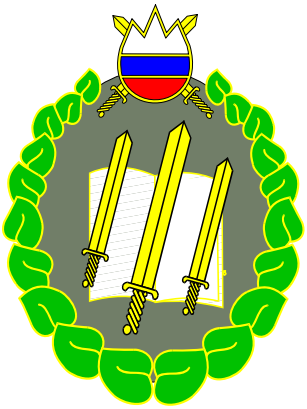
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
SLOVENSKA VOJSKA
PDRIU – POVELJNIŠKOŠTABNA ŠOLA
5. generalštabni program izobraževanja in usposabljanja



VPLIV ZMOGLJIVOSTI OMREŽNEGA DELOVANJA NA TRANSFORMACIJO SLOVENSKE VOJSKE

Slušatelj:
ppk Zoran JANKOVIČ

Mentor:
dr. Uroš SVETE

Poljče, september 2008

POVZETEK

Na izzive informacijske dobe in postmodernega vojskovališča, polnega asimetričnih virov ogrožanja, se je zavezništvo, izhajajoče iz svojega poslanstva, odzvalo z novimi koncepti in novimi zmogljivostmi. Spremembe v okolju, asimetrične grožnje, multinacionalnost izvajanja operacij in razvoj komunikacijske ter informacijske tehnologije so zahtevali izvedbo transformacije zavezništva in njenih članic. Eden ključnih izzivov in področij transformacije predstavlja vprašanje izmenjave informacij v okolju sodobnega vojskovališča in doseganje informacijske prevlade. V nalogi je skozi pregled strateških dokumentov, sprejete zaveze Republike Slovenije ter operativne zahteve SV in zavezništva, predstavljen vpliv zmogljivosti omrežnega delovanja na transformacijo Slovenske vojske v vseh njenih segmentih s težiščem na spremembah v komunikacijskih in informacijskih sistemih, ter ključni izzivi, s katerimi se pri realizaciji transformacije srečuje Slovenska vojska.

Ključne besede:
transformacija, informacijska prevlada, zmogljivosti omrežnega delovanja, cilji sil, komunikacijski in informacijski sistemi, NATO-ve odzivne sile, omrežna in informacijska infrastruktura, operacije, ki temeljijo na učinkih.

SUMMARY

We live in a new information age and the age of post modern warfare. Challenges of new information age, full of asymmetric threats, joint and multinational environment and forces conducting operations and development of communications and information systems demanded from the Alliance and national defence forces transformation through new doctrines, strategies, concepts and capabilities. One of the greatest challenge of transformation is to reach interoperability of communications and information systems and capability to exchange information from strategic down to the tactical level and to gain information superiority. Through the different strategic documents, operational demands of Alliance and Slovenian armed forces I will try to present the impact of network enabled capabilities to changes, needed in all segments of Slovenian armed forces with the center of gravity on communications and information systems through the transformation and the challenges we are going to meet through the realisation.

Keywords:
NATO network enabled capability, Network centric warfare, Transformation, Network superiority, C4ISR, communications and information systems, NATO Response Forces, NII – networking and information infrastructure, Effects Based Operations

KAZALO

1. UVOD

Vojskovališče se je v zadnjem, postmodernem obdobju izjemno spremenilo. Spremenili so se viri ogrožanja, povečala so se tveganja. Med vsemi dejavniki, ki vplivajo na vojskovališče, je eden največjih napredkov zaznan ravno na področju razvoja komunikacijskih, informacijskih in senzorskih sistemov. Le-ti zagotavljajo hitrejšo zaznavo cilja in nasprotnika, večjo preciznost oborožitvenih sistemov, zmanjšujejo porabo streliva, hkrati pa omogočajo enotno zavedanje o situaciji na bojišču z enotno sliko bojišča in s tem usklajeno delovanje koalicijskih (zavezniških) sil.

Že v preteklem obdobju, ko še operacije niso bile tako kompleksne in ni bilo toliko različnih udeležencev v različnih fazah operacij, so imele članice zavezništva veliko težav pri zagotavljanju interoperabilnosti (povezljivosti) sistemov, saj so gradile nacionalne sisteme v skladu s svojimi potrebami, merili, zahtevami in standardi. Kompleksnost se je zaradi izjemnega razvoja tehnologije in storitev, ki jih nudita komunikacijska ter informacijska tehnologija, zaradi širitve zavezništva in vse večjega števila akterjev, ki sodelujejo v operacijah zavezništva (kriznega odzivanja) še povečala. Reševanju povezljivosti C4I sistemov in doseganju informacijske nadvlade NATO in njegove članice posvečajo vedno več pozornosti. Razvoj C4I sistemov in njihovo uvajanje v operativno uporabo pa vpliva ne le na transformacijo nacionalnih obrambnih struktur, ampak na transformacijo zavezništva kot celote.

Osnovni namen razvoja zmogljivosti omrežnega delovanja je njihova sposobnost, ki omogoča izvajanje aktivnostih na operacijah na nov, drugačen, boljši način, kar prevedeno v vojaško terminologijo pomeni na podlagi novih operativnih konceptov. V tem smislu razvoj zmogljivosti omrežnega delovanja zahteva razmišljanje, kako lahko zavezništvo, raznoliko po sestavi, strukturi, usposobljenosti in opremljenosti, izvaja operacije v prihodnosti ter v kateri smeri naj se razvijajo nacionalne zmogljivosti, ki prispevajo svoje kontingente pri izvajanju operacij. Razvoj zmogljivosti omrežnega delovanja tako postaja eden ključnih področij transformacije, ki ne vpliva le na spremembe na področju tehnoloških rešitev komunikacijskih, informacijskih in senzorskih sistemov pri zagotavljanju informacijske prevlade, pač pa vpliva na spremembe na vseh ključnih področjih transformacije nacionalnih zmogljivosti in zavezništva kot celote. V nadaljevanju želim prikazati vpliv zmogljivosti omrežnega delovanja na različna področja

transformacije SV s poudarkom na spremembah, potrebnih pri razvoju omrežne in informacijske infrastrukture.

