gre za skupna dobra, ki jih v grobem lahko razdelimo na morja, zrak, vesolje in kibernetski prostor in so vitalnega pomena za mednarodno varnost in trgovino. Nemoten dostop in uporaba teh domen sta za zvezo Nato ključnega pomena, ker preko njih zveza Nato opravlja svoje temeljne naloge, dosega zastavljene cilje in skrbi za varnost držav članic. V preteklosti je bil dostop do teh domen bolj ali manj samoumeven, v sodobnem času pa se je zaradi globalizacije, hitrega razvoja tehnologij in pojava novih sovražnikov pojavilo mnogo virov ogrožanja, ki imajo sposobnost na takšen ali drugačen način ovirati dostop do teh domen (Allied Command Transformation 2011, IX). Primeri ogrožanja so piratstvo in teroristična dejavnost na morju, pojav učinkovitih tehnologij za motenje signalov v vesolju, poceni in dostopna učinkovita protiletalska orožja in razvoj škodljivih programskih kod v kibernetskem prostoru. Ker je zveza Nato močno odvisna od vseh štirih domen, je zelo pomembno, da identificira področja in vire ogrožanja, vzpostavi konkretne mehanizme za obrambo pred grožnjami ter da oceni svojo vlogo v prihodnosti na področju zagotavljanja dostopa in uporabe globalnega javnega dobra.

Tudi Slovenija je danes močno vpeta v globalizacijske procese in kot taka ni imuna na grožnje, ki prihajajo iz teh domen oziroma ogrožajo njihovo nemoteno uporabo, zato me poleg vloge zveze Nato zanima tudi vloga Slovenije, predvsem v okviru zavezništva in pa tudi kot samostojnega akterja v mednarodni skupnosti.

2 METODOLOŠKI OKVIR

2.1 Cilj in namen diplomskega dela

Cilj diplomskega dela bo preučevati vpliv globalnih javnih dober v današnjem mednarodnem varnostnem okolju in vlogo zveze NATO ter Slovenije pri zagotavljanju dostopa in uporabe globalnih javnih dober. Preučili bomo pomorsko, zračno, vesoljsko in kibernetsko komponento globalnih javnih dober, vlogo posamezne komponente za zvezo NATO, in na kakšen način se zveza NATO in znotraj nje Slovenija trudita zagotavljati prost dostop in uporabo vsake od komponent. Preučil bom kakšni izzivi čakajo zvezo NATO in Slovenijo na morju, v zraku, vesolju ter kibernetskem prostoru.

2.2 Raziskovalni vprašanji

- Kakšna je vloga zveze Nato pri zagotavljanju dostopa in uporabe globalnega javnega dobra?

- Kakšna je vloga Slovenije znotraj zveze Nato in kako lahko prispeva izven zveze Nato pri zagotavljanju dostopa in uporabe globalnega javnega dobra?

2.3 Uporabljena metodologija

Za dosego cilja bom uporabil različne družboslovne metode raziskovanja. Uporabil bom metodo analize in interpretacije pisnih virov. S to metodo bom analiziral primarne in sekundarne vire, ki jih bom dobil s pomočjo domače in tuje strokovne literature in preko spleta. Za opis obravnavane teme diplomske naloge bom uporabil diskriptivno metodo.

2.4 Zgradba diplomske naloge

Diplomsko delo je sestavljeno iz treh delov. V prvem delu je uvod, kjer je na kratko predstavljena tema diplomske naloge, sledi mu metodološki okvir, ki vsebuje raziskovalni vprašanji in metodologijo uporabljeno za izdelavo diplomske naloge. Prvi del se konča z obrazložitvijo temeljnih pojmov, potrebnih za razumevanje tematike diplomske naloge.

V drugem, osrednjem delu je predstavljena glavna tema diplomske naloge. Na začetku je opisana povezava zveze Nato z globalnim javnim dobrim, vizija, cilji in dejavnosti zveze Nato na tem področju. Temu delu sledi še vloga Slovenije na področju zagotavljanja dostopa in uporabe globalnih javnih dober. Tretji del pa predstavlja zaključek, kjer sem strnil pridobljene podatke, povzel svoje ugotovite in tako odgovoril na raziskovalni vprašanji. Zaključku sledi še seznam uporabljene literature.

2.5 Temeljni pojmi

2.5.1 Nato

Organizacija Severnoatlantske pogodbe (North Atlantic Treaty Organization) je vojaška in politična zveza 28 držav članic Evrope in Severne Amerike, katere glavni cilj je zagotavljanje svobode in varnosti držav članic. Te cilje organizacija dosega s političnimi in vojaškimi sredstvi, ki so v skladu z Ustanovno listino Združenih narodov (UL ZN) in s Severnoatlantsko pogodbo, ki je bila podpisana 4. aprila 1949 v Washingtonu (Slovenija in Nato 2015).

Temeljne naloge zavezništva za doseganje svojih osnovnih ciljev so (Slovenija in Nato 2015):

- varnost: zagotoviti temelj za stabilno varnostno okolje, ki temelji na demokratičnih institucijah in zavezanosti k mirnemu reševanju sporov,
- posvetovanje: skladno s 4. členom Washingtonske pogodbe delovati kot osnovni čezatlantski forum za razprave in posvete zaveznic o ključnih vprašanjih, ki se

nanašajo na njihove interese in varnost ter za usklajevanje njihovih prizadevanj na skupnih interesnih področjih,

- odvračanje in obramba: odvračati in braniti se pred vsako grožnjo agresije proti katerikoli članici zveze, kot predvidevata 5. in 6. člen Washingtonske pogodbe,

- obvladovanje kriznih razmer: pripravljenost prispevati k učinkovitemu preprečevanju konfliktov in k aktivnemu vključevanju v obvladovanje kriznih razmer, vključno z operacijami za odzivanje na krizne razmere, na podlagi konsenza v skladu s 7. členom Washingtonske pogodbe,

- partnerstvo: Spodbujati partnerstvo, povezovanje, sodelovanje in dialog z ostalimi državami na evro-atlantskem območju in širše z namenom izboljšati preglednost, vzajemno zaupanje in sposobnost za skupno ukrepanje z zavezništvom.

Zveza Nato ostaja medvladna organizacija, kjer vsaka država ohranja svojo suverenost, vse odločitve zavezništva pa so sprejete skupno na podlagi konsenza članic. Najpomembnejše odločevalno telo v zavezništvu je Severnoatlantski svet (North Atlantic Council), ki združuje predstavnike vseh držav članic na ravni veleposlanikov, ministrov, predsednikov vlad in držav. Glas vsake države članice je enakovreden, ne glede na njeno velikost ali politično, gospodarsko in vojaško moč (Nato Handbook 2006, 15).

Primarna naloga zveze Nato vse od ustanovitve leta 1949 do danes je kolektivna obramba držav članic, njena organizacija pa se je spreminjala glede na potrebe in zahteve članic ter glede na pojav novih morebitnih oblik in virov ogrožanja. Čeprav ob podpisu Severnoatlantske pogodbe v njej ni bil omenjen noben sovražnik, vemo, da je zavezništvo nastalo primarno zaradi skupne grožnje varnosti članic, ki so jo predstavljali Sovjetska zveza in njeni zavezniki znotraj Varšavskega sporazuma. To zaznavanje skupne ogroženosti se je po koncu hladne vojne bistveno spremenila zaradi razpada Varšavskega sporazuma, Sovjetske zveze in drugih večnacionalnih držav ter s koncem bipolarnega sistema v mednarodnih odnosih (Grizold 2005, 83). Tako je zveza Nato vse od konca hladne vojne pa do danes v postopku bolj ali manj intenzivne transformacije, katere namen je doseganje ustreznih zmožnosti za zagotavljanje varnosti v luči novih oblik ogrožanj. Terorizem, etnični konflikti, piratstvo, širjenje orožij za množično uničevanje, politične in gospodarske nestabilnosti in druge grožnje silijo zvezo Nato v nenehen razvoj tako strategij, doktrin in pravil, kot tudi razvoj bojnih in ostalih kapacitet.

Slovenija je članica zveze Nato od 29. marca 2004. S polnopravnim članstvom je Slovenija dobila možnost sodelovanja na znanstvenem, tehnološkem, informacijskem, ekonomskem in vojaškem področju najbolj razvitih držav. Poleg tega je Slovenija dobila tudi določene obveznosti, ki jih opredeljuje Severnoatlantska pogodba. Gre za posamičen in kolektivni razvoj lastnih obrambnih sil kot temelj kolektivne obrambe. Članice so prav tako dolžne spoštovati skupno sprejeta načela ter politiko in postopke za njihovo uresničevanje. Slovenija se kot članica zveze Nato čim bolj aktivno vključuje v njene dejavnosti (Slovenija in Nato 2015).

2.5.2 Globalna javna dobra

Globalna javna dobra (Global Commons) najlažje opišemo kot naravna ali umetna okolja, za katera je značilno, da niso v lasti nobene države in so hkrati skupna vsem državam sveta. »Fizična javna dobra. Štiri okolja, fizično ogromna in še vedno slabo raziskana, po mednarodnem pravu in običajih sestavljajo globalna javna dobra. So geofizično in biokemično soodvisna in povezana med sabo, hkrati pa ima vsak svojo zgodovino odnosov s človeštvom« (Cleveland 1990, 1). V najbolj osnovni in splošni razdelitvi govorimo o mednarodnih vodah, mednarodnem zračnem prostoru in vesolju; nekateri med globalna javna dobra prištevajo tudi obe polarni regiji (medtem, ko jih nekateri uvrščajo znotraj domene mednarodnih voda). V sodobnem času med globalna javna dobra štejemo tudi kibernetski prostor, ki po vseh merilih ustreza definiciji in postaja vsakodnevno bolj pomemben dejavnik v našem življenju. »Po definiciji ameriškega Ministrstva za obrambo so globalna javna dobra sestavljena iz geografskih in virtualnih domen »vesolja, mednarodnih voda, mednarodnega zračnega prostora in kibernetskega prostora«. So izvleček širše pomorske, letalske, vesoljske in kibernetske domene, katerih obstoj izhaja iz ideje prostorov, ki so dostopni vsem, ampak niso v lasti nikogar« (Redden in Hughes 2011, 1).

Tudi zveza Nato (Allied Command Transformation 2011, XII) opredeli globalna javna dobra na enak način:

> *Globalna javna dobra so sestavljena iz štirih domen: pomorske, zračne, vesoljske in kibernetske. Pomorsko in zračno sestavljajo mednarodni oceani in mednarodni zračni prostor, ki ne spadata pod oblast nobene države. Vesolje se začne na točki nad zemljo,*

kjer predmeti ostanejo na orbiti, medtem ko je kibernetski prostor v Natovem konceptu kibernetske obrambe definiran kot »digitalni svet ustvarjen z računalniškimi mrežami, kjer ljudje in računalniki sobivajo in ki vključuje vse vidike spletne aktivnosti«.

2.5.2.1 Pomorska domena

Morja kot globalna javna dobra so najstarejša in najbolje razumljena domena, saj jih človeštvo že tisočletja uporablja za trgovanje in osvajanje ozemelj. Oceani prekrivajo skoraj 70 odstotkov zemljine površine. Področje svetovnih oceanov najbolje ureja Konvencija Združenih narodov o pomorskem pravu (UNCLOS), ki je stopila v veljavo leta 1994. UNCLOS ureja pravice in dolžnosti držav glede na njihovo rabo svetovnih oceanov in tako določa smernice za koriščenje, uporabo in upravljanje z morskimi viri (United Nations Convention on the Law of the Sea).

V preteklosti je bilo skoraj celotno področje izven sodnih oblasti držav. UNCLOS pa je uveljavila ekskluzivna ekonomska območja. To so morska območja, kjer ima država posebne pravice, kar se tiče raziskovanja in izrabe virov. Tako je dovoljeno obalnim državam, da razširijo svojo oblast nad morskim dnom in vodami do 200, oziroma izjemoma do 350 navtičnih milj od obale. Kljub tej ureditvi pa še vedno več kot dve tretjini oceanov ne spadata pod oblast nobene od držav (Kaye 2007, 2).

Grožnje, ki izhajajo iz pomorske domene, lahko razdelimo na dva dela. Na eni je ogrožanje proti pristaniščem in ozemlju obalnih držav, ki izvirajo iz morja, na drugi strani pa imamo grožnje dejavnostim, ki se izvajajo znotraj pomorske domene.

Pri prvih gre za prenos orožij za množično uničevanje in drugih orožij v pristanišča za uporabo proti tej državi ali njenim zaveznicam ali za uporabo plovil za neposreden napad, bodisi iz vojaškega plovila ali ugrabljenega komercialnega plovila. Napad takšne vrste se na Zahodu še ni zgodil, bilo pa je že več primerov takšnih napadov na Bližnjem vzhodu s ciljem škodovati zahodnim interesom[1] (Kaye 2007, 3–5).

Drugi del pa predstavljajo grožnje dejavnostim v pomorski domeni. Te dejavnosti vključujejo transport, izkoriščanje zemeljskih plinov in nafte ter komunikacije prek podmorskih kablov.

[1] Nedaven primer so iranske pomorske aktivnosti v Perzijskem zalivu, vključno z napadom na singapurski tanker (Hafezi 2015).

Pri teh grožnjah prednjači pomorsko piratstvo[2]. UNCLOS na tem področju zelo dobro ureja obstoječe obče mednarodno pravo in zagotavlja univerzalno jurisdikcijo nad plovili, udeleženimi v piratstvu. Poleg napadov na plovila pa so grožnja tudi napadi na druge objekte na morju. Tu je govora predvsem o velikem številu naftnih ploščadi v mednarodnih vodah, ki bi lahko bile tarča za morebitne teroristične napade. Poleg ploščadi zelo pomemben del predstavljajo tudi podmorski kabli in plinovodi. Napadi na plinovode bi lahko imeli velike posledice, od višanja cen nafte in zemeljskega plina na svetovnih trgih do velikih okoljskih katastrof ob izlivu. Napadi na podmorsko komunikacijsko infrastrukturo pa bi lahko povzročili velike motnje v telekomunikacijskih omrežjih po vsem svetu, saj podmorski kabli (predvsem optični) prenašajo večino svetovnih telefonskih in elektronskih podatkov (Kaye 2007, 6–8).

2.5.2.2 Zračna domena

Zračno domeno kot globalno javno dobro lahko obravnavamo z dveh vidikov. Nanjo lahko gledamo kot na podnebje in vreme ali pa z vidika uporabe.

Tako vreme kot podnebje nista v lasti nobene države. Obstajajo določeni načini za kratkoročno vplivanje na vreme, vendar to še ni pripeljalo do kakršnegakoli mednarodnega konflikta. Onesnaženost zraka pa je že »krivec za mednarodne konflikte (kisel dež), mednarodno sodelovanje (za preprečitev nadaljnje škode plastem ozona) in mednarodno skrb (o učinku tople grede, ki ga ustvarjajo plini v ozračju, ki so rezultat človeških dejanj)« (Cleveland 1990, 3). Onesnaženost zraka je eden od problemov upravljanja z globalnim javnim dobrim. Onesnaževalci so lahko trdi delci, kapljice ali plini, ki so ali naravni ali rezultat človeških dejanj. Na tem področju je bilo uveljavljenih več ukrepov, ki bi pripomogli k zmanjšanju onesnaženosti zraka. Močno podporo v evropski skupnosti in pri državah Organizacije za ekonomsko sodelovanje in razvoj (OECD) ima tako imenovana »razširjena odgovornost proizvajalca«. Pri tem gre za to, da je proizvajalec, ki onesnažuje okolje, odgovoren za plačilo škode, ki jo je s tem povzročil (OECD 2015). Omeniti velja tudi Konvencijo o dolgoročni čezmejni onesnaženosti zraka iz leta 1979, ki je eden zgodnejših poskusov mednarodne skupnosti, da postopno zmanjša in prepreči onesnaževanje zraka in

[2] Pomorsko piratstvo je kriminalna dejavnost, ki ima dva kazniva elementa: rop, kjer je cilj ukrasti plovilo ali njegov tovor in ugrabitev, kjer se ugrabi tudi posadko dokler se ne plača odkupnina (UNODC, 2015).

Protokol o snoveh, ki izčrpavajo ozonski plašč iz Montreala, ki je stopil v veljavo leta 1989. Poleg onesnaževanja zraka je tu še globalno »zamegljevanje«, ki nastaja zaradi povečanja trdnih delcev, še posebej sulfatnih aerosolov v ozračju zaradi človeških dejanj. Omeniti velja tudi Kjotski protokol, ki je mednarodna okoljska pogodba, ki postavlja zavezujoče naloge industrializiranim državam, da zmanjšajo emisije toplogrednih plinov. Trenutno je 192 podpisnic, od tega 191 držav in EU, vendar pa je niso vse podpisnice tudi ratificirale (Henson 2006, 15–6).

Drug vidik zračne domene kot globalnega javnega dobra pa je skozi uporabo le tega. Čeprav smo ljudje sposobni izkoriščati zračni prostor v namene trgovine in transporta šele dobro stoletje[3], pa je mednarodni zračni prostor eden ključnih elementov današnje globalne ekonomije. »Komercialna letala so leta 2010 prepeljala več kot 2 milijardi ljudi na skupno več kot 20 milijonih letih. Istočasno rastoča letalska industrija prevoza tovora danes prepelje več kot 35 odstotkov svetovnih proizvodnih izdelkov glede na njihovo vrednost. Po ocenah naj bi več kot 30 milijonov ljudi po vsem svetu danes posredno ali neposredno živelo od industrije zračnega transporta« (Allied Command Transformation 2011, 14).

Pomembna podlaga za konvencije, ki urejajo uporabo zračnega prostora, je ponovno UNCLOS. Tako kot pri morski domeni, ima država suverenost nad svojim državnim zračnim prostorom, ki je nad državnim ozemljem, notranjimi vodami, arhipelaškimi vodami in nad teritorialnim morjem, medtem ko je mednarodni zračni prostor odprt za vse. Velik mejnik v regulaciji zračnega prostora predstavlja Konvencija o mednarodnem civilnem letalstvu iz leta 1944, v kateri so države vzpostavile osnovne letalske standarde za opremo in urjenje, vzpostavile globalni pravni režim in norme, ki omogočajo udejstvovanje in dostop do zračnega prostora (Allied Command Transformation 2011, 14–5).

2.5.2.3 Vesolje

V vesolju za razliko od oceanov in ozračja noben del ne spada pod nikogaršnjo oblast. Pravico dostopa do vesolja imajo vsi, ki imajo sredstva, da ga dosežejo. Prav tako imajo vsi pravico do njegove uporabe. Najpomembnejši dokument na tem področju je Vesoljska

[3] Čeprav je ideja o letenju in letečih napravah stara že več stoletij, sta prvi polet z motornim letalom opravila brata Orville leta 1903 (Nasa, 2014).

pogodba (Open Space Treaty), ki ponuja okvir za mednarodno vesoljsko pravo. Ureja zakonsko področje uporabe vesolja s strani držav. Poleg tega tudi izrecno prepoveduje pošiljanje atomskega orožja v vesolje. V zadnjih desetletjih smo bili priča hitremu razvoju vesoljske tehnologije, nenehnim odkritjem v astronomiji in digitalni revoluciji v kibernetskem prostoru. Tako imamo danes več kot tisoč satelitov, ki krožijo okrog zemlje in zbirajo, oddajajo in prenašajo informacije, kot so telekomunikacije, meteorološko slikovno gradivo in obveščevalne podatke, ki so uporabni tako v komercialne kot v varnostne namene. Vesoljska domena v povezavi s kibernetskim prostorom predstavlja zelo pomemben del globalne mreže trgovine in informacij. Tako zračni, pomorski, kot kopenski promet so danes odvisni od globalnega sistema pozicioniranja (GPS). Svetovna dobavna veriga je odvisna od telekomunikacij in GPS podatkov satelitskih sistemov. Danes se vse civilne, kot tudi vojaške operacije pri svojem delovanju opirajo na uporabo vesolja v navezi s kibernetskim prostorom, predvsem za povečanje varnosti, na vojaškem področju pa tudi za povečanje učinkovitosti samih vojaških operacij in aktivnosti. Vesolje danes predstavlja enega ključnih dejavnikov na gospodarskem področju in področjih vojaškega poveljevanja in kontrole, operacij in logistike (Allied Command Transformation 2011, 22).

2.5.2.4 Kibernetski prostor

Kibernetski prostor je domena, ki sama po sebi ne zaseda fizičnega prostora, kot ga ostale tri. Do danes ne obstaja ena univerzalno sprejeta definicija kibernetskega prostora. V ožjem smislu bi lahko rekli, da gre za elektromagnetni prostor, prek katerega potujejo digitalne informacije. V širšem smislu pa kibernetski prostor zajema tudi samo digitalno informacijo, celoten sistem kablov, satelitskih telekomunikacij na zemlji, računalnikov, mrež strežnikov in predvsem internet, ki zagotavlja uporabnost celotnega spektra. Bolj kot pri drugih domenah, kibernetski prostor gledamo skozi način uporabe, kar za večino predstavljata internet in svetovni splet (Allied Command Transformation 2011, 34). Talinski priročnik (Schmitt 2013, 15) definira kibernetski prostor, kot »okolje formirano prek fizičnih in nefizičnih komponent, za katerega je značilna uporaba računalnikov in elektromagnetnega spektra z namenom hranjenja, spreminjanja in izmenjave podatkov prek uporabe računalniških mrež«.

Internet je mednarodna mreža strežnikov, prek katere se pošiljajo digitalne informacije iz enega naslova na drugega. Ustvarjen je bil v vojaške namene v 60. letih prejšnjega stoletja.

Svetovni splet pa je izumil neki britanski inženir programske opreme kot sredstvo za zbiranje informacij, ki se jih nato naloži na »splet«. Dostop do teh informacij na spletu pa je bil omogočen s sočasnim razvojem brskalnikov (Allied Command Transformation 2011, 34).

> *Od leta 2003 do leta 2009, se je uporaba interneta na globalni ravni letno povečala za 290 odstotkov. Trenutno ima dostop do interneta okrog 1.8 milijarde ljudi, kar je približno četrtina svetovne populacije. V razvitih državah je do leta 2009 internet dosegel skoraj dve tretjini prebivalstva, v razvijajočih se državah pa le okrog 18 odstotkov (in samo 14 odstotkov na Kitajskem, ki ima zelo restriktivno politiko dostopa do interneta). Bolj kot postaja razviti svet povezan, bolj bo dostop do kibernetske domene pomemben tudi za razvijajoče se države* (Allied Command Transformation 2011, 35).

3 NATO IN GLOBALNA JAVNA DOBRA

3.1 Nato in pomorska domena

Danes mnogi smatrajo pomorsko domeno kot obtočni sistem globalizacije. Več kot 70 odstotkov Zemlje pokriva voda, približno 80 odstotkov svetovnega prebivalstva živi znotraj 160 kilometrov od obale, okrog 85 odstotkov vseh surovin in blaga je danes prepeljano med državami po morju in več kot tri četrtine tega tovora na neki točki potuje skozi mednarodne točke zgostitve, kot so prekopi in ožine. Vsa transportna in distribucijska omrežja v pomorski domeni so zelo ranljiva in dovzetna za motnje, kar bi imelo resne posledice za mednarodno trgovino in posledično za gospodarstva držav članic zveze Nato in njihovo blaginjo ter varnost. Poleg tega so morja pomemben vir hrane in surovin. Klimatske spremembe imajo potencialno velike varnostne posledice; taljenje arktičnega ledu prinaša nove potencialne morske poti in izboljšan dostop do morskih surovin na celotnih obalnih policah Azije, Evrope in Severne Amerike. Svetovni oceani in morja istočasno postajajo vse bolj privlačna okolja za mednarodni kriminal in teroristične dejavnosti. Največji grožnji sta transport orožij za množično uničevanje in podobnih sredstev ter kriminalna dejavnost, predvsem vse večji obseg piratskih napadov. Treba se je zavedati, da pomorska domena ne pomeni samo ladij in

pristanišč. Današnja zmožnost prenosa informacij, ukazov, nadzora, poizvedovanja, navigacije je poleg vesoljske mreže satelitov odvisna tudi od medcelinskih podmorskih kablov (Alliance Maritime Strategy; Allied Command Transformation, 4–6).

Vse to so dejavniki, ki od zveze Nato danes zahtevajo močno prisotnost sil na morju, izdelano strategijo odvračanja, kooperativno varnost skozi partnerstva, dialog in sodelovanje. Zveza Nato je tako kot že v preteklosti tudi na zasedanju vrha v Walesu leta 2014 v zaključni deklaraciji izpostavila pomembnost pomorske domene za zvezo. Predvsem je poudarila pomembnost okrepitve pomorskih zmogljivosti. Na ta način se je zavezala k pospešeni implementaciji najnovejše pomorske strategije in ponovni okrepitvi stalnih mornariških sil zveze Nato, tako da se njihova sestava in prispevek zaveznic naredi bolj fleksibilen in poveča njihova izobrazba in usposobljenost. Prav tako so poudarili pomen sodelovanja z drugimi pomembnimi mednarodnimi organizacijami in partnerskimi ter drugimi državami na področju pomorske domene (Nato, 2014b).

3.1.1 Pomorska strategija zveze Nato

V odgovor na sodobne grožnje v pomorski domeni je zveza Nato leta 2011 sprejela Zavezniško pomorsko strategijo. S to strategijo je zveza Nato v skladu z najnovejšim strateškim konceptom iz leta 2010 začrtala smeri in načine, kako lahko njene pomorske sile in kapacitete pomagajo pri reševanju kritičnih varnostnih izzivov. Strategija opredeljuje štiri temeljna področja, na katerih lahko pomorske sile prispevajo k varnosti. Prva tri so, kot jih navaja že strateški koncept, »temeljne naloge« zavezništva: odvračanje in kolektivna obramba, krizno upravljanje in kooperativna varnost skozi partnerstva, dialog in sodelovanje. Pomorska strategija pa kot četrto področje dodaja pomorsko varnost (Nato, 2015g).

Zveza Nato bo zagotavljala kolektivno obrambo s svojimi pomorskimi zmožnostmi in fleksibilnimi pomorskimi silami, kar je ključno pri odvračanju agresije. Tako bo prispevek pomorskih sil na tem področju vseboval (Nato, 2011a):

a) nadaljnjo podporo pri jedrskem odvračanju v skladu s strateškim načrtom,

b) zmožnost hitro dostaviti odločilno silo proti kateremukoli nasprotniku s širokim naborom konvencionalnih možnosti za hitro odzivanje na podlagi superiornih pomorskih, amfibijskih in zračnih sil,

c) ohranjanje zmožnosti za premestitev, vzdrževanje in podporo učinkovitim ekspedicijskim silam prek nadzora nad logističnimi potmi, ohranjanjem svobode plovbe in učinkovitimi protiminskimi dejavnostmi.

Pomorske sile zveze Nato lahko igrajo ključno vlogo pri kriznem upravljanju. Te dejavnosti lahko vključujejo preprečevanje konfliktov, operacije kriznega odzivanja, operacije vsiljevanja miru, embargo na orožje, protiteroristične dejavnosti, odstranjevanje min,… Čeprav je osnovni fokus operacij kriznega odzivanja na kopnem, lahko pomorske sile nudijo podporo pri embargu na orožje in misijah onemogočanja ter podporo kopenskim operacijam s pomorskimi natančnimi udari in fleksibilnim razvojem amfibijskih sil za kopenske operacije (Nato, 2011a).

Pomorske sile ne prispevajo le k varnosti same zveze Nato. Sodelovanja s partnerji utrjujejo tudi regionalno varnost in stabilnost, pripomorejo k preprečevanju konfliktov in pospešujejo dialog. Vse te dejavnosti prav tako pospešujejo sodelovanje z drugimi ključnimi akterji na področju pomorske domene, kot so Združeni narodi (ZN) in EU (Nato, 2015f).

Pomorska strategija poudarja obvezo zveze Nato za varovanje ključnih pomorskih logističnih poti in ohranjanje svobode plovbe. To bo zavezništvo dosegalo z nadzorom, izmenjavo informacij, pomorskim onemogočanjem in prispevanjem k energetski varnosti, vključno z varovanjem kritične infrastrukture (Nato, 2015f). Zveza Nato in njene članice se zavedajo pomena pomorske varnosti in so odločene implementirati pomorsko strategijo. Ta proces vključuje popolno posodobitev in prenovo zavezniških pomorskih sil, obširen večletni program pomorskih vaj in usposabljanj in povečano sodelovanje zveze Nato s svojimi partnerji in tudi drugimi mednarodnimi akterji, še posebej z EU (Nato, 2015f).

3.1.2 Natove Stalne mornariške sile in zmožnosti

Zveza nato ima Stalne mornariške sile (Standing Naval Forces), ki ji omogočajo nenehno pomorsko prisotnost. Gre za večnacionalne odvračalne sile, ki danes predstavljajo ključno

pomorsko komponento zveze Nato. Zadolžene so za izvajanje načrtovanih vojaških vaj, manevrov in obiskov pristanišč, prav tako pa so lahko hitro premeščene v kriznih obdobjih. Sestavljene so iz štirih skupin: Stalni Natovi mornariški skupini (Standing NATO Maritime Groups – SNMG) SNMG1 in SNMG2 ter Stalni Natovi skupini za protiminske ukrepe (Standing Nato Mine Countermeasures Groups – SNMCMG) SNMCMG1 in SNMCMG2 (Nato, 2015f).

Stalni Natovi mornariški skupini SNMG1 in SNMG2 sta integrirani, multinacionalni skupini, sestavljeni iz plovil različnih držav članic zveze Nato. Pomembno je to, da so ta plovila stalno dosegljiva zvezi Nato za opravljanje različnih nalog, od vaj do operativnih misij. Prav tako pomagajo pri uveljavljanju prisotnosti zveze Nato, pri izkazih solidarnosti, opravljajo tudi rutinske diplomatske obiske v različne države, nudijo podporo partnerskim dejavnostim in nudijo pomorsko vojaško pomoč trenutnim misijam zveze Nato. Njuna sestava se spreminja, po navadi pa sta sestavljeni iz dveh do šestih ladij iz prav toliko držav članic. Spadata pod Pomorsko poveljništvo zavezniških sil (Allied Maritime Command – MARCOM), ki ima dva podrejena poveljništva. To sta Poveljstvo podmorniških zavezniških sil (Submarine Command – COMSUBNATO) in Poveljstvo pomorskega vojaškega letalstva zavezniških sil (Maritime Air Command – COMMARAIR) (Nato, 2015f).

Stalni Natovi skupini za protiminske ukrepe SNMCMG1 in SNMCMG2 sta prav tako multinacionalni skupini, ki se primarno ukvarjata z operacijami iskanja in odstranjevanja eksplozivnih sredstev. Obe skupini sta del Natovih odzivnih sil (Nato Response Force – NRF) in sta sposobni opravljanja več vlog, od humanitarnih nalog do operacij. Imata sposobnost hitre premestitve in sta pogosto prvi skupini na območju delovanja. SNMCMG1 je bila ustanovljena leta 1973 v belgijskem pristanišču Ostend z namenom zagotavljanja varne plovbe med pristanišči v angleškem kanalu in severozahodni Evropi. Danes je skupina zmožna delovati po vsem svetu. SNMCMG2 pa je bila ustanovljena leta 1969 kot skupina za mediteransko območje. Obe skupini sta trenutno ime dobili leta 2006 (Nato, 2015f).