Za temo sem se odločil, ker se tudi sam nahajam na enem od odgovornejših mest, povezanih z razvojem in zagotavljanjem storitev C4I v SV, hkrati pa smatram, da iz različnih razlogov, predvsem pa dilem, povezanih z razmejitvijo pristojnosti in odgovornosti za razvoj C4I sistema za potrebe SV med Generalštabom SV in ministrstvom za obrambo (MORS) nimamo ustreznega strateškega dokumenta, ki bi na celovit način opredeljeval strategijo razvoja tega področja. Hkrati pa z zmogljivostmi omrežnega delovanja (Network enabled capabilities – NEC) niso seznanjeni oziroma mnogi ključni akterji v procesu planiranja zmogljivosti temu vprašanju ne posvečajo potrebne pozornosti. To področje je prepuščeno le tistemu segmentu, ki se ukvarja s tehnološkim delom komunikacijske in informacijske infrastrukture, ki naj bi zagotavljala povezljivost (interoperabilnost) teh sistemov v enoten sistem zavezništva.

V okviru naloge bom poskušal predstaviti osnovne pojme, povezane z zmogljivostmi omrežnega delovanja, obstoječe stanje zmogljivosti omrežnega delovanja v SV, predstaviti nacionalne zaveze, ki jih je dala RS zavezništvu v zvezi z implementacijo zmogljivosti, in predstaviti sledi teh zavez v nacionalnih strateških dokumentih, predstaviti področja transformacije, opredeljena v dokumentih zavezništva s poudarkom na vplivu omrežnega delovanja na razvoj teh področij, predvsem pa področja omrežne in informacijske infrastrukture v SV. V zaključku bom predstavil ugotovitve in izzive, ki čakajo RS in SV pri razvoju teh zmogljivosti ter njihovi implementaciji; opisal bom dileme in spoznanja, do katerih sem prišel pri preučevanju literature ter verificiral hipoteze.

Pri raziskavi teme sem uporabil le javno dostopne vire in vire, ki niso označeni s stopnjo tajnosti. Tako se v zaključni nalogi ne bom dotikal podrobnosti, ki so opredeljene v dokumentih s stopnjo tajnosti, kar predstavlja omejitev pri zagotavljanju celovitega vpogleda v problematiko tega področja.

1.1 HIPOTEZA, DELOVNO VPRAŠANJE, TEZA ALI TRDITEV

V razmerah sodobnega vojskovanja in uporabe ekspedicijskih vojaških ter nevojaških zmogljivosti, ki izvajajo aktivnosti v okviru operacij kriznega odzivanja, se nahaja vse več različnih akterjev, ki morajo biti medsebojno povezani. Med zmogljivostmi iz RS, ki na teh operacijah sodelujejo, so tudi enote SV ter pripadniki drugih vladnih in nevladnih

organizacij. Zaradi novih varnostnih izzivov, načina delovanja nasprotnika in prilagajanja zavezniških zmogljivosti na te spremembe ter zagotavljanja informacijske prevlade, so se članice zveze NATO z zavezami Praške konference PCC (angl. Prague Capability commitments) obvezale, da bodo zagotovile nove zmogljivosti, ki bodo usmerjene v realizacijo sprejetih ciljev transformacije zavezništva, v okviru tega pa vseh zahtev, povezanih s podporo C4ISR sistemov.

Slovenska vojska je na poti za doseganje zmogljivosti omrežnega delovanja posamezne korake že izvedla. Vprašanja, ki se zastavljajo, so ali je RS tem vprašanjem namenila zadovoljive vire, predvsem pa dovolj pozornosti vsem področjem transformacije in njihovi usklajenosti. Izhajajoč iz vsebine naloge in teh vprašanj, postavljam naslednjo hipotezo:

- zmogljivosti omrežnega delovanja zajemajo mnogo širše področje transformacije SV in zavezništva kakor le transformacijo komunikacijskega in informacijskega sistema SV in zavezništva.

1.2 NAMEN IN CILJI RAZISKAVE

Področje, ki zajema omrežno delovanje, je izjemno široko, zato je obstajala možnost, da se v nalogi presežejo okviri želenega. Namen naloge ni obdelati področja le s tehnološkega vidika in vpliva le-tega na transformacijo, pač pa je osnovni namen in temeljni cilj te naloge ugotoviti stopnjo implementacije ciljev sil v vseh segmentih, s težiščem na ciljih sil, ki neposredno vplivajo na zmogljivosti omrežnega delovanja, ki jih je v okviru zavez, povezanih s transformacijo, sprejela RS, in celovito oceniti vpliv, ki naj bi ga imelo omrežno delovanje na transformacijo SV v vseh njenih segmentih.

Z vsebino, opisano v nalogi, želim spodbuditi predvsem ključne dejavnike, odgovorne za transformacijo in razvoj zmogljivosti SV v razmišljanje o nujni povezanosti različnih sprejetih ciljev sil pri zagotavljanju ključnih zmogljivosti SV v želeni smeri transformacije SV ter s kritično analizo problemov spodbuditi razvoj v smeri zagotovitve potrebnih virov za učinkovito realizacijo transformacije. Naloga lahko služi kot pomoč pri reševanju težav, s katerimi se soočajo načrtovalci in izvajalci, odgovorni za izvajanje transformacije v SV ter drugih strukturah MORS in državne uprave.

1.3 METODE DELA

V procesu verifikacije hipoteze in doseganja zastavljenih ciljev proučevanja so bile uporabljene naslednje metode raziskovanja:

- metoda sistematičnega zbiranja primarnih in sekundarnih virov, ki obravnavajo temeljno problematiko;
- metoda analize in interpretacije relevantnih pisnih virov, kot osnovna metoda pri oblikovanju naloge;
- metoda primerjalne analize pri primerjavi in ocenjevanju dosežene stopnje implementacije zavez RS za zagotavljanje zmogljivosti omrežnega delovanja;
- metoda raziskovanja z udeležbo.

2. VPLIV ZMOGLJIVOSTI OMREŽNEGA DELOVANJA NA TRANSFORMACIJO SLOVENSKE VOJSKE

Zmogljivosti omrežnega delovanja (Network enabled capabilities) predstavljajo povezavo senzorjev, odločevalcev in oborožitvenih sistemov, mednarodnih vojaških zmogljivosti, zmogljivosti vladnih in nevladnih organizacij ter ostalih sodelujočih na operacijah kriznega odzivanja v mednarodnem okolju na strateški, operativni in taktični ravni v enoten, sodelujoč sistem presojanja, načrtovanja, izvajanja in spremljanja sprejetih odločitev.
Zmogljivost omrežnega delovanja je povezana s sprejemanjem novega načina razmišljanja, je nova filozofija in ne zgolj zmogljivost, ki zahteva drugačen, celovit pristop. S polno implementacijo zmogljivosti omrežnega delovanja se zagotavlja učinkovitejše izvajanje operacij. Ta učinek se dosega z izmenjavo informacij, zagotavljanjem skupne slike bojišča in dvigom zavedanja/spoznanja o situaciji/stanju na bojišču oziroma operaciji kriznega odzivanja. Na ta način dosežemo samosinhronizacijo vseh, ne le bojnih zmogljivosti (enot na bojišču), za doseganje namere poveljnika. Zmogljivosti omrežnega delovanja povečujejo hitrost poveljevanja in zagotavljajo informacijsko prevlado, s tem pa tudi prevlado na bojišču, ki se izraža v obliki povečanega tempa operacij, izboljšanja odzivnosti in zmanjšanja tveganja, zmanjšanja porabe/stroškov in povečanja učinkovitosti na operacijah. Omrežno delovanje se osredotoča na doseganje bojnih in tudi nebojnih učinkov, ki jih dosegamo z medsebojnim povezovanjem različnih zmogljivosti. Tako lahko v okviru zmogljivosti omrežnega delovanja govorimo o implikacijah na vojaški segment in učinke pri izvajanju operacij ter na nevojaški segment, ki sodeluje pri izvajanju operacij.

2.1 OBSTOJEČE STANJE ZMOGLJIVOSTI OMREŽNEGA DELOVANJA V SV

Generalno lahko rečemo, da se SV, praktično že ves čas od njenega nastanka naprej, nahaja v neke vrste transformaciji. K transformaciji sta se RS in SV zavezali že v ključnih strateških dokumentih, ki so nastajali od leta 2001. Težišče v teh dokumentih je bilo namenjeno spremembam, potrebnim prilagajanju zahtevam zavezništva in naporom, povezanim z željo po vključevanju v NATO. Skozi kronološki pregled dokumentov in zavez v dokumentih ter trenutno stopnjo doseženih zmogljivosti lahko spremljamo tudi stopnjo implementacije teh zavez.

2.1.1 Zaveze RS za transformacijo skozi NATO-ve in nacionalne strateške dokumente

Resolucija o strategiji nacionalne varnosti je temeljni dokument za izdelavo področnih strategij oziroma razvojnih in doktrinarnih dokumentov. Viri ogrožanja sicer že upoštevajo asimetrično okolje in vire ogrožanja, ki iz njega izhajajo. Dokument omenja tudi RS kot razvito informacijsko družbo, ki postaja ranljiva tudi na področju informacijske varnosti. Ena ključnih zavez je namenjena vključevanju v NATO, sodelovanju v mirovnih operacijah in prevzemu zavezniških nalog s pomočjo akcijskega načrta za članstvo in partnerstva za mir.

V okviru segmenta Resolucije, ki opredeljuje obrambno politiko, se nanaša tudi zaveza RS, ki bo usmerjena k ustreznemu prilagajanju strukture SV in usklajevanju tehnoloških rešitev ter vojaške opreme standardom zavezništva, obrambna politika pa bo zagotovila financiranje obrambnih potreb, ki bo po obsegu in strukturi primerljivo s financiranjem v državah članicah zavezništva.

Resolucija je sestavljena iz različnih politik, povezanih z različnimi resorji. Te politike pa v nobeni točki niso medsebojno povezane v smislu doseganja sinergije na državni ravni, ki naj bi jih zagotavljale zmogljivosti omrežnega delovanja. Resolucija je kvaliteten dokument, rezultat tedanjega časa ter prilagojen takratnim ciljem. Ključna v Resoluciji je zaveza, da bo Državni zbor RS po potrebi celovito ocenil uveljavljanje Resolucije ter jo dopolnjeval. Smatram, da je bila dolžnost vseh vladnih resorjev opozoriti na potrebo po spremembah in pripravljati dopolnitve Resolucije, ki bi zajemale tudi zagotavljanje zmogljivosti omrežnega delovanja. Resolucija je bila objavljena leta 2001 in je vsekakor potrebna sprememb. Resolucija kot takšna ni mogla zajemati segmentov omrežnega delovanja, ki so bili izpostavljeni kot del transformacije zavezništva veliko kasneje, zato velja osnovna zamera neažurnosti pri spremljanju sprememb v zavezništvu, neustreznemu prilagajanju nacionalnih strateških dokumentov ter v skladu s tem načrtovanja in izvajanja skupne strategije RS pri realizaciji aktivnosti za doseganje zmogljivosti omrežnega delovanja. Prepričan sem tudi, da tisti, ki sprejemajo tovrstne dokumente, niso ustrezno seznanjeni z zahtevami in iz njih izhajajočimi potrebami po zagotavljanju ustreznih virov za zagotavljanje zmogljivosti omrežnega delovanja. Tako ostaja mnogo zavez le mrtva črka na papirju, ali pa se sprejete zaveze oddaljujejo v nedoločeno prihodnost.

Splošni dolgoročni progam razvoja in opremljanja Slovenske vojske opredeljuje Strateški koncept NATA kot dodatno vodilo za preoblikovanje in priprave Slovenske

vojske za članstvo v zvezi NATO in za izvajanje kolektivne obrambe ter sodelovanje z zavezniki in partnerji. Omenjeno je, da se mora obrambni sistem Republike Slovenije prilagajati spremembam v strateškem okolju in pri tem upoštevati zmogljivosti ter razpoložljive vire. Preoblikovanje obrambnega sistema mora biti v skladu s SDPRO usmerjeno v zagotavljanje sil in zmogljivosti za izvajanje lastne ter kolektivne obrambe in aktivno sodelovanje v operacijah v podporo miru.