Poleg Natovih Stalnih mornariških sil pa pomembno pomorsko zmožnost zveze Nato predstavlja Natov center za ladijski promet (Nato Shipping Centre). Je ključna vez med Natovimi pomorskimi silami in skupnostjo trgovskih ladij. Center predstavlja primarno kontaktno točko za izmenjavo trgovskih informacij med Natovimi vojaškimi organi in mednarodno ladijsko skupnostjo. Je glavni svetovalec ladijski trgovini o potencialnih grožnjah in možnih navzkrižjih oziroma oviranju pomorskih operacij. Poleg sodelovanja v

Natovih pomorskih operacijah Ocean Shield in Active Endeavour sodeluje tudi v Natovih nacionalnih in mednarodnih operacijah. Poleg tega je zadolžen za razvoj in uporabo koncepta Pomorskega sodelovanja in usmerjanja ladijskega prometa[4] (Naval Cooperation and Guidance Shipping – NCAGS) in operira z Zavezniškim informacijskim sistemom za globalno navigacijo[5] (Allied Worldwide Navigation Information System – AWNIS). Glavne naloge centra so izboljšanje izmenjave informacij o trgovskem ladijskem prometu, pospeševanje prostovoljnega sodelovanja med vojaškimi poveljniki in upravniki komercialnega ladijskega prometa. Prav tako center zbira in obdeluje informacije o trgovskem ladijskem prometu in tako skrbi za izgradnjo celovite slike ladijskega prometa na interesnih območjih v podporo vojaškim operacijam (Nato Shipping Centre, 2015).

3.1.3 Natove pomorske operacije

V kontekstu zagotavljanja globalnega javnega dobra velja omeniti dve Natovi pomorski operaciji, Active Endeavour in Ocean Shield. Čeprav je cilj obeh operacij ožji, pa s svojim delovanjem in rezultati močno vplivata na možnost dostopa in uporabe pomorske domene.

A) Operacija Active Endeavour

V operaciji Active Endeavour sile zveze Nato nadzorujejo Sredozemlje in kontrolirajo ladijski promet z namenom odvračanja in obrambe ter zaščite pred teroristično dejavnostjo. Gre za edino Natovo protiteroristično operacijo, ki izhaja iz 5. člena Washingtonske pogodbe, kot podpora Združenim državam Amerike takoj po 11. septembru[6]. Tako je cilj operacije izkazati pripravljenost in solidarnost v boju proti terorizmu in pomagati pri odkrivanju in odvračanju od teroristične dejavnosti v Sredozemlju (Nato Maritime Command, 2015b). Nato je v času operacije pregledal več kot 122.000 plovil in se vkrcal na več kot 160 sumljivih ladij. Z izvajanjem te pomorske operacije je zveza Nato močno pripomogla k izboljšanju percepcije varnosti na celotnem območju. Zveza Nato s to operacijo varuje morje, ščiti ladijski promet in

[4] NCAGS deluje kot nekakšen vmesnik med vojaškimi operacijami in trgovskim ladijskim prometom. Vključuje pripravo vojaškega sodelovanja, usmerjanja in podpore ladijskemu trgovskemu prometu. Glavni namen je povečati varnost sodelujočih trgovskih ladij na območjih vojaških operacij (Nato Shipping Centre, 2015).
[5] AWNIS primerja, koordinira in posreduje navigacijske varnostne podatke trgovskemu ladijskemu prometu in vojaškim enotam na območju vojaških operacij. Operira tako z informacijami zaupne kot splošne narave (Nato Shipping Centre, 2015).
[6] Teroristični napad na Združene države Amerike 11. septembra 2001

nadzira sumljiva plovila. Poleg tega operacija omogoča krepitev odnosov s partnerskimi državami, še posebej s tistimi, ki so del Sredozemskega dialoga[7] (Nato, 2015g).

Operacija Active Endeavour se izvaja pod poveljstvom Štaba pomorskega poveljstva (Maritime Command Headquarters) lociranega v Northwoodu (Velika Britanija), preko namenskih sil, nameščenih v Sredozemlju. Namenske sile Endeavour so sestavljene iz nabora površinskih sil, podmornic in pomorskega letalstva. Operacija redno uporablja dve Natovi fregatni sili visoke pripravljenosti, ki sta v stalni pripravljenosti in sposobni širokega nabora pomorskih dejavnosti. V operaciji sodelujejo tudi Natove stalne mornariške sile, ki skrbijo za periodično podporo operaciji v celoti ali pa prek posameznih enot na klic (Nato, 2015g).

B) Operacija Ocean Shield

Piratstvo v Adenskem zalivu, Afriškem rogu in Indijskem oceanu močno otežuje humanitarne dejavnosti v Afriki in spodkopava varnost na območju ene najbolj prometnih pomorskih poti na svetu, skozi Sueški prekop. Operacija Ocean Shield je Natova protipiratska operacija, ki se izvaja na območju Adenskega zaliva in Afriškega roga od leta 2008, na prošnjo ZN. Glavna naloga operacije je pomoč pri mednarodnih naporih odvračanj in prekinitve pomorskih piratskih napadov, varovanje plovil in hkratna pomoč pri zagotavljanju višjega nivoja varnosti v regiji s sodelovanjem pri izgradnji kapacitet držav v regiji. Operacija se izvaja v tesnem sodelovanju z drugimi pomorskimi silami, vključno z ameriškimi pomorskimi silami (Ameriške združene namenske sile 151), pomorskimi silami EU (operacija Atalanta) in nacionalnimi silami držav v regiji (Nato, 2015b).

Plovila, ki nadzirajo območje, se danes za namen operacije nameščajo v presledkih, v času, ko na območju ni ladij pa za nadzor skrbi pomorsko letalstvo, ki opravlja prelete in zbira informacije. Število napadov, motenj in ugrabitev se je od leta 2008 do danes drastično zmanjšalo, od maja leta 2012 pa na območju ni zabeleženih uspešnih piratskih napadov (Nato Maritime Command, 2015a).

[7] Program, ustvarjen leta 1994, da bi prispeval k regionalni varnosti in stabilnosti in okrepil medsebojno razumevanje in sodelovanje med zvezo Nato in njenimi sredozemskimi partnericami. Te države so: Alžirija, Egipt, Izrael, Jordanija, Mavretanija, Maroko in Tunizija (Nato, 2015g).

3.1.4 Natova vloga v prihodnosti

Pomorske sile zveze Nato bodo glede na pomorsko strategijo imele štiri ključne naloge v pomorski domeni: odvračanje in kolektivno obrambo, krizno upravljanje, kooperativno varnost in pomorsko varnost. Kot politično-vojaška zveza z močno pomorsko zgodovino, bo imela zveza Nato v prihodnosti ključno vlogo pri zagotavljanju uporabe in dostopa do pomorske domene. Posredno je lahko, prek sodelovanja s partnerji in zavezniki zunaj samega zavezništva, eden glavnih zagovornikov in podpornikov pomorskih pravnih norm in sprejemljivega vedenja. UNCLOS predstavlja enega pomembnejših dokumentov mednarodnega pomorskega prava, ki ureja mednarodni dostop do pomorske domene. Ena od nalog zveze Nato je, da skrbi, da se to mednarodno pravo upošteva in uveljavlja ob pojavu novih groženj in izzivov. Tudi prihajajoči izzivi v Arktičnem oceanu predstavljajo tako skrb kot tudi priložnost za zvezo Nato. Štiri od petih držav, ki že uveljavljajo teritorialne zahteve nad deli Arktike, so članice zveze Nato (Danska, Kanada, Norveška in Združene države Amerike). Peta država je Rusija, ki ima od leta 2002 poseben partnerski status v zvezi Nato[8], kar pomeni, da lahko zveza Nato v prihodnosti služi kot prostor, kjer bodo omenjene države izvajale pogovore o njihovih interesih in skrbeh glede prihodnosti arktične regije. Pomorski kriminal, teroristična dejavnost in piratstvo predstavljajo grožnjo pomorski varnosti. Zato je nadaljnje izvajanje operacij, ki preprečujejo te dejavnosti vitalnega pomena za zagotavljanje dostopa in možnost uporabe pomorske domene. Protipiratske operacije na Afriškem robu so tudi dober primer sodelovanja med zvezo Nato, EU, ZN, lokalnimi oblastmi, komercialnimi subjekti in drugimi regionalnimi akterji, kako reševati problem, ki ima globalne posledice. Pomembno je, da zveza Nato spodbuja pomorske države, da sprejemajo konkretne protipiratske zakone v skladu z resolucijami ZN in tako pomagajo omejiti piratske dejavnosti (Allied Comand Transformation 2011, 9–11).

[8] Sodelujeta preko sveta Nato – Rusija, ustanovljenega leta 2002 na vrhu v Rimu. Je mehanizem za konzultacije, iskanje konsenza, sodelovanje, skupno odločanje in skupno delovanje, kjer članice zveze Nato in Rusija sodelujejo na podlagi skupnih interesov pri varnostnih zadevah. Sodelovanje je trenutno prekinjeno zaradi ruskega vojaškega posredovanja v Ukrajini, ki ga zavezništvo grobo obsoja (Nato, 2015e).

3.2 Nato in zračna domena

Varnost civilnega in vojaškega letalstva je ključnega pomena za zvezo Nato. Letalska trgovina je danes ključen element globalne ekonomije, njeno nemoteno in varno delovanje pa je pomembno za blaginjo in ekonomsko varnost. Večina mednarodnih letališč se nahaja na ozemlju članic zveze Nato in predstavlja vstopne točke v mednarodni zračni prostor. Izguba dostopa že za nekaj dni bi imela posledice za zavezništvo, kar so dokazali tudi primeri vulkanskih izbruhov in hudih zim v preteklih letih. Dostop do mednarodnega zračnega prostora je zelo pomemben za zvezo Nato tudi iz obrambnega vidika. Zračna obramba in skupne zračne operacije imajo veliko vlogo v zvezi Nato.

3.2.1 Grožnje zagotovljenemu dostopu in uporabi zračne domene

Grožnje lahko razdelimo na tri dele; na protiletalske sisteme, potencialne sovražnike v prihodnosti in okolje. Zveza Nato v okvir protiletalskih sistemov šteje celoten spekter zemeljskih orožnih sistemov, za katere je značilna različna stopnja učinkovitosti in dostopnosti in jih razdeli v tri glavne skupine (Joint Air Power Competence Centre 2014, 156–7):

1) Manjša orožja / zrak – zrak: sestavljajo jih manjša orožja in nevodeni izstrelki, ki so splošno dostopni in jih je nemogoče popolnoma nadzirati, imajo pa omejeno učinkovitost proti zračnim platformam.

2) Ročno prenosljivi protiletalski obrambni sistemi (Man Portable Air Defence Systems - MANPADS): niso tako lahko dostopni, kot manjša orožja, vendar jih je še vedno v obiliju. Čeprav zahtevajo določeno stopnjo usposobljenosti, so dokaj preprosti za uporabo. Prednost teh sistemov je v težki zaznavi, lahki prenosljivosti in potencialni visoki učinkovitosti proti zračnim platformam brez učinkovite obrambe. Dober primer so nedavni incidenti v Ukrajini, kjer so separatisti, podprti s strani države, povzročali veliko težav ukrajinskim zračnim silam pri nemotenem dostopu in uporabi zračnega prostora. Primer je izguba transportnega letala in 49 ljudi na krovu 14. junija 2014, ki naj bi bilo sestreljeno prav s takšnim lahkim prenosnim sistemom.

3) Kopenska zračna obramba (Ground Based Air Defence – GBAD) in integrirani sistemi zračne obrambe (Integrated Air Defence Systems – IADS): te sistemi so široko dostopni s strani več držav. Takšni obrambni sistemi so izredno učinkoviti tudi proti letalom najnovejše generacije, a so zelo dragi za nabavo in vzdrževanje. Vodilna sila na tem področju ostaja Rusija, ki je takšne sisteme izvozila tudi v Iran in Sirijo. Poleg tega pa so nedavni dogodki pokazali, da takšni sofisticirani sistemi niso več le v domeni držav; 17. julija 2014 naj bi bilo s tovrstnim sistemom zračne obrambe v Ukrajini sestreljeno malezijsko letalo s strani separatistov. Čeprav ni povsem jasen izvor sistema, pa možnost operativnega upravljanja takšnih sistemov s strani neregularnih sil predstavlja veliko grožnjo zagotavljanju dostopa in uporabe zračne domene.

V preteklosti je bil poudarek na terorističnih omrežjih, vendar so se v zadnjem času pojavile druge skupine in organizacije, ki bi v bližnji prihodnosti lahko ogrozile nemoten dostop do zračne domene. ISIS oziroma IS (Islamska država Iraka in Levanta) je ena od dobro oboroženih skupin, ki predstavlja potencialno grožnjo. Prav tako smo bili priča omejevanju dostopa do zračne domene v Ukrajini, s strani različnih skupin. Čeprav je bila v preteklosti pozornost zveze Nato predvsem v Iraku in Afganistanu, pa so razvile močna orožja tudi druge države. Združene države Amerike vse večjo pozornost posvečajo Kitajski in njenim zračnim kapacitetam. Poleg tega so tu še Rusija, Severna Koreja in Iran. Združene države Amerike so začele reševati problem vse večjih groženj s strani protiletalskih kapacitet z razvojem zračno-pomorskega koncepta[9] (Joint Air Power Competence Centre 2014, 157).

Motnje pri zagotavljanju dostopa in uporabe zračne domene pa ne prihajajo nujno le s strani oborožitvenih sistemov in potencialnih sovražnikov. Tudi okolje ima v tem kontekstu pomembno vlogo. Spomladi in pozimi leta 2010 sta veliko težavo predstavljali vulkanska dejavnost in ostre zimske razmere. Ob izbruhu islandskega vulkana Eyjafjallajokull so nastali oblaki vulkanskega pepela, ki so ohromili letalski promet čez celoten trans-atlantski koridor za več kot dva meseca. Škoda je bila ocenjena na več kot 140 milijonov evrov dnevno (Assured Access to Global Commons 2011, 16). Močno sneženje in nizke temperature februarja leta 2010 so močno ovirale letalski promet po Evropi. V zahodni Evropi so bila takrat ohromljena najmanj štiri večja letališča (Delo, 2010).

[9] Zračno-pomorski koncept (Air-Sea Battle Concept – ASB) – gre za koncept globinskega bojevanja, vendar namesto fokusiranja na zemeljsko domeno iz zraka poudarja integrirane operacije iz vseh petih domen (zrak, zemlja, morje, vesolje in kibernetski prostor) za doseganje prevlade. Gre za koncept, ki bi bil v prihodnosti uporaben tudi za Zvezo Nato (Joint Air Power Competence Centre 2014, 157).

3.2.2 Odziv zveze Nato za zagotavljanje dostopa in uporabe zračne domene

Odziv zveze Nato mora biti večplasten in mora obsegati več področij delovanja. Na strateškem nivoju bi bila ena od možnih rešitev vpeljava koncepta »preprečevanja, priprave, zaščite in prizadevanja«. Koncept izhaja iz osnovne protiteroristične strategije in predstavlja način, kako bi lahko deloval celostni pristop k reševanju problema. Gre za pristop, kjer ni pomembna le zračna komponenta, ampak tudi vesoljska, pomorska, zemeljska in kibernetska (Joint Air Power Competence Centre 2014, 160). Vsebuje štiri korake, ki imajo vsak svojo funkcijo (Joint Air Power Competence Centre 2014, 160–1):

- preprečitev: gre za zmožnost preprečitve nabave, usposabljanja, pridobivanje znanja in premikanja sistemov. Med drugim vključuje obveščevalno dejavnost (tudi na kibernetskem področju), omejitve pri izvozu, sankcije, gospodarske predpise in zakone,

- priprava: razvoj taktik, usposabljanj in postopkov (Tactics, Training and Procedures – TTP) in njihovo izvajanje v operativno degradiranem okolju, razvoj vojaških in civilnih kriznih načrtov ter obveščevalna dejavnost,

- zaščita: aktivacija vojaških in civilnih kriznih načrtov, obveščevalna dejavnost, onemogočanje sovražnikove zračne obrambe (Suppression of Enemy Air Defence – SEAD), sile za specialno delovanje, fizični napadi, elektronski in kibernetski napadi,

- prizadevanje: napad na omrežja, ki vključuje skupek fizičnih in nefizičnih dejavnosti na vojaškem in medvladnem področju.

Danes letalske sile zveze Nato ne morejo delovati v novem okolju in se soočati z novimi izzivi brez primernih obrambnih ukrepov za zavarovanje teh sil. Tu nastane vprašanje, na kakšen način opremiti nacionalne letalske sile, da bodo imele dovolj veliko stopnjo zaščite. Nove letalske platforme so zelo učinkovite, vendar, če si države ne morejo privoščiti vzdrževanja teh platform in predvsem sistemov za obrambo[10] teh platform, je njihova uporabnost in zmožnost manevra zelo okrnjena. Zato bi zveza Nato lahko uporabila strategijo, upoštevajoč učinkovitost naproti stroškom, ki bi šla v smeri nadgradnje obstoječih letalskih sil

[10] Sistemi za obrambo (Defense Aids Systems) so sistemi vojaških letal, ki jih varujejo pred različnimi izstrelki. Običajno so sestavljeni iz trakov za motenje radarjev, svetilnih raket in elektronskih ukrepov za zaznavo groženj (Wikipedia, 2015).

namesto nakupa moderne opreme, ki je potem države ne bi zmogle finančno vzdrževati (Joint Air Power Competence Centre 2014, 161).

Določeni Natovi projekti (npr. zračni sistem zgodnjega opozarjanja in nadzora) dokazujejo, da lahko zveza Nato priskrbi visoko-tehnološko opremo za zoperstavljanje širokemu spektru groženj. Vendar pa je večina programov oziroma področij, ki bi okrepili zmožnost zagotavljanja uporabe in dostopa do zračne domene (na primer področje onemogočanja sovražnikove zračne obrambe) finančno zelo zahtevnih, kar pomeni, da je nemogoče, da bi katerakoli od držav članic zveze Nato, razen Združenih držav Amerike, v prihodnosti sama financirala takšen program, in bi bilo zato treba najti drugačen način. Ena od možnosti je, da bi posamezne države prevzele le določene segmente programa, zveza Nato pa bi nato s povezavo teh segmentov dobila celotno infrastrukturo. Takšne rešitve bodo sicer zahtevale ogromne politične napore in izkaze volje in zaupanja znotraj držav članic (Joint Air Power Competence Centre 2014, 161–2).

Poleg materialnih rešitev je naloga zveze Nato zagotoviti zadostno stopnjo usposobljenosti in interoperabilnosti, ki se mora vzdrževati na dolgi rok. Zveza Nato mora posvetiti velik del pozornosti usposabljanju kadra za delovanje v zahtevnih pogojih. Ob upoštevanju vse manjših finančnih virov je celostno in posodobljeno usposabljanje na manj moderni tehnologiji in opremi veliko bolj učinkovito, kot investiranje v sodobno opremo, ki zahteva drago usposabljanje (Joint Air Power Competence Centre 2014, 162).

Za zagotovljen dostop do zračne domene v prihodnosti bo pomembno, da zveza Nato nadaljuje grajenje močnih vezi s partnericami in potencialnimi zavezniki, in da izboljša deljenje informacij in obveščevalnih podatkov s temi državami. To ji bo pomagalo zagotoviti varen dostop svojih sil na potencialna problematična območja (Joint Air Power Competence Centre 2014, 162–3).

Zelo pomemben vidik zračnega delovanja danes predstavljajo brezpilotni zračni sistemi. Te sistemi imajo vse večjo vlogo pri operacijah opazovanja, izvidovanja, obveščanja in tudi pri ofenzivnih operacijah. Poleg tega predstavljajo potencialno grožnjo v rokah sovražnika. Zato je naloga zveze Nato, da natančno opredeli vlogo teh sistemov in nato razvije standarde uporabe in interoperabilnost teh sistemov v zavezništvu (Allied Command Transformation 2011, 18). Dober primer uporabe teh novejših tehnologij je razvoj Natovih kapacitet imenovanih Zavezniški talni nadzor (Alliance Ground Surveillance – AGS) znotraj koncepta

pametne obrambe[11]. Skupina držav članic bo zagotovila pet brezpilotnih zračnih vozil Global Hawk in pripadajočih nadzornih postaj. Zveza Nato bo z njimi opravljala in jih vzdrževala v imenu vseh 28 članic. Sistem bo omogočal zvezi Nato nenehen nadzor širokega področja z velikih višin in z velikih razdalj v kakršnihkoli vremenskih pogojih, tako podnevi kot ponoči (Nato, 2015a).

3.3 Nato in vesolje

Zagotovljen dostop in uporaba vesolja imata velik pomen za zvezo Nato iz dveh glavnih razlogov; ker ima uporaba vesolja vlogo multiplikatorja moči in ker bi lahko v prihodnosti vesoljske komponente postale tarče napadov.

Vesoljska komponenta je skupaj s kibernetsko vse bolj pomembna v sodobnem svetu. Prek uporabe satelitov nam je omogočeno pozicioniranje, navigacija, opozarjanje in ocena groženj, spremljanje okolja, komuniciranje, nadzor, obveščanje in izvidovanje. Te storitve omogočajo zvezi Nato učinkovito navigacijo, zaščito in namestitev sil, raketno obrambo, vodenje izstrelkov, napovedovanje vremena, izbor streliva, ocene bojne škode, komunikacijo,… Vesolje tako nastopa v vlogi multiplikatorja moči, kjer uporaba vesoljskih tehnologij močno poveča moč in učinkovitost, obenem pa bi onemogočen dostop do vesolja imel ogromen negativni učinek na sposobnost zveze Nato, da projicira moč, izvaja poveljevanje in nadzor in oskrbuje svoje sile (Joint Air Power Competence Centre 2012, 8). Zveza Nato se je zanašala na uporabo vesolja tudi pri operacijah ISAF v Afganistanu. Ta uporaba je med drugim obsegala komunikacije, pozicioniranje, navigacijo, zaznavanje okolja, opozorila pred izstrelki in iskanje pogrešanih. Uporaba vesoljske tehnologije je zelo pomembna tudi pri pomorskem nadzoru in posledično boju proti piratstvu. Uporablja se v navezi z drugimi nadzornimi sistemi in tako omogoča nadziranje pristanišč, obalnih območij, sledenje trgovini z ljudmi in

[11] Koncept pametne obrambe je način zagotavljanja sodobnih obrambnih zmogljivosti za potrebe zveze Nato na čim bolj učinkovit, povezan in stroškovno ugoden način. Gre za koncept, kjer se države članice zveze Nato spodbuja, da skupaj razvijajo, pridobivajo, uporabljajo in vzdržujejo vojaške zmogljivosti, da lahko zavezništvo dosega osnovne cilje (Nato, 2015h).

drogami, identifikacijo piratskih čolnov, ugrabljenih plovil in nezakonitega ribarjenja (Remuss 2010, 2–4).

3.3.1 Grožnje dostopu in uporabi vesolja

Grožnje uporabi in dostopu do vesoljske domene padejo v dve široki kategoriji; fizično škodo na infrastrukturi v vesolju ali na tleh in dejavnosti, katerih namen je motenje sprejema in oddaje satelitskih signalov brez neposredne fizične škode na infrastrukturi.

Pri povzročanju fizične škode je danes malo verjetno, da bi to uporabljale teroristične organizacije ali podobni subjekti iz očitnih razlogov. Prvič, sestrelitev satelita ima manjše fizične in psihične posledice, kot če usmerijo izstrelke ali jedrske naprave na tarče na Zemlji. Drugič, izstrelitev izstrelkov v vesolje je še danes zelo drag postopek za večino akterjev pod nacionalnim in korporacijskim nivojem. In tretjič, izstrelitve se težko izvedejo neopaženo zahvaljujoč učinkovitemu satelitskemu nadzoru, tako da to odvrača države, da bi pomagale pri izstrelitvah, saj se zavedajo, da bi bile tarče ostrih povračilnih ukrepov. Večjo grožnjo dostopu do vesolja predstavlja nagel razvoj protisatelitskih tehnologij držav. Obstaja več načinov onesposobitve ali uničenja satelita v vesolju, tudi z usmerjenimi energetskimi orožji in mikrovalovi. V bližnji prihodnosti se bo razvoj teh tehnologij samo še stopnjeval. Pri nefizičnih metodah, ki so usmerjene predvsem na motenje komunikacijskih procesov satelitov in vesoljskih plovil, gre predvsem za radijsko motenje signalov (jamming) in ugrabitev signalov (spoofing). Pri radijskem motenju gre za prekinitev povezave med satelitom in njegovo postajo na Zemlji s pomočjo elektronskih signalov. Pri ugrabitvi signalov pa gre za kibernetsko ugrabitev kontrolnega signala sistema (Allied Command Transformation 2011, 26–27).

3.3.2 Natova vloga v vesolju

Pomembno dejstvo je, da zveza Nato nima v lasti svojih satelitov, ampak je odvisna od tehnologij svojih članic in komercialnega sektorja. Trenutno ima zveza Nato od leta 2005, do

leta 2019 zakupljene satelitske kapacitete treh držav članic: Velike Britanije, Francije in Italije[12] (Spacenews 2013).

Prav tako zveza Nato nima svoje vesoljske politike, nima vojaške vesoljske strategije ali vesoljske doktrine. Tako zveza Nato nima razdelanega področja vesoljskih operacij, težave pa nastajajo tudi pri strateškem in operativnem načrtovanju zaradi težav pri integraciji vesoljskih kapacitet. Ker zveza Nato ne postavlja vojaških zahtev na tem področju, države članice razvijajo vesoljske kapacitete individualno za potrebe nacionalne obrambe in varnosti (Remuss 2010, 5–6).

Danes se pojavlja utemeljeno vprašanje, zakaj zveza Nato potrebuje svojo vesoljsko tehnologijo in usmeritev, če to počne že EU, Evropska vesoljska agencija (ESA) in države članice same. Evropska unija je po hladni vojni našla svojo vlogo v poudarjanju mehke moči in civilnega kriznega upravljanja, medtem ko zveza Nato še vedno predstavlja vojaško moč in obrambo. In ravno zaradi teh različnih področij udejstvovanja je pomembno, da tudi zveza Nato začne razmišljati o razvoju svojih vesoljskih zmožnosti, ki ji bodo omogočile multiplikacijo moči na svojem področju. Pomembno je tudi, da obe organizaciji upoštevata kapacitete druge in jih vključita v svoje načrtovanje (Remuss 2010, 6).

Prvi in najpomembnejši korak v to smer bo sprejem vesoljske politike. Sprejem vesoljske politike ima tri glavne namene: omogoča utemeljeno sprejemanje nadaljnjih odločitev, zastavi smer delovanja in predstavi zastavljene cilje in postopke. Na operacijskem nivoju to omogoča smotrno načrtovanje, zastavlja porabo in razdelitev sredstev, služi kot podlaga za napredek in predstavlja vir zapisanih smernic za pomoč osebju pri delu. V končni fazi bo sprejeta vesoljska politika omogočala primerno in napredno pripravljenost. S političnega vidika sprejeta politika omogoča nadzor in skladnost. Brez sprejete politike in zastavljenih ciljev lahko odločitve prinesejo nepričakovane rezultate in ne omogočijo doseganja ciljev, sploh če ti niso jasno definirani (Joint Air Power Competence Centre 2012, 2). S sprejetjem vesoljske politike bi se zveza Nato poleg Evropske vesoljske agencije pokazala kot še ena od organizacij, kjer je možno sodelovanje med državami na področju vesolja. Na področju vesolja Evropska unija, civilne vesoljske agencije in države članice zveze Nato kažejo napredek. ESA in EU sta že začeli sami raziskovati varnostne in obrambne možnosti, s tem pa se pojavlja tveganje za marginalizacijo zveze Nato na vesoljskem področju. Zato je

[12] Zveza Nato ima zakupljene satelitske kapacitete preko vojaških komunikacijskih sistemov: britanski Skynet, francoski Syracuse 3 in italijanski Sicral

pomembno, da zveza Nato skupaj s svojimi članicami definira vesoljske vojaške cilje, operativne zahteve in sheme financiranja ter ustvari kooperativno okolje, ki bo povezovalo civilne in vojaške vesoljske kapacitete in omogočalo dostop do njih vsem članicam. Vesoljska politika mora zastaviti tudi strukturno shemo (Joint Air Power Competence Centre 2012, 3):

- v strateška, operativna in taktična poveljstva morajo biti nameščeni strokovnjaki iz vesoljskega področja,
- usposabljanje na vesoljskem področju mora biti inkorporirano v splošno izobrazbo,
- predavanja in predmeti morajo biti inkorporirani v vojaške izobraževalne tečaje, da se prepreči splošno pomanjkanje izobrazbe in zavedanje o vesoljskih operacijah,
- potrebna je koordinacija na strateškem političnem nivoju, da se omogoči popolna izraba nacionalnih vesoljskih zmogljivosti.

Zelo pomembno vlogo bo imelo povečevanje sodelovanja z drugimi organizacijami. Tekmovanje v naporih med akterji na področju vesoljske varnosti ima negativne posledice. Tako EU, ESA, kot države članice zveze Nato zasledujejo svoje vesoljske interese in gradijo različne zmogljivosti. Zato je ena ključnih vlog zveze Nato, da med mednarodnimi organizacijami, ki se ukvarjajo z razvojem vesoljske tehnologije za povečanje varnosti, najde svojo vlogo. Treba bi bilo najti dogovor o razvoju vesoljskih zmogljivosti, ki bi preprečeval nepotrebno podvajanje (na podoben način, kot imata razdeljene vloge zveza Nato in EU na področju zunanjih varnostnih operacij) (Remuss 2010, 7–8).

Da se čim bolj optimizira uporaba obstoječih zmogljivosti, prepreči, oziroma zmanjša podvajanje naporov in zagotovi interoperabilnost med različnimi vesoljskimi sistemi in službami je potrebno povečano sodelovanje med državami, zvezo Nato in evropskimi organizacijami. Zato je potrebno aktivno sodelovanje zveze Nato z evropskimi vladami, EU, Evropsko vesoljsko agencijo in Evropsko obrambno agencijo, da se določijo varnostne in obrambne potrebe obstoječih in planiranih vesoljskih sistemov. V ta namen bi se lahko ustvarila Natova vesoljska pisarna znotraj poveljništva, po možnosti v obliki koordinacijskega centra (Remuss 2010, 8).