Vsebino dokumenta, v okviru katerega se nahajajo tudi načrti ter strategija za preoblikovanje SV, ki zajemajo segment posodobitve sistema nadzora in upravljanja s komunikacijsko-informacijskim sistemom, je potrebno gledati iz konteksta stanja, ko je SDPRO tudi nastal, težišče sprememb pa je bilo namenjeno spremembam strukture in obsega SV ter kadrovskemu preoblikovanju. Posebej je bila večkrat poudarjena potreba po usklajenosti načrtov z viri, ki so nam za preoblikovanje na voljo. Ob analizi vsebine in zavez iz SDPRO in ReDPROSV, ki je nastal kot posledica sprememb v letu 2004, ter v primerjavi s trenutnim stanjem lahko ugotovimo, da dejansko stanje v letu 2008 odstopa od načrtovanega stanja v omenjenem dokumentu. Tudi ReDPROSV namreč še ni bil posodobljen v skladu z zavezami, izhajajočimi iz kasneje nastalih dokumentov, ki opredeljujejo obveznosti za izvedbo transformacije, je pa opredelil kot razvojno prednost tehnično in kadrovsko zagotovitev delovanja komunikacijskih in informacijskih sistemov obrambnega sistema ter povezav znotraj zavezništva.

Republika Slovenija je v procesu približevanja in vključevanja v zvezo NATO z akcijskim načrtom za članstvo v NATO in v procesu planiranja sprejela 52 partnerskih ciljev. Ti cilji so določali osnovne usmeritve, naloge in aktivnosti, ki jih mora država kandidatka uresničiti do vključno leta 2006. Poleg dokončanja oblikovanja zmogljivosti za posredovanje so bili prednostni cilji namenjeni tudi nadgrajevanju sistema poveljevanja in kontrole, logistike in zračne obrambe. Že začete projekte na teh področjih je bilo potrebno nadaljevati in zaključiti.

Program nadgrajevanja sistema poveljevanja ter kontrole je obsegal vzpostavitev povezljivosti s sistemi zveze NATO na področju medsebojnega posredovanja sporočil, vzpostavitvi sistema frekvenčnega upravljanja in harmonizacijo z NATO-m, dopolnjevanju informacijske podpore poveljstvom in povezav z NATO-m ter zagotovitve avtomatizirane obdelave in logističnega poročanja med najvišjimi nacionalnimi logističnimi poveljstvi ter podrejenimi enotami. Uvesti je bilo potrebno tudi taktični telekomunikacijski sistem Slovenske vojske. Zaveze iz partnerskih ciljev so že vsebovale segmente prve faze (odprave neskladij) med sistemi poveljevanja in kontrole NATA ter nacionalnih sistemov.

Edini nacionalni dokument, ki se je v vmesnem obdobju dopolnjeval, je Srednjeročni obrambni program (SOPR). **SOPR 2007–2012** je zadnji potrjeni srednjeročni program razvoja SV. Po svoji vsebini je sicer razvojno naravnan, ne sledi pa filozofiji razvoja zmogljivosti omrežnega delovanja, saj ne deluje kot celota, usmerjena v razvoj zmogljivosti SV, ki bi bile sposobne udejaniti informacijsko prevlado, ki jo omogočajo zmogljivosti omrežnega delovanja in bi bile, kot je opredeljeno v zavezah, sposobne delovati v skladu s koncepti, po katerih naj bi delovale bodoče sile zavezništva. Zmogljivosti omrežnega delovanja so omenjene le v poglavju 7 (izgradnja zmogljivosti, podpoglavje glavna oprema - elektronska in komunikacijska oprema), pri čemer je zapisano, da bo SV razvijala in zagotovila prehod na omrežno delovanje ter zagotavljanje NNEC zmogljivosti informacijskega sistema poveljevanja in kontrole (IS PINK).

Kot del procesa planiranja zmogljivosti se skozi proces DRR (Defence requirement revue) ugotavlja, katere zmogljivosti potrebuje zavezništvo, članice pa se v procesu sprejemanja ciljev sil obvežejo, da bodo cilje sil, ki jih sprejmejo, s tem pa tudi zmogljivosti, ki iz njih izhajajo, tudi implementirale.

Na vrhu v Pragi, novembra 2002, še pod vplivom dogodkov 11. septembra 2001, je dozorela odločitev za transformacijo zavezniških sil, ki bo omogočala izvajanje vseh vrst operacij v kateremkoli okolju. Tako so sprejeli zavezo za formiranje NATO-vih odzivnih sil NRF (angl. NATO Response Force), ki bodo predstavljale tehnološko napredne, fleksibilne, premestljive, interoperabilne in vzdržljive sile, sestavljene iz elementov vseh zvrsti, ki se bodo sposobne v najkrajšem možnem času premestiti kamorkoli. Zavezali so se tudi za spremembe poveljniške strukture v smislu zmanjševanja, večje odzivnosti in premestljivosti poveljstev ter poveljniških mest, večji poudarek pa nameniti tudi zmogljivostim NRKB obrambe, področju obveščevalnih zadev, sistemov za hitro zaznavanje ciljev, nadzornih sistemov, sistemov poveljevanja in kontrole, zmogljivosti strateškega transporta in »air to air refuelling« s ciljem zagotavljanja večje učinkovitosti enot. Na podlagi tega je bil januarja 2003 izdelan koncept NATO-vih odzivnih sil (Military concept for the NATO Response Force - NRF).

Kot odgovor na sprejete smernice Vrha v Pragi (angl. Prague Summit) v povezavi z zmogljivostmi NNEC, ki podpirajo koncept NRF [1]in EBO, so poveljniki strateških poveljstev NATA razvili nabor transformacijskih ciljev in ciljnih področij transformacije

[1] MC 477 – Military Concept for the NATO Response Force, v katerem je opredeljeno, da koncept predstavlja temeljni kamen transformacije zavezniških sil.

(slika 1), ki bi podpirali razvoj zmogljivosti bodočih sil zavezništva. Na ta način bi bile sile sposobne izvajati bodoče naloge zavezništva v skladu z ustreznimi koncepti.

Junija 2005 je bila, kot plod sodelovanja 12 članic NATA ob podpori in usmeritvah NC3B, izdelana študija izvedljivosti NNEC, v kateri opredeljuje operativne potrebe in zahteve s predvideno strategijo in dinamiko izvajanja sprememb, povezanih z zagotavljanjem omrežne in informacijske infrastrukture v podporo transformacije zavezništva ter v podporo razvoja NATO-vega koncepta omrežnega delovanja.

Na Vrhu v Rigi, novembra 2006, so predsedniki držav in vlad med drugimi v skupni deklaraciji ter političnih usmeritvah podprli tudi napore NC3O (NATO C3 organisation) za razvoj NATO-vih zmogljivosti omrežnega delovanja (NNEC - NATO Network Enabled Capability), ki bi zagotavljale izmenjavo informacij, zanesljivost in varnost obveščevalnih informacij ter zaščito pred kibernetskimi napadi na informacijske sisteme ter s tem dosego informacijske prevlade.