Vojaški, civilni in komercialni sektorji so vse bolj odvisni od vesoljskih kapacitet in posledično se veča verjetna grožnja napadov na vesoljske zmogljivosti s strani potencialnih sovražnikov, zato je pomembno, da se vse vesoljske zmogljivosti in sisteme, vključno s

sredstvi za zaščito teh zmogljivosti, vključi v prihodnje vojaško načrtovanje zveze Nato. Prav tako se mora zveza Nato zavzemati za vse večjo integracijo nacionalnih vesoljskih zmogljivosti tako obstoječih kot prihodnjih sistemov. Treba je izboljšati postopke zbiranja, upravljanja, deljenja in razpošiljanja informacij med vključenimi subjekti (Remuss 2010, 8).

3.2 Nato in kibernetski prostor

»Kot večina modernih organizacij, je tudi zveza Nato močno vpeta v omrežje na vsakem nivoju, od vodstvenih struktur do poveljevanja in kontrole, od urejanja dokumentov do vojaških operacij. Kot taka je potencialna tarča hekerjev, hkrati pa postaja pomemben globalni vir za nove raziskave in razmišljanja o kibernetski obrambi« (Allied Command Transformation 2011, 37).

Tako zveza Nato, kot posamezne države članice, so kot uporabniki kibernetske domene dovzetni za znana in neznana tveganja. Vse večja odvisnost od kibernetskega prostora je velika ranljivost, ki bo sčasoma vodila v zmanjšano vsesplošno odpornost zveze Nato na različne grožnje, če se ne investira v razvoj instrumentov in metod za zagotavljanje varnosti. Prekinitev ali izguba dostopa do kibernetskega prostora bi imela takojšen vpliv na zmožnost izvajanja nalog. To vključuje nabavo in organizacijo vojaških zmožnosti, sodelovanje v političnih procesih, ki podpirajo in so v skladu z operacijami zveze Nato ter administracijo in nadzor nad vodstvenimi elementi in silami, ki delujejo v dejavnostih zveze Nato. Vse te dejavnosti so odvisne od varnega dostopa in uporabe kibernetskega prostora. Temeljna naloga zveze Nato je najprej natančno razumeti in definirati svoje šibkosti, identificirati vire ogrožanja v kibernetskem prostoru in nato izdelati primerne strategije in razviti zmožnosti za zagotavljanje varnosti v kibernetskem prostoru (Klimburg 2012, 180–2).

Nato opredeljuje kibernetske grožnje kot resen vir ogrožanja tudi v svojem najnovejšem strateškem načrtu in ugotavlja, da so vse bolj pogoste, organizirane in imajo sposobnost povzročanja vse večje škode vladnim službam, podjetjem, gospodarstvu in ostali kritični infrastrukturi in kot take predstavljajo grožnjo nacionalni in evroatlantski blaginji, varnosti in stabilnosti. Kot potencialne vire ogrožanja strateški načrt opredeljuje tuje vojaške in obveščevalne službe, skupine organiziranega kriminala ter teroristične in ekstremistične skupine (Nato strateški koncept 2010 12. čl.). Kibernetskih groženj se je zveza Nato dotaknila

tudi v Lizbonski izjavi, po vrhu v Lizboni leta 2010, kjer jih je označila kot hitro rastoče in razvijajoče.

Primarna naloga zveze Nato je varovanje komunikacijskih in informacijskih sistemov v svoji lasti, enako pomembna pa je zanesljiva in varna podporna infrastruktura posameznih držav članic, še posebej tista, ki je ključnega pomena za dejavnosti zveze Nato. Zato je ena od prioritet tudi sodelovanje s posameznimi državami članicami z namenom zagotoviti merila, standarde in mehanizme, ki bodo omogočale primerno raven kibernetske varnosti nacionalne informacijske infrastrukture (Nato, 2015c).

Čeprav se zveza Nato zaveda pomena kibernetskega prostora in kibernetske varnosti in je že na začetku novega tisočletja pozivala k izboljšanju zmogljivosti članic za kibernetsko obrambo, so se bolj odločni premiki na tem področju zgodili šele po kibernetskem napadu na Estonijo leta 2007[13]. Leto kasneje so sprejeli politiko zveze Nato za kibernetsko obrambo, ki vzpostavlja tri osrednje elemente politike zveze Nato na področju kibernetskega prostora (Revija Nato, 2011):

- Subsidiarnost
- Nepodvajanje
- Varnost

Strateški načrt zveze Nato iz leta 2010 je poleg opredelitve kibernetskih groženj zelo pomemben tudi pri določitvi pomena kibernetskega prostora za zvezo Nato. Z novim strateškim načrtom se zavezništvo zavezuje k nadaljnjemu razvoju svojih varnostnih zmožnosti v kibernetskem prostoru za preprečitev, zaznavo in obrambo ter okrevanje pred kibernetskimi napadi, vključno z izboljšanjem in koordinacijo posameznih nacionalnih kapacitet za kibernetsko obrambo in postavitvijo vseh teles zavezništva pod centralizirano kibernetsko obrambo (Nato strateški koncept 2010 19. čl.). Da se zagotovi nemoten in stalen dostop do kibernetskega prostora in zagotovi integriteto ključne infrastrukture, se mora kibernetska razsežnost modernih konfliktov vključiti v obrambno doktrino, hkrati pa je treba izboljšati sposobnosti za odkrivanje, oceno, preprečitev, obrambo in okrevanje po morebitnem kibernetskem napadu na sisteme, ki so ključnega pomena za zvezo Nato. Preko Natovega

[13] Aprila 2007 je Estonija doživela vrsto kibernetskih napadov. Napadi so bili usmerjeni na več pomembnih vladnih spletnih strani, kot tudi na spletne strani bank, univerz in estonskih časopisnih hiš. Povod za kibernetske napade je bil umik spomenika sovjetske vojne v Talinu. Napadi so imeli velike varnostne posledice na področju kibernetske varnosti (International Affairs Review, 2015).

procesa obrambnega načrtovanja[14] se bo promoviral razvoj sposobnosti zveze Nato za kibernetsko obrambo, pomagalo posameznim članicam in optimiziralo izmenjavo informacij, sodelovanje in medsebojno povezljivost (Nato, 2010).

Leta 2011 je bila sprejeta področna politika kibernetske obrambe, z naslovom Zaščitimo omrežja, ki je dejansko povzela stališča strateškega koncepta in lizbonske izjave. Zveza Nato bo pozornost pri razvoju kibernetske obrambe usmerila v (Nato, 2011b):

- integracijo ukrepov za kibernetsko obrambo v Natove strukture in proces načrtovanja za nemoteno opravljanje temeljnih nalog kolektivne obrambe in kriznega opravljanja,
- preprečitev, odpornost in obrambo ključne kibernetske infrastrukture zveze Nato in zaveznic,
- razvoj učinkovitih zmožnosti kibernetske obrambe in centralizacija zaščite svojih omrežij,
- postavitev minimalnih zahtev za kibernetsko obrambo nacionalnih omrežij, ključnih za zvezo Nato,
- podpora zaveznikom pri doseganju minimalne ravni kibernetske obrambe in zmanjšanju ranljivosti ključne nacionalne infrastrukture,
- sodelovanje s partnerji, mednarodnimi organizacijami, zasebnim sektorjem in akademsko sfero.

Zveza Nato v svojem novem strateškem konceptu in nadaljnje v svoji politiki za kibernetsko obrambo zelo jasno pove, da se kolektivna obramba po 5. členu Washingtonske pogodbe nanaša tudi na kibernetski prostor in lahko sproži kolektivno obrambo, čeprav se takšen kibernetski napad, ki bi sprožil vojaško posredovanje, še ni zgodil. Kibernetski napadi na Estonijo iz leta 2007, na primer, se kljub svoji ostrosti niso smatrali kot zadostni, da bi bila potrebna vojaška kolektivna obramba, so pa ostale članice nudile tehnično in nadzorstveno pomoč. Poleg tega so v Natovi politiki za kibernetsko obrambo jasno dogovorjeni postopki za

[14] Natov proces obrambnega načrtovanja (Defence Planning Process - NDPP) je proces, s katerim zveza Nato identificira ključne zmogljivosti in promovira njihov razvoj s strani članic, da bi lahko izpolnila svoje varnostne in obrambne cilje. NDPP vpliva na nacionalno obrambno načrtovanje, da je v skladu s potrebami zveze Nato. Vključuje več domen: sile, viri, oborožitev, logistika, zračna in raketna obramba, C3, kontrola zračnega prometa, standardizacija, obveščevalna dejavnost, vojaška medicinska podpora, znanost in tehnologija in kibernetska domena (Nato, 2014a).

razpravo po 4. členu ustanovne pogodbe v primeru resnega kibernetskega napada (Klimburg 2012, 182).

Zelo pomemben dokument, ki se ukvarja s tem, kako se mednarodno pravo nanaša na kibernetske konflikte in kibernetsko bojevanje je t. i. Talinski priročnik (Tallin Manual on the International Law Applicable to Cyber Warfare). Izdan je bil leta 2013, napisan s strani mednarodne skupine strokovnjakov. Priročnik se mi zdi vredno omeniti, ker v pravilu številka 16 govori o kolektivni samoobrambi. Priročnik navaja, da se sme kolektivna samoobramba, ki vključuje oborožen napad, izvajati izključno na prošnjo napadene države in le v okviru te prošnje. Poleg tega loči dva načina izvajanja kolektivne samoobrambe; prvi način je prek ad hoc dogovora, drugi pa na podlagi prej podpisane pogodbe o kolektivni obrambi, kamor spada tudi Washingtonska pogodba in njen člen o kolektivni samoobrambi (Schmitt 2013, 67 – 8). Tako tudi ta dokument potrjuje, da se kolektivna obramba zavezništva po 5. členu nanaša tudi na kibernetsko obrambo in da lahko kibernetski napad sproži obrambne ukrepe po tem členu. Pomembno je predvsem povabilo oziroma prošnja napadene države in pa strinjanje članic zveze Nato, da napad zadošča merilom.

Zveza Nato je v povsem funkcionalnem smislu zadolžena le za svoja računalniška omrežja, ne pa tudi za omrežja posameznih držav. Natove zmogljivosti za odzivanje na računalniške incidente (NATO Computer Incident Response Capability – NCIRC), ki skrbijo za varovanje omrežij, so bile ustanovljene leta 2003 in razširjene v letu 2011 in predstavljajo ključno operativno zmogljivost na področju kibernetske obrambe. V okviru koncepta pametne obrambe in združevanja in souporabe zmogljivosti[15] se predpostavlja tudi možnost razvoja Natove skupine za hitro odzivanje v okviru NCIRC. Gre za skupino strokovnjakov na področju informacijske varnosti, ki bi nudili podporo državi na njeno prošnjo, ki je lahko politične ali strateške narave. Pomoč lahko obsega reševanje tehničnih težav ali pa neodvisno zbiranje dokazov o naravi oziroma vzroku incidenta. Še en korak pri zagotavljanju varnosti v kibernetskem prostoru je ustanovitev Natove komunikacijske in informacijske agencije (Nato

[15] Koncept združevanja in souporabe zmogljivosti (Pooling and sharing initiative) je koncept, ki ga je razvila Evropska obrambna agencija skupaj s članicami EU. Nanaša se na pobude in projekte za združevanje in souporabo vojaških zmogljivosti med članicami EU (Europan Defence Agency, 2014).

Communications and Information Agency – NCI), ki zvezi Nato zagotavlja informacijsko tehnologijo in C4ISR[16] (Klimburg 2012, 181–3).

Leta 2008 je bil v Estoniji, v Talinu, ustanovljen Natov kooperativni center odličnosti za kibernetsko obrambo (Nato Cooperative Cyber Defence Centre of Excellence – CCD COE), katerega namen je priskrbeti tehnično strokovno znanje na področju kibernetske obrambe in se ukvarjati z raziskavami in usposabljanjem na področju kibernetskega bojevanja. Poleg tega je bil ustanovljen tudi Urad za upravljanje kibernetske obrambe (Cyber Defence Management Authority), ki je zadolžen za usklajevanje kibernetske obrambe po celotni zvezi Nato (Allied Command Transformation 2011, 37–42).

Čeprav je temeljna naloga razvoj ustreznih kapacitet znotraj zveze Nato in v posameznih državah članicah, se zveza Nato v zadnjih letih osredotoča tudi na sodelovanje z nečlanicami. Leta 2011 je Avstrija kot prva vstopila v posebno bilateralno sodelovanje z zvezo Nato, ki obsega vse pomembne vidike kibernetske varnosti. Od takrat je podobne bilateralne sporazume z zvezo Nato podpisalo že 6 držav. Takšni sporazumi lahko vključujejo različne oblike sodelovanja: usklajevanje postopkov kriznega upravljanja, izmenjava pomembnih informacij in ocen, usposabljanja, skupne raziskovalne projekte, ustanavljanje in nadgradnja kapacitet in postopkov, ki so namenjeni kibernetski varnosti,… (Klimburg 2012, 185).

Zelo pomemben vidik predstavlja tudi sodelovanje med zvezo Nato in EU. V splošnem velja vodilo, da njune institucije delujejo skupaj z namenom doseganja prostora, kjer se promovira varnost in kjer obstaja skladnost med socialnimi, ekonomskimi in nacionalno-varnostnimi politikami. V okviru evropske Skupne zunanje in varnostne politike je eden pomembnejših dogovorov t. i. »Berlin Plus« dogovor. Gre za dogovor, ki EU zagotavlja podporo zveze Nato pri njenih naporih znotraj njene skupne zunanje in varnostne politike, v okviru kibernetske obrambe pa je pomembno, da dogovor ureja izmenjavo tajnih podatkov. V zadnjih letih se je povečalo tudi sodelovanje z Evropsko obrambno agencijo, ki je znotraj svojega načrta razvoja kapacitet jasno opredelila kibernetsko obrambo kot prioriteto (Klimburg 2012, 186–7).

Leta 2014 na vrhu zveze Nato v Walesu je bila sprejeta tudi Izboljšana politika kibernetske obrambe (Enhanced Cyber Defence Policy). Predstavlja nadaljevanje prejšnje in tako le še utrdi stališča zveze Nato na področju kibernetske obrambe. Sprejet je bil tudi predlog estonskih obrambnih sil o uporabi njihovih kibernetskih poligonov kot osrednjega dela

[16] Poveljevanje, vodenje, komunikacije, računalniški sistemi, obveščanje, nadzor in izvidovanje (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance – C4ISR)

usposabljanj zveze Nato na področju kibernetske obrambe. Celotna deklaracija sprejeta na vrhu v Walesu pa omenja tudi pomembnost sodelovanja zveze Nato z industrijskim sektorjem skozi novonastalo Natovo industrijsko kibernetsko partnerstvo (Nato Industry Cyber Partnership). Tehnološke inovacije in znanje iz zasebnega sektorja namreč zveza Nato vidi kot pomemben dejavnik doseganja zastavljenih ciljev iz svojega strateškega koncepta in svoje kibernetske politike (CCDCOE, 2014).

4 SLOVENIJA IN GLOBALNA JAVNA DOBRA

4.1 Slovenija in pomorska domena

Zagotovljen dostop in uporaba pomorske domene ima za Slovenijo zagotovo precejšen pomen, predvsem v smislu razvoja gospodarstva. Luka Koper kot naše največje in edino mednarodno tovorno pristanišče je odvisno od nemotene mednarodne pomorske trgovine. Motnje v dostopu in uporabi pomorske domene bi lahko imele vpliv na delovanje pristanišča, katerega gospodarski učinki segajo na področje trgovinskih, turističnih, gostinskih, finančnih, pomorskih, špedicijskih dejavnosti in dejavnosti, ki so vezane na cestne in železniške prevoze.

Neposredno vojaško ogrožanje Slovenije s strani pomorske domene je minimalno, zato so interesi po zagotavljanju uporabe in dostopa predvsem znotraj interesov zveze Nato. Pri vojaškem udejstvovanju na morju se Slovenija vidi predvsem v regionalnem okolju s težiščem delovanja na območju Jugovzhodne Evrope. Tu imamo zaradi geografske bližine, zgodovinske, politične, gospodarske in kulturne povezanosti poleg obrambnih in varnostnih tudi politične in gospodarske ter druge interese (Ministrstvo za obrambo, 2012).

Pomorsko komponento v Slovenski vojski predstavlja 430. mornariški divizion, ki je glede na vlogo v bojnem delovanju umeščen pod sile za bojno podporo. Namen je zagotavljanje vojaške obrambe slovenskega akvatorija in sodelovanje v sistemu zaščite, reševanja in pomoči na morju. Glavne naloge so (Slovenska vojska, 2015a):

- zagotavljanje pripravljenosti za delovanje v akvatoriju,

- vzpostavitev vojaške kontrole in izvajanje vojnega režima plovbe,
- izvajanje protiminskega ter protidiverzantskega delovanja,
- sodelovanje v protiladijskem delovanju,
- sodelovanje v protiteroristični zaščiti lastnih in zavezniških vojaških objektov,
- odkrivanje in obveščanje o virih ogrožanja v akvatoriju,
- izvajanje nalog po načrtih v primeru nesreč,
- sodelovanje pri organizaciji in izvajanju nalog podpore državi gostiteljici.

Za izvajanje nalog ima slovenska vojska v lasti dve ladji: Triglav 11[17] in Ankaran[18]. V okviru mednarodnega udejstvovanja ima glavno vlogo večnamenska ladja Triglav 11, ki je v letih 2013 in 2014 sodelovala pri operaciji Naše morje[19], letos pa se pripravlja za sodelovanje na mednarodni operaciji Evropske unije EUNAVFOR MED[20]. Slovenska vojska bo v operaciji sodelovala v poveljniški strukturi in v južnem delu osrednjega Sredozemlja z zdravstveno skupino ROLE 2 in večnamensko ladjo Triglav 11 s posadko. Oblikovana bosta dva kontingenta, ki bosta v enoletnem mandatu delovala v šestmesečni rotaciji (STA, 2015).

[17] Večnamenska ladja Triglav 11. Glavna naloga je nadzor teritorialnih voda Slovenije. Ob namestitvi dodatne opreme pa lahko izvaja tudi naloge podpore delovanja potapljačev in sodeluje pri nalogah zaščite in reševanja na morju (Slovenska vojska, 2015b)

[18] Ankaran je hitra patruljna ladja, ki se uporablja za izvidovanje in nadzor akvatorija (Slovenska vojska, 2015b).

[19] Operacija Naše morje (Mare Nostrum) je humanitarna vojaška operacija italijanske mornarice, katere glavna naloga je bila nadzor mednarodnih voda s ciljem krepitve pomorske varnosti in pomoči beguncem, ki so iz severne Afrike in Bližnjega vzhoda po morju hoteli v Evropo. Slovenska vojska je sodelovala z vojaško ladjo in 41 člani posadke, imela pa je večinoma humanitarno vlogo (Obramba, 2013).

[20] European Union Naval Force Mediterranean (EUNAVFOR MED) je misija Evropske unije, katere namen je identificirati, zajeti in uničiti plovila in druge zmogljivosti, ki jih uporabljajo ali se sumi, da jih uporabljajo tihotapci z ljudmi (European Union External Action, 2015). Je del celovitega pristopa Evropske unije in mednarodne skupnosti, da se reši problem tihotapljenja ljudi in ilegalnih migracij v regiji (STA, 2015b).

4.2 Slovenija in zračna domena

Za zagotavljanje dostopa in uporabe zračne domene je najprej pomembna učinkovita obramba lastnega zračnega prostora. Nadzor zračnega prostora glede na vlogo v bojnem delovanju slovenske vojske spada pod sile za podporo poveljevanja. Zračna obramba Slovenije poleg nadzora zračnega prostora zajema še sistem zračnega poveljevanja in kontrole ter aktivno in pasivno zračno obrambo (Furlan in drugi 2006, 62).

Nacionalni predpisi, ki služijo kot podlaga za nadzor in kontrolo zračnega prostora, so Resolucija o strategiji nacionalne varnosti Republike Slovenije, Zakon o obrambi, Zakon o letalstvu in Uredba o načinu izvajanja nadzora zračnega prostora (Vidergar 2010, 51–3).

Ker Slovenija nima lastnih bojnih letal in ker varovanje zračnega prostora predstavlja veliko finančno breme tudi po nakupu letal[21], se je Slovenija v okviru zveze Nato dogovorila za operacije varovanja zračnega prostora (air policing) s strani partnerskih držav. Tako slovenski zračni prostor od leta 2007 varujejo italijanske zračne sile, od leta 2015 pa tudi madžarske (Obramba, 2014). Operacije varovanja zračnega prostora spadajo pod in so ključna naloga Natovega integriranega sistema zračne obrambe (Nato Integrated Air and Missile Defence System – NATINAMDS) (Nato, 2015č).

Eden od pomembnejših projektov, pri katerem sodeluje Slovenija na področju zračne domene, je Natov sistem AGS. Gre za sistem za opazovanje tal iz zraka s pomočjo brezpilotnih letal Global Hawk, ki bo omogočal poveljnikom sliko položaja na tleh interesnih območij. Leta 2009 je bila ustanovljena Natova Zavezniška agencija za opazovanje tal (Alliance Ground Surveillance Management Agency – NAGSMA), ki je odgovorna za nabavo zmogljivosti sistema AGS. Leta 2012 je nato 15 od 28 članic zveze Nato podpisalo pogodbo za nakup petih brezpilotnih letal Global Hawk. Ena od teh držav je tudi Slovenija, ki je za sistem prispevala 6,8 milijona evrov. Prvo brezpilotno letalo je bilo predstavljeno junija letos, začetno operativno sposobnost pa naj bi sistem dosegel leta 2017 (Obramba, 2015).

Slovenija je tudi del programa Strateških zračnih zmogljivosti (Strategic Airlift Capability – SAC), kjer je še 14 ostalih držav članic in dve partnerski državi. Preko tega programa so bila kupljena tri strateška transportna letala Boeing C-17 (Nato, 2015i). Sodelovanje v tem programu je za Slovenijo pomembno, ker so strateške zračne zmogljivosti ena od zahtev

[21] Ura letenja enega samega letala stane okrog 80 tisoč evrov (Siol.net, 2014)

zveze Nato. Slovenija je uporabila 110 ur letenja v obdobju treh let, kar predstavlja približno dvoodstotni delež celotne uporabe. Ure so bile porabljene za strateški transport vojakov, opreme, humanitarne potrebe in potrebe EU (Bokal 2014, 28–9).

4.3 Slovenija in vesolje

Ker zveza Nato nima svoje vesoljske politike, vesoljskih struktur in ne razvija svojih vesoljskih zmožnosti, je delovanje Slovenije na področju vesolja v okviru zveze Nato minimalno. Slovenija tudi nima kapacitet, ki bi jih zveza Nato trenutno lahko koristila. Kljub temu pa je Slovenija zelo dejavna na vesoljskem področju, precej bolj kot bi pričakovali glede na to, da je bilo v preteklosti raziskovanje vesolja rezervirano za ekonomsko najmočnejše države sveta.

Slovenija je že zgodovinsko povezana z vesoljem preko enega od pionirjev kozmonavtike, vesoljskih poletov in tehnologij Hermana Potočnika Nordunga. Poleg tega imamo tudi nekaj vesoljcev slovenskega porekla in tudi pomembnih strokovnjakov za vesolje (Ministrstvo za gospodarski razvoj in tehnologijo, 2015).

O našem aktivnem udejstvovanju na področju vesolja pričajo tudi številne ustanove, ki so aktivne na področju vesolja, in dosežki, kot so center odličnosti Vesolje-SI s svojo zemeljsko postajo in satelitom v razvoju, Univerza v Mariboru (FERI) s svojimi dolgoletnimi izkušnjami in satelitom v razvoju, Center Planica v sodelovanju z Inštitutom Jožeta Štefana, dolgoletno sodelovanje podjetja Dewesoft z ameriško vesoljsko agencijo NASA in aplikacije podjetja Sinergise na osnovi satelitskih posnetkov. Slovenija je od leta 2009 tudi sodelujoča država Evropske vesoljske agencije (Ministrstvo za gospodarski razvoj in tehnologijo, 2015).

4.3.2 Evropska vesoljska agencija - ESA

Evropska vesoljska agencija (European Space Agency – ESA) je medvladna organizacija, ki je bila ustanovljena leta 1975. Danes ESA združuje 22 članic in 5 sodelujočih držav, ki nimajo polnopravnega članstva. Glavni namen je zagotavljati in promovirati, v izključno

mirne namene, sodelovanje evropskih držav na področju raziskovanja vesolja, vesoljskih tehnologij in njihovih možnih aplikacij (European Space Agency, 2015b). ESA je odgovorna za razvoj usklajene vesoljske politike in z njo povezane gospodarske politike, tako da predlaga cilje na vesoljskem področju za države članice in skrbi za integracijo nacionalnih programov z evropskim vesoljskim programom. Področja, na katerih je aktivna ESA, so: vesoljski poleti s človeško posadko, projekt mednarodne vesoljske postaje, raziskovanje Zemlje, Lune ter ostalega vesolja ter številne raziskave na področju vesoljske znanosti in komercialne izstrelitve telekomunikacijskih satelitov (European Space Agency 2015a, 6–9).

4.3.3 Slovenija in ESA

Slovenija ima status sodelujoče države v ESI od leta 2009. Od leta 2010 tako sodeluje v petletnem Programu za evropske sodelujoče države (Programme for European Cooperation States – PECS). Ker Slovenija še ni polnopravna članica ESE, ima zelo omejene možnosti sodelovanja v večini njenih programov. Slovenija je morala kot članica po veljavnem sporazumu poravnati tudi vsakoletne finančne obveznosti, tako da je vsako leto prispevala nekaj več kot milijon evrov, večino teh sredstev pa so potem prejeli slovenski izvajalci projektov znotraj ESE. Trenutno se financira 25 slovenskih projektov v skupni vrednosti več kot pet milijonov evrov. Gre za projekte na področjih znanosti o vesolju, opazovanja zemlje in področju tehnologij (Ministrstvo za gospodarski razvoj in tehnologijo, 2015) Letos se Sloveniji izteče petletno obdobje PECS, zato se je morala Slovenija odločiti, ali zaprosila za polnopravno članstvo, ki bi Sloveniji omogočilo dostop do vseh delovnih teles in dogodkov, kjer bi imeli interes. Polnopravno članstvo bi Sloveniji omogočilo tudi sodelovanje pri dejavnostih, ki jih doslej sicer že financira[22]. Polnopravno članstvo pa bi omogočilo tudi aktivno sodelovanje pri teh programih oziroma projektih (Ministrstvo za gospodarski razvoj in tehnologijo, 2015). Slovenska vlada je letos tako sprejela izhodišča za sodelovanje Slovenije v ESI kot polnopravni članici in pooblastila ministrstvo za gospodarski razvoj in tehnologijo, da v imenu Slovenije poda prošnjo za pristop. Nadaljnje sodelovanje Slovenije v ESI pozdravlja tudi gospodarstvo, saj naj bi to imelo dolgotrajne neposredne pozitivne učinke, zagotovilo naj bi nova delovna mesta in ustvarilo dodano vrednost podjetjem (RTVSLO,

[22] Slovenija posredno financira naslednje dejavnosti v vesolju: navigacijski sistem EU Galileo, sistem EU za opazovanje zemlje Copernicus, mednarodne satelite Eumestat, komunikacijske satelite Eutelstat, itd. (Ministrstvo za gospodarski razvoj in tehnologijo, 2015).

2015). Če bo Slovenija nadaljevala članstvo v ESI kot polnopravna članica, je Ministrstvo za gospodarski razvoj in tehnologijo predlagalo ustanovitev Sveta Republike Slovenije za vesoljsko politiko in Službe Republike Slovenije za vesolje in vesoljske tehnologije, v poštev pa bi prišla tudi izdelava Strategije Republike Slovenije o vesolju in vesoljskih tehnologijah (Ministrstvo za gospodarski razvoj in tehnologijo, 2015).

4.3.4 Center odličnosti Vesolje-SI

V zadnjih letih smo priča občutnemu znižanju stroškov razvoja vesoljskih tehnologij in vse večji uporabi mikro in nano satelitov, kar pomeni, da je udejstvovanje na tem področju postalo dostopno tudi drugim akterjem, ne le velikim državam in industrijskim konglomeratom. V ta namen je bil v Sloveniji ustanovljen Center odličnosti Vesolje-SI, ki je sestavljen iz akademskih ustanov in visoko tehnoloških malih in srednje velikih podjetij. Združuje akademske, znanstvene in tehnološke potenciale v Sloveniji in omogoča konkurenčno sodelovanje pri vesoljskih raziskavah in misijah (Vesolje-SI, 2015). Center odličnosti Vesolje-SI deluje na naslednjih področjih (Vesolje-SI, 2015):

- daljinsko zaznavanje,
- vremenoslovje,
- astrofizika,
- tehnologije mikro in nano satelitov,
- sodelovanje v mednarodnih vesoljskih misijah,
- razvoj multidisciplinarnega laboratorija za testiranje vesoljskih tehnologij,
- satelitske komunikacije, hibridne antene in radarske tehnologije,
- prenos vesoljskih tehnologij na zemeljske aplikacije.

4.4 Slovenija in kibernetski prostor

Tako kot v vseh ostalih državah članicah zveze Nato in v zvezi Nato samo, so tudi slovenska nacionalna varnost, blaginja in gospodarstvo odvisni od nemotenega dostopa in uporabe kibernetskega prostora. Tako kot ostali subjekti je tudi Slovenija tarča modernih kibernetskih

groženj in je kot taka odvisna od učinkovite kibernetske obrambe. Slovenija še nima nacionalne strategije za kibernetsko obrambo, ki bi natančno in sistematsko urejala to področje. Operativne zmogljivosti za odzivanje na kibernetske grožnje obstajajo, čeprav so kadrovsko in funkcionalno precej podhranjene, poleg tega pa Slovenija nima organa na strateškem nivoju, ki bi skrbel za koordinacijo. V preteklih letih se je v Sloveniji posvečalo zelo malo pozornosti kibernetski varnosti, vendar je po podatkih SI-CERT razvidno, da smo priča ogromnemu povečanju obravnavanih incidentov (iz 323 leta 2008, na 2060 leta 2014), kar predstavlja povečano grožnjo kibernetski varnosti v Sloveniji (SI-CERT 2015, 12).

4.4.1 Nacionalna normativna podlaga na področju kibernetske varnosti

Omrežna in informacijska varnost je v slovenski zakonodaji obravnavana v več zakonih. Glavni zakon, ki opredeljuje kazniva dejanja, in sankcije je kazenski zakonik Republike Slovenije. Poleg njega področje omrežne in informacijske varnosti pokrivajo še Zakon o elektronskih komunikacijah, Zakon o elektronskem poslovanju in elektronskem podpisu. Slovenija ima tudi komisijo za informacijsko varnost, ki je bila imenovana leta 2008. Sestavljena je iz predstavnikov ministrstva za javno upravo, ministrstva za notranje zadeve, ministrstva za obrambo, ministrstva za zunanje zadeve, Slovenske obveščevalno-varnostne agencije in Urada vlade Republike Slovenije za varovanje tajnih podatkov (Urad vlade RS za varovanje tajnih podatkov, 2015). Glavne naloge Komisije za informacijsko varnost so (Urad vlade RS za varovanje tajnih podatkov, 2015):

- priprava tehničnih in normativnih rešitev za varovanje tajnih podatkov v komunikacijskih in informacijskih sistemih (KIS),
- določitev primernih načinov in postopkov za identifikacijo in overitev dostopa uporabnikov v KIS,
- potrjevanje šifrirnih sistemov za uporabo v KIS,
- priprava zahtev za povezovanje KIS,
- priprava varnostnih zahtev za izvajanja zaščite proti neželenemu elektromagnetnemu sevanju.