Severnoatlantski svet NAC (North Atlantic Council) je februarja 2007 določil NATO-v odbor za posvetovanje, poveljevanje in nadzor (NC3B) kot odbor, ki bo izvajal vodstveno vlogo v upravljanju in doseganju zmogljivosti NNEC v NATU. NC3B se je tako v novembru leta 2007 prvič sestal v formatu upravljanja NNEC (angl. NNEC Governance Session) skupaj z ostalimi pomembnimi odbori NATA, kjer je potrdil dokument na visoki ravni o upravljanju NNEC za predložitev NAC-u. NAC je v januarju leta 2008 potrdil omenjeni dokument, s katerim so opredeljene vloge in odgovornosti ključnih vplivnikov (Stakeholders) v NATU in tudi držav članic pri upravljanju NNEC. Ob tem je pozval ključne vplivnike k poglobljenemu delu in zadolžil NC3B za zagotovitev usklajenosti NATO-vih in Nacionalnih aktivnosti na področju uvajanja zmogljivosti omrežnega delovanja. Posebej je izpostavil pomembnost tega področja in pozval države članice k večji angažiranosti pri zagotavljanju teh zmogljivosti, kakor tudi v delu s tem povezanih NATO-vih odborov. Države članice morajo zagotoviti skladnost Nacionalnih procesov in izdelkov z razvojem NATO-vih zmogljivosti omrežnega delovanja in omogočiti izmenjavo informacij z drugimi o lastnih konceptih, izdelkih ter izkušnjah.

NC3B je potrdil predlog dveh letnih sestankov NC3B v formatu upravljanje NNEC v ojačani sestavi (zraven najvišjega nacionalnega predstavnika za C3, še pristojna oseba za upravljanje zmogljivosti omrežnega delovanja v posamezni članici, ki je načeloma in v večini primerov na višji ravni) ter po potrebi več sestankov na nižji ravni.

Na obrambnem Vrhu v Bukarešti so se predsedniki držav, vlad in obrambni ministri seznanili z napredkom pri transformaciji, vključno z razvojem NATO-vih zmogljivosti omrežnega delovanja.

Pričakovali bi, da bodo zaveze iz Vrha v Pragi, Rigi in Bukarešti na ustrezen način, povezan z nacionalnimi interesi in zmožnostmi, prevedene v nacionalne strateške dokumente.

Edina zaveza, ki poskuša slediti zgoraj navedenim zavezam, je SOPR, ki vsebuje tudi sprejete cilje sil. Zadnji sprejeti **cilji sil** se nanašajo na leto 2008. Spremembe, ki se nanašajo na stare cilje sil in zahtevane zmogljivosti, sprejete v letu 2008, se bistveno razlikujejo le po tem, da so stari cilji sil koncentrirani pod skupnim imenom posameznih zmogljivosti, ki podpirajo transformacijo NEC. Iz štirinajstih ciljev sil, ki so zagotavljali zmogljivosti s področja komunikacijskih in informacijskih sistemov, je število ciljev zmanjšano na pet ciljev sil, ki so neposredno vezani na zmogljivosti omrežnega delovanja s težiščem na zagotavljanu zmogljivosti omrežnega delovanja za potrebe premestljivih sil in izgradnji omrežne ter informacijske infrastrukture. V njih so vsebinsko koncentrirani vsi stari cilji, dodano pa je še nekaj novih vsebin.

Zavedati se moramo, da so vsi predlogi ciljev sil usmerjeni v zagotavljanje zmogljivosti bodočih premestljivih zavezniških oz. koalicijskih sil, ki bodo s pravočasno in časovno usklajeno implementacijo ciljev, za katere se je posamezna članica zavezala, nacionalnim silam zagotovile povezljivost/interoperabilnost z ostalimi članicami. Cilji sil niso usmerjeni le na področje transformacije omrežne in informacijske infrastrukture, pač pa na vsa področja, opredeljena na sliki 1. Del ciljev sil, ki sodi na področje „omogočanja“ (Enabling), se nanaša na zagotavljanje zmogljivosti omrežnega delovanja oziroma na omrežno in informacijsko infrastrukturo. Ti cilji sil pa se nanašajo praktično na vse ostale zmogljivosti in vplivajo na vsa ostala področja transformacije. Zato je zelo kratkoviden tisti pogled na transformacijo, ki vidi zmogljivosti omrežnega delovanja le v okvirih sprememb komunikacijske in informacijske infrastrukture ter nalog segmentov ministrstva in SV, ki se ukvarjajo z informatiko ter komunikacijami, ne pa kot celoto sprememb, povezanih s potrebno transformacijo SV kot celote. Vsebina ciljev sil, ki se nanaša neposredno na zmogljivosti omrežnega delovanja za potrebe SV, se nahaja v posebnem poglavju. Eden ključnih ciljev sil, ki jih je sprejela RS, zahteva zmogljivosti omrežnega delovanja za vse zmogljivosti SV, glede na njihovo vlogo v bojevanju, in sicer za sile za bojevanje, sile za bojno podporo, sile za zagotovitev delovanja in sile za podporo

poveljevanja, kar je nedvoumno zapisano v zahtevah za izvedbo (realizacijo) (Adoption of the NNEC enhancement as described in the NNEC FPs) cilja sil L 0035.

2.1.2 Trenutna stopnja doseženih zmogljivosti omrežnega delovanja v SV

Ko ocenjujemo trenutno stopnjo doseženih zmogljivosti omrežnega delovanja, moramo to ocenjevati skozi operativne zahteve, izražene na posameznih področjih, predvsem na področjih inženirske podpore, zračne obrambe, komunikacijskih in informacijskih sistemov, (Intelligence, Surveillance, Target Acquisition, Reconnaissance – ISTAR), NRKB, logistične zagotovitve, zdravstvene zagotovitve, civilno-vojaškega sodelovanja, bojne učinkovitosti oborožitvenih sistemov in avtomatizacije procesa poveljevanja ter kontrole z ene strani in implementacije ciljev sil, sprejetih leta 2006 in 2008, ki so usmerjeni v zagotavljanje zmogljivosti omrežnega delovanja na drugi strani. Ob tem moramo upoštevati tudi izraženo raven ambicij glede sodelovanja SV na operacijah. Generične zmogljivosti teh enot se namreč morajo razvijati v smeri zmogljivosti, izraženih v sodobnih konceptih, kot so NRF in koncept operacij, ki temeljijo na učinkih.