Omeniti velja Resolucijo o strategiji nacionalne varnosti Republike Slovenije, ki je temeljni razvojno-usmerjevalni dokument na področju nacionalne varnosti. V njej so opredeljeni interesi in cilji Slovenije, viri ogrožanja, načini odzivanja na ta ogrožanja in organiziranost sistema nacionalne varnosti. Resolucija kot enega nadnacionalnih virov ogrožanja poleg terorizma, nedovoljene dejavnosti na področju konvencionalnega orožja, orožij za množično uničevanje in jedrske tehnologije, organiziranega kriminala, nezakonitih migracij, dejavnosti tujih obveščevalnih služb in vojaških groženj navaja v točki 4.2.5 tudi kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov. Zaradi močne odvisnosti od neprekinjenega delovanja informacijskih sistemov, motnje v delovanju pomenijo resno grožnjo za javni in zasebni sektor, predvsem pa za ključne funkcije države in družbe. V točki 5.3.5 je v resoluciji opredeljeno odzivanje na kibernetske grožnje. Slovenija bo kot odziv na kibernetske grožnje izdelala nacionalno strategijo za odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij in sprejela potrebne ukrepe za zagotavljanje učinkovite kibernetske obrambe. Kot eno od prioritet na tem področju opredeljuje ustanovitev nacionalnega koordinacijskega organa za kibernetsko varnost (Pravno-informacijski sistem, 2010).

Naslednji relevanten dokument, ki se nanaša na kibernetski prostor je Obrambna strategija Republike Slovenije. Obrambna strategija je temeljni razvojno-usmerjevalni dokument države na obrambnem področju in kot tak izhaja iz Resolucije o strategiji nacionalne varnosti Republike Slovenije. Tudi obrambna strategija kot eno od varnostnih groženj in tveganj na obrambnem področju prepozna kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov. Tako se bodo tudi na obrambnem področju izvajali ukrepi za zagotovitev učinkovitih zmogljivosti kibernetske varnosti, posebna pozornost pa bo namenjena usklajenosti in celovitosti ukrepov za zaščito informacijsko-komunikacijskih sistemov in druge podobne infrastrukture v državi. Pomembno je tudi, da odzivanje Slovenije na grožnje in tveganja za nacionalno in mednarodno varnost temelji na skupnem delovanju znotraj ZN, EU, Organizacije za varnost in sodelovanje v Evropi (OVSE) in znotraj zveze Nato (Ministrstvo za obrambo, 2012).

Slovenija nima nacionalne strategije o kibernetski obrambi. Leta 2014 je bil v javno razpravo poslan osnutek Strategije kibernetske varnosti. Marca 2015 je bila objavljena zadnja verzija (v 2.5) osnutka Nacionalne strategije kibernetske varnosti. Glavni namen je urediti področje zagotavljanja kibernetske varnosti. Strategija nastaja v okviru medresorske delovne skupine na ministrstvu za izobraževanje, znanost in šport. Kot je zapisano v osnutku strategije, je glavni cilj vzpostavitev celovitega sistema zagotavljanja kibernetske varnosti, ki bo kot eden

ključnih integralnih dejavnikov nacionalne varnosti v Sloveniji zagotovil odprt, varen in varovan kibernetski prostor ter tako nudil podporo ključnim funkcijam države in predstavljal osnovo za konkurenčno gospodarstvo in blaginjo posameznikov in celotne družbe. Glavni cilj je do leta 2020 zagotoviti učinkovit in delujoč sistem za zagotavljanje kibernetske varnosti, ki bo preprečeval in odpravljal posledice varnostnih incidentov. Predpostavlja ustanovitev nacionalnega organa za kibernetsko varnost na strateški ravni, ki bo skrbel za koordinacijo vseh zmogljivosti za zagotavljanje kibernetske varnosti na nižjih nivojih. Na operativnem nivoju predpostavlja delovanje naslednjih organov: SI-CERT na nacionalni ravni, MORS-CERT na obrambnem področju in področju varstva pred naravnimi in drugimi nesrečami, SIGOV-CERT za sisteme javne uprave in Policije na področju zatiranja kibernetskega kriminala. Za dosego tega cilja se bodo uresničili naslednji podcilji: varnost državljanov, razvoj in gospodarstvo, zanesljivo delovanje kritične infrastrukture, zatiranje kibernetskega kriminala, obrambna sposobnost države, krepitev nacionalne kibernetske varnosti skozi mednarodno sodelovanje ter vzpostavitev nacionalnega organa, zadolženega za kibernetsko varnost. Te cilje bo Slovenija dosegla s preprečevanjem, odzivanjem in ozaveščanjem (Ministrstvo za izobraževanje, znanost in šport, 2015).

4.4.2 SI-CERT

SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Deluje od leta 1995 v okviru javnega zavoda Arnes (SI-CERT 2015, 6). Glavne naloge so (SI-CERT 2015, 6–7):

- upravljanje nacionalne kontaktne točke za odzivanje na incidente,
- dejavnosti pri zaščiti nacionalne internetne infrastrukture,
- sodelovanje z operaterji, ponudniki storitev in Agencijo za komunikacije in omrežne storitve RS,
- koordinirano odzivanje na incidente s Centrom za računalniško preiskovanje Generalne policijske uprave,
- mednarodno sodelovanje in dejavnosti,

- izgradnja laboratorija za analizo škodljive kode,
- obveščanje javnosti o tveganjih in njihovem zmanjševanju,
- usposabljanje in izobraževanje kadra v drugih ustanovah države,
- sodelovanje pri odzivanju na incidente na področju kritične infrastrukture,
- sodelovanje z drugimi deležniki v državi z namenom izboljšanja stanja informacijske varnosti.

Leta 2014 so na SI-CERT začeli z usposabljanjem pripadnikov Slovenske vojske na področju obravnave in preiskovanja računalniških incidentov. Slovenska vojska ustanavlja kapacitete za odzivanje na omrežne incidente v vojski, za kar je potreben kader s praktičnim znanjem pri spopadanju s poskusi zlorabe obrambne informacijske infrastrukture (SI-CERT 2015, 27).

Slovenska vojska je sicer že leta 2014 napovedala tudi ustanovitev osemčlanske enote, ki bi skrbela za kibernetsko obrambo slovenskih vojaških sistemov, a jim te enote do sedaj še ni uspelo sestaviti, glavni razlog pa je pomanjkanje kadra z ustreznim znanjem. Vzpostavitev enote je še vedno planirana letos, glavne naloge enote pa bodo usposabljanje, analiza varnostnih tveganj, sodelovanje pri zaznavanju in odpravi posledic incidentov, izvajanje analiz napadov in sodelovanje na vojaških vajah na področju kibernetske varnosti doma in v tujini (STAkrog 2015).

SI-CERT je v letu 2014 sodeloval na dveh vajah iz kibernetske varnosti. Vaja Cyber Europe 2014 je bila organizirana s strani Evropske agencije za omrežno in informacijsko dejavnost ENISA, obsegala pa je tehnično, operativno in strateško raven. Vaja Cyber Coalition 14 pa je potekala v okviru zveze Nato in je vključevala nacionalne odzivne centre, šlo pa je za preverjanje zmožnosti odzivanja na državni ravni (SI-CERT 2015, 28).

5 ZAKLJUČEK

Namen diplomskega dela je bil odgovoriti na dve povezani raziskovalni vprašanji; kakšna je vloga Nato pri zagotavljanju dostopa in uporabe globalnega javnega dobra ter kakšna je vloga Slovenije znotraj zavezništva in izven.

Zveza Nato se je skozi zgodovino močno spremenila. Postala je večja, močno je razširila svoje območje delovanja, na takšen ali drugačni način se je povezala z državami celega sveta. Njen glavni namen še vedno ostaja kolektivna varnost držav članic, poleg tega pa imata pomembno vlogo krizno upravljanje in partnerstvo. Čeprav te osnovne naloge zveze ostajajo enake, pa je v zadnjih letih zveza prepoznala pomen globalnih javnih dober in kako zagotovljen dostop do teh področij in njihova uporaba vplivata na njeno sposobnost doseganja zastavljenih ciljev.

Pomorska domena ima velik pomen za zvezo Nato in tudi za varnost in blagostanje držav članic tako z vidika pomorske trgovine kot tudi sredstva, prek katerega je zvezi Nato omogočeno delovanje na oddaljenih območjih. Zveza Nato že sedaj igra pomembno vlogo pri zagotavljanju dostopa in uporabe pomorske domene, ta vloga pa se bo v prihodnosti le še povečevala. Zato bodo pomembne nadaljnja implementacija njene pomorske strategije, povečanje prisotnosti svojih sil na morju in nadaljnjo izvajanje pomorskih operacij. Zveza Nato vidi pomembno vlogo tudi kot zgled ostalim mednarodnim subjektom pri spoštovanju zakonov, pravil in norm mednarodnega pomorskega prava, prav tako pa se ob postopnem odpiranju arktičnega kroga v prihodnosti vidi kot posrednica med državami, ki imajo svoje interese na tem območju.

Lahko rečemo, da ima danes v zraku zveza Nato svetovno premoč in kot taka pomembno vlogo pri zagotavljanju dostopa in uporabe zračne domene. Vendar pa ta premoč ni samoumevna in v prihodnosti ne bo zagotovljena brez nadaljnjega razvoja. V mednarodnem okolju se nenehno pojavljajo novi potencialni sovražniki, ki lahko ob pojavu vse cenejših in lahko dostopnih učinkovitih protiletalskih zmogljivosti ogrozijo dostop in zmožnost uporabe zračne domene. Poleg tega tudi ostale svetovne države razvijajo zelo učinkovite sisteme protiletalske obrambe. Zato je cilj zveze Nato nadaljnji razvoj svojih zračnih zmogljivosti, posodobitev obstoječih zmogljivosti, usposabljanje kadra, sodelovanje z državami nečlanicami, še večja interoperabilnost in standardizacija ter vpeljava novih tehnologij (primer brezpilotnih letalskih sistemov) v svoje dejavnosti.

Vesoljska domena je zelo specifična in vloga zveze Nato na tem področju bo v veliki meri odvisna od njenih korakov v prihodnosti. Trenutno zveza Nato nima svojih vesoljskih zmogljivosti, nima vesoljske politike in je na tem področju odvisna od posameznih držav članic. Po mojem mnenju je njena trenutna vloga na vesoljskem področju majhna, dodatno »težavo« pa predstavlja dejstvo, da države članice pospešeno razvijajo vesoljske zmogljivosti

na nacionalni ravni in v okviru drugih mednarodnih organizacij, predvsem Evropske vesoljske agencije in EU. Ob nadaljevanju tega trenda se pojavlja možnost, da se bo vloga zveze Nato na področju vesolja še dodatno zmanjšala in marginalizirala. Zato mora biti cilj zveze Nato ustvariti lastno vesoljsko politiko, uskladiti razvoj vesoljskih zmožnosti posameznih držav članic s svojimi cilji in bodočimi zmogljivostmi ter poiskati svojo vlogo v mednarodni skupnosti in na tem področju začeti intenzivno sodelovati z drugimi mednarodnimi organizacijami.

Zveza Nato je v preteklih nekaj letih prepoznala izjemen pomen kibernetskega prostora za svoje delovanje in tako že naredila odločne korake za zagotavljanje dostopa in uporabe te domene. Na strateški ravni je v svojem najnovejšem strateškem konceptu poudarila pomen učinkovite kibernetske obrambe in kibernetske grožnje označila kot potencialni aktivator kolektivne obrambe po 5. členu Washingtonske pogodbe. Razvila je ustrezno področno politiko za kibernetsko obrambo ter pospešeno razvija svoje kibernetske zmogljivosti. Ustanovila je tudi center odličnosti za kibernetsko področje, ki skrbi za raziskave in razvoj na tem področju. Poleg tega pa zveza Nato pomaga državam članicam pri razvoju lastnih nacionalnih zmogljivosti za kibernetsko obrambo, hkrati pa sodeluje tudi z vse več državami nečlanicami na področju kibernetske obrambe.

Vloga Slovenija tako znotraj, kot izven zveze Nato je precej različna glede na posamezno domeno globalnega javnega dobra. Glede na našo geografsko lego, naše zmogljivosti in v končni fazi tudi glede na naše interese je logično, da lahko nekje prispevamo več, nekje manj.

Pri pomorski domeni smo precej omejeni s svojimi zmogljivostmi, saj so naše pomorske sile primerne predvsem za lokalno in delno regionalno delovanje, medtem ko za globalno delovanje niso zadostne. Večnamenska ladja Triglav 11 bi v prihodnosti lahko bila uporabljena v Natovih operacijah na področju zahodne, južne in vzhodne Afrike. Do sedaj smo na mednarodnem področju pomagali pri varovanju mednarodnih voda in pomoči beguncem, v prihodnosti pa bo Slovenija pomagala EU pri reševanju problema tihotapljenja ljudi in ilegalnih migracij v sredozemski regiji prek misije EUNAVFOR MED.

Tudi na področju zagotavljanja dostopa in uporabe zračne domene je Slovenija zelo omejena s svojimi zmogljivostmi. Nimamo svojih bojnih letal, tako da je že varovanje našega zračnega prostora v rokah zveze Nato. Večjo vlogo Slovenije na tem področju v prihodnosti vidim predvsem pri sodelovanju pri projektih na tem področju v smislu razvoja tehnologij in

finančnega prispevka. Primer je sodelovanje Slovenije pri Natovem projektu AGS in najemu strateških zračnih zmogljivosti.

Čeprav Slovenija nima svoje vesoljske politike in nima večjih vesoljskih zmogljivosti, je zelo aktivna na področju razvoja vesoljskih tehnologij in ima veliko vesoljskih strokovnjakov. Trenutno Slovenija zelo aktivno sodeluje z Evropsko vesoljsko agencijo. V prihodnosti je cilj Slovenije polnopravno članstvo v Evropski vesoljski agenciji, kar bi ji omogočilo še intenzivnejše sodelovanje pri vesoljskih projektih. V okviru zveze Nato pa bi Slovenija lahko pomagala pri izdelavi vesoljske politike zveze Nato, s svojim znanjem bi lahko delovala v bodočih Natovih vesoljskih strukturah, s svojim delom na področju razvoja vesoljskih tehnologij pa bi lahko ogromno prispevala pri izgradnji Natovih lastnih vesoljskih zmogljivosti.

V kibernetskem prostoru ima lahko Slovenija precej veliko vlogo pri zagotavljanju dostopa in uporabe, saj ima kibernetske zmogljivosti, vzpostavitev učinkovite kibernetske obrambe pa bi veliko prispevala h kibernetski varnosti v celotni zvezi Nato. Pri kibernetski obrambi zveze Nato je tako, da je močna le toliko kot je močna kibernetska obramba držav članic oziroma najšibkejše države članice. Vendar pa je dejstvo, da je Slovenija v preteklosti to področje precej zapostavljala, ogromen porast dejavnosti na področju kibernetskih groženj pa kaže, da čaka Slovenijo v prihodnosti precej izzivov. Najprej bo potrebna izdelava celovite nacionalne strategije na področju kibernetske obrambe, ki bo sistematično uredila področje in zastavila jasne cilje države. Nato je pomembna vzpostavitev organa za kibernetsko obrambo na strateški ravni, ki bo nadzoroval in usklajeval delovanje vseh nižjih, organov za kibernetsko obrambo. Potrebna bo tudi razširitev in povečanje števila organov na operativni ravni ter njihova posodobitev in nadaljnji razvoj.