V smislu zagotavljanja zmogljivosti omrežnega delovanja je bilo sprejetih kar nekaj ciljev in začetih projektov modernizacije SV, z uvedbo katerih se bodo zagotovile zmogljivosti omrežnega delovanja ter zmožnost delovanja SV v okviru zavezništva. Informacijska prevlada se bo z uvedbo zmogljivosti omrežnega delovanja izražala v povečanju bojne moči, v večji dinamiki bojnih delovanj, izboljšanju možnosti za preživetje, povečanju natančnosti oborožitvenih sistemov, skrajšanju trajanja nalog in zmanjšanju potrebnih sil za realizacijo nalog.

Obdobje je zaznamovalo intenzivno opremljanje enot in poveljstev SV s komunikacijskimi in informacijskimi sistemi, saj nas k temu med drugim sili hiter razvoj tehnologije na tem področju. Večina ključnih projektov, ki so navedeni v nadaljevanju, je bila vezanih na realizacijo ciljev sil. Le-teh je bilo na področju zmogljivosti omrežnega delovanja skupaj 11.

Uvajali smo programske rešitve za podporo zavedanja situacije skladno z NATO in MIP standardi. Bistveno so izboljšane omrežne storitve, ki so dosegljive do ravni bataljona. Povečane so bile prenosne zmogljivosti in vključene redundantne poti. Izboljšana je funkcionalna podpora enot in poveljstev z uporabo programskih rešitev, zasnovanih na strukturiranih bazah podatkov.

Ključni projekti in zmogljivosti omrežnega delovanja se zagotavljajo skozi naslednje projekte, ki so povezani z zmogljivostmi, zahtevanimi v sprejetimi cilji sil. Le-ti so:

- projekti na področju komunikacijskih sistemov in storitev se nanašajo predvsem na modernizacijo taktičnega telekomunikacijskega sistema (TTKS) in radijskih sistemov kot mobilnih telekomunikacijskih sistemov SV, zagotavljanje zmogljivosti satelitskih komunikacij za povezavo z zavezniškimi enotami in povezavo enot na operacijah z domovino (SATCOM) ter zagotavljanju zmogljivosti video telekonference (VTC);
- projekti na področju informacijskih sistemov in storitev se nanašajo predvsem na informacijski sistem poveljevanja ter kontrole (IS PINK), ki zagotavlja strojno in programsko opremo za zagotavljanje enotne slike bojišča na vseh ravneh poveljevanja v stacionarnem in mobilnem okolju z integriranim geografskim informacijskim sistemom in analitičnimi orodji za analizo terena, z možnostjo istočasne izdelave skupnega povelja, operativnim pregledom kadrov in materialnih sredstev ter izmenjavo podatkov preko replikacijskih mehanizmov, projekt opremljanja poveljniškega centra SV (POVC), projekt zagotavljanja zmogljivosti vojaškega sporočilnega sistema MMHS (angl. Military message handling system) in projekt informacijskega sistema logistike (ISLOG);
- projekti na področju informacijske varnosti se nanašajo predvsem na zagotavljanje IP kriptografskih sistemov in infrastrukture javnih ključev (PKI).

V zadnjem obdobju je bilo izdelano nekaj konceptualnih[2] in izvedbenih dokumentov. Organizacija in popolnjevanje enot za zveze in informatiko, prav tako pa tudi spremembe v organizacijsko-formacijski strukturi enot ni sledila opremljanju. V tem obdobju smo lahko priča velikemu odtoku strokovnega kadra, kar predstavlja enega od glavnih razlogov, da transformacija v želenih okvirih ne uspe. Prav tako proces nabave od izdelave investicijske dokumentacije naprej še ni dovolj usklajen s stopnjo razvoja in implementacije komunikacijskih ter informacijskih sistemov. Integracija senzorskih in komunikacijskih ter informacijskih sistemov še ni na ustrezni ravni. Izogniti se moramo možnosti, da postanejo komunikacijski in informacijski sistemi tehnološki otok ter sami sebi v namen.

[2] Koncept uporabe in razvoja zmogljivosti C4I v MOTB in BBSK.
Koncept delovanja informacijskega sistema poveljevanja in kontrole (IS PINK).

2.2 CILJI IN PODROČJA TRANSFORMACIJE Z VIDIKA OMREŽNEGA DELOVANJA

Zmogljivosti omrežnega delovanja se gradijo na podlagi naslednjih načel. Le-ta so:

1) zmogljivosti omrežnega delovanja niso le omogočevalec (Enabler), ampak predstavljajo pogoj za transformacijo zavezništva in so bistvene za dosego učinkovitega izvajanja operacij po novih konceptih (NRF, Effects Based Operations);
2) zmogljivosti omrežnega delovanja obsegajo proces posvetovanja in odločanja od najvišje – politične do najnižje – taktične ravni. Zato je nujna sprememba miselnosti in dosežena politična volja ter zaveza, ki bo zagotavljala izmenjavo informacij (information sharing) in ne njihovega skrivanja. Razvoj tehnoloških rešitev namreč omogoča vse;
3) NNEC Natu in članicam omogoča dosego ciljev z manjšimi silami ob uporabi moderne tehnologije. Obenem to predstavlja poslovne priložnosti na drugih obrambnih področjih;
4) zmogljivosti omrežnega delovanja vsaki posamezni državi omogočajo določitev njene lastne ravni zavez, z maksimalno uporabo obstoječih sistemov, ne pa s splošno zamenjavo le-teh;
5) prvi korak v smeri uvajanja zmogljivosti omrežnega delovanja je usmerjen v podporo konceptu NATO-vih odzivnih sil (NRF);
6) implementacija zmogljivosti omrežnega delovanja zahteva tesno sodelovanje vlad in industrij posameznih članic.

Najbolj jasen odgovor v zvezi s pomembnostjo doseganja zmogljivosti omrežnega delovanja za uspešno izvedbo transformacije je verjetno zapisan v knjižici nizozemskega obrambnega ministrstva o razvoju zmogljivosti omrežnega delovanja na Nizozemskem z naslednjimi besedami: »If you can't plug in, you can't play«[3].