Tako zveza Nato kot tudi Slovenija imata določeno vlogo pri reševanju tematike in bosta v prihodnosti to vlogo nedvomno ohranili oziroma jo še povečali. Skozi raziskovanje sem ugotovil, da se zveza Nato vidi kot zelo pomemben akter na področju zagotavljanja dostopa in uporabe globalnega javnega dobra, močno pa se zaveda, da ni edini akter. Krepitev vloge v prihodnosti bo močno odvisna od nadaljnjega razvoja zmogljivosti zveze, razvoja učinkovitih strategij in okrepljenega sodelovanja in povezovanja z drugimi mednarodnimi akterji, ki imajo vpliv na tem področju. Menim, da ima zveza Nato trenutno ogromno vlogo pri pomorski in zračni domeni, na področju kibernetskega prostora je bil v zadnjih letih narejen velik napredek, največ prostora za napredek pa je na področju vesolja.

Slovenija ima glede na svojo velikost in svoje zmogljivosti pričakovano dokaj majhno vlogo na področju zagotavljanja dostopa in uporabe globalnega javnega dobra. Vendar pa je treba poudariti prizadevanja Slovenije za aktivno sodelovanje na vseh štirih področjih. Na pomorskem in zračnem področju smo precej omejeni s svojimi zmogljivostmi, vendar pa imamo ogromen potencial za prispevek na področju kibernetskega prostora in vesolja. Osebno menim, da je naš prispevek lahko precejšen na področju razvoja novih tehnologij in pri sodelovanju naših strokovnjakov na posameznih področjih, kljub temu pa bo največji prispevek Slovenije v zvezi Nato skozi integracije in sodelovanja pri različnih projektih.

6 LITERATURA

1) Allied Command Transformation. 2011. *Assured Access to Global Commons. Final Report.* Dostopno prek: http://www.act.nato.int/globalcommons (29. avgust 2015).

2) Bokal, Luka. 2014. *Pametna obramba- prihodnost NATA.* Diplomsko delo. Ljubljana: Fakulteta za družbene vede.

3) CCDCOE. 2014. *NATO Summit Updates Cyber Defence Policy.* Dostopno prek: https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html (3. september 2015).

4) Cleveland, Harland. 1990. Introducing the Global Commons. *National Forum 70 (1).* Dostopno prek: https://www.questia.com/read/1G1-8571595/introducing-the-global-commons (27. avgust 2015).

5) Delo. 2010. *Sneg in mraz ohromila letalski promet po Evropi.* Dostopno prek: http://www.delo.si/clanek/131219 (25. avgust 2015).

6) European Defence Agency. 2014. *Pooling & Sharing.* Dostopno prek: http://www.eda.europa.eu/what-we-do/eda-priorities/pooling-and-sharing (7. september 2015).

7) European Space Agency. 2015a. *The European Space Agency.* Dostopno prek: http://esamultimedia.esa.int/multimedia/publications/ESA-Presentation/ (9. september 2015).

8) --- 2015b. *Welcome to ESA. ESA's Purpose.* Dostopno prek: http://www.esa.int/ About_Us/Welcome_to_ESA/ESA_s_Purpose

9) European Union External Action. 2015. *EUNAVFOR MED.* Dostopno prek: http://www.eeas.europa.eu/csdp/missions-and-operations/eunavfor-med/index_en.htm (8. september 2015).

10) Furlan, Branimir, Petelin Darko, Toič Bruno, Gutman Albin in Šteiner Alojz. 2006. *Vojaška doktrina.* Ljubljana: Defensor.

11) Grizold, Anton. 2005. *Slovenija v spremenjenem varnostnem okolju.* Ljubljana: Fakulteta za družbene vede.

12) Hafezi, Parisa. 2015. *Iran uses maritime confrontations to project power in Gulf.* Dostopno prek: http://www.reuters.com/article/2015/05/18/us-iran-saudi-gulf-idUSKBN0O31JQ20150518 (4. september 2015).

13) Henson, Robert. 2006. *The rough guide to climate change.* London: Rough Guides.

14) International Affairs Review. 2015. *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security.* Dostopno prek: www.iar-gwu.org./node/65 (2. september 2015).

15) Joint Air Power Competence Centre. 2012. *Filling the Vacuum. A Framework for a NATO Space Policy.* Dostopno prek: http://www.japcc.org/wp-content/uploads/SPP_2012_web.pdf (6. september 2015).

16) --- 2014. *Air & Space Power in NATO. Future Vector Part II.* Dostopno prek: http://www.japcc.org/wp-content/uploads/JAPCC_FV_III_web.pdf (5. september 2015).

17) Kaye, Stuart. 2007. Threats from the Global Commons: Problems of Jurisdiction and Enforcement. *Melbourne Journal of International Law 8 (1).* Dostopno prek: https://www.questia.com/read/1G1-167305293/threats-from-the-global-commons-problems-of-jurisdiction (2. september 2015).

18) Klimburg, Alexander. 2012. *National Cyber Security Framework Manual*. Dostopno prek: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (1. september 2015).

19) *Konvencija Združenih narodov o pomorskem pravu – United Nations Convention on the Law of the Sea.* 1982. Dostopno prek: http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf (29. avgust 2015).

20) Ministrstvo za gospodarski razvoj in tehnologijo. 2015. *ESA*. Dostopno prek: http://www.mgrt.gov.si/si/delovna_podrocja/podjetnistvo_konkurencnost_in_tehnologija/spodbujanje_inovacij_in_tehnoloskega_razvoja/sodelovanje_z_evropsko_vesoljsko_agencijo_esa/esa/ (9. september 2015).

21) Ministrstvo za izobraževanje, znanost in šport. 2015. *Nacionalna strategija kibernetske varnosti. Osnutek, v2.5.* Dostopno prek: http://www.mizs.gov.si/fileadmin/mizs.gov.si/

pageuploads/Informacijska_druzba/pdf/DSi_NSKV_v2.5_20150306.pdf (3. september 2015).

22) Ministrstvo za obrambo. 2012. *Obrambna strategija Republike Slovenije*. Dostopno prek: http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/javne_objave/2012/obr_strategija.pdf (4. september 2015).

23) Nasa. 2014. *Wright Brother's Aircraft.* Dostopno prek: http://wright.nasa.gov/airplane/powered.html (8. september 2015).

24) *Nato Handbook*. 2006. Bruselj: NATO Public Diplomacy Division.

25) Nato Maritime Command. 2015a. *Marcom Factsheet: Operation Ocean Shield.* Dostopno prek: http://www.mc.nato.int/about/Pages/Operation%20Ocean%20Shield.aspx (5. september 2015).

26) --- 2015b. *Operation Active Endeavour.* Dostopno prek: http://www.mc.nato.int/ops/Pages/OAE.aspx (4. september 2015).

27) Nato Shipping Centre. 2015. *About us.* Dostopno prek: http://www.shipping.nato.int/Pages/aboutus.aspx (2. september 2015).

28) Nato. 2010. *Lisbon Summit Declaration.* Dostopno prek: http://www.nato.int/cps/en/natolive/official_texts_68828.htm (2. september 2015).

29) --- 2011a. *Alliance Maritime Strategy.* Dostopno prek: http://www.nato.int/cps/en/natohq/official_texts_75615.htm (4. september 2015).

30) --- 2011b. *Defending the networks. The NATO Policy on Cyber Defence.* Dostopno prek: http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf (3. september 2015).

31) --- 2014a. *The NATO Defence Planning Process.* Dostopno prek: http://www.nato.int/cps/en/natolive/topics_49202.htm (7. september 2014).

32) --- 2014b. *Wales Summit Declaration.* Dostopno prek: http://www.nato.int/cps/en/natohq/official_texts_112964.htm (5. september 2015).

33) --- 2015a. *Alliance Ground Surveillance (AGS).* Dostopno prek: http://www.nato.int/cps/en/natolive/topics_48892.htm (29. avgust 2015).

34) --- 2015b. *Counter-piracy operations*. Dostopno prek: http://www.nato.int/cps/en/natohq/topics_48815.htm (5. september 2015).

35) --- 2015c. *Cyber Security*. Dostopno prek: http://www.nato.int/cps/en/natohq/topics_78170.htm (2. september 2015).

36) --- 2015č. *NATO Air Policing*. Dostopno prek: http://www.airn.nato.int/page5931922/-nato-air-policing.aspx (7. september 2015).

37) --- 2015d. *NATO and Libya*. Dostopno prek: http://www.nato.int/cps/en/natolive/topics_71652.htm# (5. september 2015).

38) --- 2015e. *NATO-Russia Relations*. Dostopno prek: http://www.nato.int/cps/en/natohq/topics_51105.htm (9. september 2015).

39) --- 2015f. *NATO's maritime domain*. Dostopno prek: http://www.nato.int/cps/en/natolive/topics_70759.htm (4. september 2015).

40) --- 2015g. *Operation Active Endeavour*. Dostopno prek: http://www.nato.int/cps/en/natolive/topics_7932.htm (4. september 2015).

41) --- 2015h. *Smart Defence*. Dostopno prek: http://www.nato.int/cps/en/natohq/topics_84268.htm (7. september 2015).

42) --- 2015i. *Strategic Airlift Capability (SAC)*. Dostopno prek: http://www.nato.int/cps/en/natolive/topics_50105.htm (7. september 2015).

43) Obramba. 2013. *Vojaška ladja Triglav kmalu na pot na operacijo Naše morje – Lampedusa*. Dostopno prek: http://www.obramba.com/novice/vojaska-ladja-triglav-kmalu-na-pot-v-operacijo-nase-morje-lampedusa/ (8. september 2015).

44) --- 2014. *Slovenski zračni prostor bodo varovali tudi madžarski lovci*. Dostopno prek: http://www.obramba.com/novice/slovenski-zracni-prostor-bodo-varovali-madzarski-lovci/ (7. september 2015).

45) --- 2015. *Slovenija v projektu Natovih opazovalnih global hawk AGS*. Dostopno prek: http://www.obramba.com/novice/slovenija-v-projektu-natovih-opazovalnih-global-hawk-ags/ (7. september 2015).

46) OECD. 2015. *Extended producer responsibility.* Dostopno prek: http://www.oecd.org/env/tools-evaluation/extendedproducerresponsibility.htm (4. september 2015).

47) Pravno-informacijski sistem. 2010. *Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1).* Dostopno prek: http://www.pisrs.si/Pis.web/pregledPredpisa?id=RESO61# (3. september 2015).

48) Redden, Mark E. in Hughes P. Michael. 2011. Defense Planning Paradigms and the Global Commons. *Joint Force Quarterly (60).* Dostopno prek: https://www.questia.com/read/1G1-275489741/defense-planning-paradigms-and-the-global-commons (28. avgust 2015).

49) Remuss, Nina-Louisa. 2010. *NATO and Space: Why is Space Relevant for NATO?* Dostopno prek: http://www.espi.or.at/images/stories/dokumente/Perspectives/ESPI_Perspectives_40.pdf (7. september 2015).

50) Revija Nato. 2011. *Nove grožnje: kibernetska razsežnost.* Dostopno prek: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/SL/index.htm (2. september 2015).

51) RTVSLO. 2015. *Slovenija bo zaprosila za članstvo v Esi.* Dostopno prek: https://www.rtvslo.si/znanost-in-tehnologija/slovenija-bo-zaprosila-za-clanstvo-v-esi/368866 (9. september 2015).

52) Schmitt N., Michael. 2013. *Talinn Manual on the International Law Applicable to Cyber Warfare*. Dostopno prek: https://ccdcoe.org/tallinn-manual.html (2. september 2015).

53) SI-CERT. 2015. *Poročilo o omrežni varnosti za leto 2014.* Dostopno prek: https://www.cert.si/wp-content/uploads/2015/05/Porocilo-o-omrezni-varnosti_2014.pdf (2. september 2015).

54) Siol.net. 2014. *Ali Evropa potrebuje 28 zračnih obramb?* Dostopno prek: http://www.siol.net/novice/svet/2014/08/ali_evropa_potrebuje_28_zracnih_obramb.aspx (7. september 2015).

55) *Slovenija in NATO.* 2015. Dostopno prek: http://nato.gov.si/slo/ (28. avgust 2015).

56) Slovenska vojska. 2015a. *430. mornariški divizion.* Dostopno prek: http://www.slovenskavojska.si/struktura/430-mornariski-divizion/ (8. september 2015).

57) Slovenska vojska. 2015b. *Mornariška oprema in plovila.* Dostopno prek: http://www.slovenskavojska.si/oborozitev-in-oprema/mornariska-oprema-in-plovila/ (8. september 2015).

58) Spacenews. 2013. *NATO sets Mid-2014 Deadline for Securing Future Satcom Capacity.* Dostopno prek: http://spacenews.com/33025nato-sets-mid-2014-deadline-for-securing-future-satcom-capacity/ (7. september 2015).

59) STA. 2015a. *Slovenia to Join Italy-Led NATO Group.* Dostopno prek: https://english.sta.si/2113316/slovenia-to-join-italy-led-nato-group (5. september 2015).

60) --- 2015b. *Triglav na rednem vzdrževanju, sledi vključitev v mednarodno operacijo v Sredozemlju.* Dostopno prek: https://www.sta.si/2163813/triglav-na-rednem-vzdr zevanju-sledi-vkljucitev-v-mednarodno-operacijo-v-sredozemlju (8. september 2015).

61) STAkrog. 2015. *Slovenska vojska po slabem letu še vedno brez enote za kibernetsko obrambo.* Dostopno prek: https://krog.sta.si/2107658/slovenska-vojska-po-slabem-letu-se-vedno-brez-enote-za-kibernetsko-obrambo (3. september 2015).

62) *Strateški koncept Nata – Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation.* 2010. Dostopno prek: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (2. september 2015).

63) UNODC. 2015. *A transnational organized crime threat assessment. Full report.* Dostopno prek: www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_ 2010_low_res.pdf (10. september 2015).

64) Urad vlade RS za varovanje tajnih podatkov. 2015. *Komisija za informacijsko varnost.* Dostopno prek: http://www.uvtp.gov.si/si/delovna_podrocja/varnost_kis/komisija_za_ informacijsko_varnost/ (2. september 2015).

65) Vegič, Vinko. 2005. Vloga in funkcije Nata po koncu hladne vojne. *V Sodobni vojaški izzivi,* ur. Anton Bebler, 181-200. Ljubljana: Fakulteta za družbene vede.

66) Vesolje-SI. 2015. *Center odločnosti vesolje, znanost in tehnologije. Predstavitev.* Dostopno prek: http://www.space.si/o-centru/predstavitev/ (9. september 2015).

67) Vidergar, Aleksander. 2010. *Sistem nadzora in zaščite zračnega prostora Republike Slovenije v sklopu Natove kolektivne zaščite zračnega prostora.* Magistrsko delo. Ljubljana: Fakulteta za družbene vede.

68) Wikipedia. 2015. *Defensive Aids System.* Dostopno prek: https://en.wikipedia.org/wiki/Defensive_aids_system (9. september 2015).

69) Yost, David S. 1998. *NATO Transformed. The Alliance's New Roles in International Security.* Washington: United States Institute for Peace.