Znano dejstvo v zvezi z zmogljivostmi mrežnega delovanja je, da bo NATO zagotovil največ 10 % zmogljivosti, ostalih 90 % pa je v nacionalni pristojnosti in odgovornosti. Posamezne članice, posebej Nizozemska in ostalih 11 članic, ki so financirale študijo izvedljivosti za zagotavljanje zmogljivosti omrežnega delovanja, so na tem področju zelo dejavne. Da se z zmogljivostmi omrežnega vojskovanja ne ukvarjajo le članice zavezništva

[3] Networked operations, The Netherlands Defence organisations steps into the future with Network Enabled Capabilities, NEC steering group of the Netherlands Ministry of Defence in Cooperation with TNO Defence, Security and Safety, Netherlands Ministry of Defence, October 2006.

NATO je, kot je zapisal dr. Uroš Svete, tudi Avstrija umestila koncept na omrežju temelječih oboroženih silah v svoje varnostno-politično okolje[4]. Ko govorimo o konceptu operacij, ki temeljijo na učinkih, ne moremo mimo dejstva, da pri realizaciji aktivnosti ne sodeluje le vojska in obrambni sektor, pač pa mnogi drugi sektorji. Tega se zavedajo v mnogih članicah zavezništva. Zato so pristopili k skupnim projektom na državni ravni za izgradnjo skupne omrežne in informacijske infrastrukture, ki bi poenotila komunikacijsko ter informacijsko infrastrukturo vseh državnih organov, predvsem pa tistih, ki dajejo največji prispevek k operacijam. S tem se zagotovi večja učinkovitost, preglednejša arhitektura sistema, poenostavi se sistem upravljanja in vzdrževanja, zmanjšajo se stroški in potrebna kadrovska struktura. V enoten sistem so namreč povezane vse državne ustanove od vojske, policije, gasilcev, reševalcev, carinikov in drugih javnih služb po vzoru zmogljivosti omrežnega delovanja, kjer vsak upravlja in nadzira svoj del sistema. Dodati posamezne uporabnike iz drugih struktur, ki, izhajajoč iz konceptov, sodelujejo pri izvajanju operacije, ni nikakršen problem. Proces je seveda zelo zapleten, saj ruši obstoječe vrtičke in pridobljene ugodnosti posameznih struktur različnih državnih organov, ki se na ta račun bohotijo in vzdržujejo obstoječe stanje.

[4] Uroš Svete, Varnost v informacijski družbi (str. 113).

2.2.1 Področja transformacije

Slika 1: Področja transformacije

Vir: NATO Network enabled capability feasibility study, Executive summary, Version 2.0, 2005.

Slika 1 prikazuje področja transformacije, ki so jih opredelili v strateških poveljstvih NATA (Strategic Commands – SC) in so potrebna za razvoj bodočih zmogljivosti zavezništva, ki bodo sposobne izvajati vse naloge ter se odzivati na vse morebitne vire ogrožanja. Eno izmed teh zmogljivosti predstavljajo tudi zmogljivosti omrežnega delovanja (Network Enabled Capabilities - NEC). Z njimi zagotavljamo povezavo med senzorji, odločevalci in oborožitvenimi sistemi, prav tako pa povezujemo mednarodne vojaške zmogljivosti z zmogljivostmi vladnih in nevladnih organizacij ter ostalih akterjev v mednarodnem okolju v enoten, sodelujoč sistem presojanja, načrtovanja, izvajanja in spremljanja sprejetih odločitev. Zmogljivosti omrežnega delovanja tako na pomemben način prispevajo k učinkoviti uporabi enot, izvajanju ekspedicijskih operacij, zagotavljanju integrirane logistike in učinkovitosti izvajanja civilno-vojaškega sodelovanja v okviru CIMIC.

Nadaljnji razvoj zmogljivosti omrežnega delovanja temelji na povezovanju zmogljivosti omrežnega delovanja z NATO-vimi koncepti operacij, predvsem konceptom NATO-vih odzivnih sil in konceptom operacij, ki temeljijo na učinkih. Zmogljivosti omrežnega delovanja bodo v največji meri dosežene le, če bo vzpostavljena jasna povezava in sinhronizacija med koncepti izvajanja operacij zavezništva, vizijo strateških poveljnikov o načinu izvajanja teh operacij ter potrebnimi C4ISR zmogljivostmi, ki bodo podpirale to vizijo.

Inovacije v tehnologiji so neposredno in tesno povezane z dolgoročnimi spremembami pravil izvajanja posameznih aktivnosti. Spremembe v kulturi, pravilih in orodjih (oborožitvenih sistemih …), s pomočjo katerih izvajamo aktivnosti/operacije, določajo način izvajanja teh operacij. Zahtevane operativne zmogljivosti bodočih sil NATA in SV morajo izhajati iz koncepta izvajanja operacij, iz tega pa spremembe, ki morajo biti izvedene na različnih področjih. Ta področja zajemajo vse segmente, predvsem pa spremembe v doktrinarnem segmentu, organizaciji in kadrih, izobraževanju ter usposabljanju, vodenju in poveljevanju ter sistemu nabav za zagotavljanje zmogljivosti omrežnega delovanja.

2.2.2 Operativne zahteve transformacije

Proces identifikacije dejanskih zahtev po zmogljivostih NNEC je bil izveden skozi proces DRR (Defence Requirement Review) planskih situacij in z uvajanjem novih konceptov operativne uporabe, pri čemer posameznih konceptov NATO v vojaški odbor še ni potrdil. Operativne zahteve[5] so opredeljene v okviru različnih področij transformacije (Slika 1) na podlagi virov ogrožanja in spremenjenih konceptov. Ocena potrebnih zmogljivosti omrežnega delovanja zajema operativne zahteve na področjih učinkovite uporabe enot in oborožitvenih sistemov, integrirane logistike, zagotavljanja izvajanja ekspedicijskih operacij ter nadgrajevanja zmogljivosti CIMIC.

Operativne zahteve na področju **učinkovite uporabe enot** in oborožitvenih sistemov se nanašajo predvsem na povezave na relaciji senzor – strelec/oborožitveni sistem – odločevalec s poudarkom na časovno občutljivih ciljih (TST – Time Sensitive Targeting). Zahteva hitro, prilagodljivo in natančno uporabo sistemov s poudarkom na zmanjšanju časovnega odzivanja povezanega z detekcijo ter uporabo oborožitvenega sistema.

[5] Bartolomasi P., NATO Network enabled capability, Feasibility study, (2005) Volume I, Overwiev of NATO Network Centric Operational Needs and Implications for the Development of Net-Centric Solutions, Version 2.0.

Zmogljivost TST predstavlja enega največjih tehnoloških izzivov v okviru zmogljivosti omrežnega delovanja in je predstavljena v okviru koncepta Joint Precision Engagement.

Operativne zahteve v zvezi z **integrirano logistično podporo** so povezane z zahtevami po logistični podpori NATO-vih enot na operaciji. Med najzahtevnejše sodi oskrba enot od APOD ali SPOD do lokacije razmestitve NATO-vih odzivnih sil (NRF), ki zahteva premike na relacijah, tudi daljših od 1000 km, pri čemer so sile mednarodne sestave. Trenutno se v zvezi s tem vprašanjem srečujemo s težavami, povezanimi s podvajanjem in presežki/pomanjkanjem posameznih storitev, predvsem zaradi ločenih nacionalnih logističnih kanalov podpore. Osnovne operativne zahteve se nanašajo na nadgradnjo sledenja lokacije pošiljk, izboljšanja pregleda nad stanjem sredstev, potrošnega materiala, sredstev za vzdrževanje in rezervnih delov na operacijah (NATO-vih poveljnikov kakor tudi poveljnikov nacionalnih kontingentov), zagotavljanju boljšega pregleda nad statusom reševanja zahtev, izboljšanja sistema planiranja v mednarodnem okolju in strateškega transporta.

Operativne zahteve v okviru nadgrajevanja **zmogljivosti CIMIC** se nanašajo na zmogljivosti, potrebne poveljniku operativnih sil pri nadgrajevanju medsebojnih razmerij z lokalnim prebivalstvom in lokalnimi oblastmi. Nadgrajevanje zmogljivosti omogoča zagotavljanje stabilnejšega okolja za izvajanje operacije. V tem smislu se od zmogljivosti omrežnega delovanja zahteva povezljivost z vojaškimi silami na operacijah, hkrati pa tudi povezljivost z lokalnimi oblastmi, vladnimi in nevladnimi organizacijami ter drugimi akterji na območju operacije, ki prispevajo k stabilizaciji razmer, dvigu kvalitete in varnosti izmenjave informacij ter izboljšanju koordinacije in usklajenosti aktivnosti CIMIC. Te zmogljivosti se zahtevajo v različnih vrstah in fazah operacij ter na različnih ravneh PINK. Posebna pozornost je namenjena aktivnostim, povezanimi s kritično/ključno infrastrukturo, humanitarnim aktivnostim, aktivnostim, povezanimi z reševanjem statusa beguncev itd.

Operativne zahteve v okviru zagotavljanja izvajanja **ekspedicijskih operacij** so vezana na različna funkcijska področja, nanašajo pa se predvsem na omejene zmogljivosti premeščanja in delovanja poveljniških struktur v rajon izvajanja operacije ter omogočanja t.i. »reach back« povezav oz. dostopa do podatkov/storitev v domovini in s tem zmanjševanja potrebnih sil za realizacijo nalog (in-theatre footprint) oz. potreb po izvajanju posameznih aktivnosti/storitev na sami lokaciji operacije. To je področje, kjer so odkrite ključne pomanjkljivosti pri zagotavljanju robustne komunikacijske in informacijske

infrastrukture za potrebe uspešnega delovanja poveljstev, je eden ključnih segmentov zagotavljanja zmogljivosti omrežnega delovanja.

2.3 KLJUČNA PODROČJA TRANSFORMACIJE SV Z VIDIKA ZMOGLJIVOSTI OMREŽNEGA DELOVANJA

2.3.1 Vpliv mrežnega delovanja na spremembe zmogljivosti sistemov C4ISR

Omrežna in informacijska infrastruktura (NII – networking and information infrastructure) je ključen segment, ki zagotavlja povezljivost vseh dejavnikov na bojišču v enoten sistem, ki omogoča boljši pregled nad situacijo na bojišču ter v končni fazi prevlado na bojišču. Povečano število senzorjev, oborožitvenih sistemov in avtomatizacija sistemov odločanja zahteva izboljšano omrežno ter informacijsko infrastrukturo. Dosedanji sistemi in način njihovega delovanja ter uporabe, ki postajajo ozko grlo, se bodo morali umakniti novi tehnologiji in konceptom, ki omogočajo ustrezno raven izmenjave informacij in njihovo varnost med vsemi dejavniki na bojišču. Povečano število dejavnikov povečuje tudi kompleksnost te infrastrukture. Vedno večje so zahteve za zagotovitvijo ustrezne pasovne širine komunikacijskih poti, podatkovnih baz, zgrajenih na skupnih standardih ter varnosti prenosa, hranjenja in obdelave podatkov. Povečana kompleksnost zahteva optimizacijo omrežne infrastrukture, predvsem na taktični ravni.

Cilj Ministrstva za obrambo in Slovenske vojske je vzpostaviti varno in prilagodljivo komunikacijsko ter informacijsko omrežno infrastrukturo skladno z zahtevami zmogljivosti omrežnega delovanja, izraženimi v ciljih sil ter sistem poveljevanja in kontrole, ki bo zajemal različna funkcijska področja.

Osnovni namen omrežne in informacijske infrastrukture NII (angl. Networking and Information Infrastructure) je zagotoviti robustno, razvijajočo se komunikacijsko-informacijsko infrastrukturo med članicami zveze NATO, ki zagotavlja možnost medsebojnega povezovanja znotraj zavezništva, kakor tudi med partnerskimi državami in drugimi vladnimi ter nevladnimi organizacijami. Zahteva v zvezi z razvojem komunikacijske in informacijske infrastrukture je, da ima vsaka članica svoje avtonomno omrežje, ki ga sama upravlja in nadzira. Na skupnih akcijah zavezništva se ta omrežja povežejo med seboj tako, da tvorijo enotno omrežje, ki nima centralnega sistema nadzora in upravljanja, kljub temu pa omogoča neovirano komunikacijo med sodelujočimi na operacijah. Infrastruktura NII mora zagotavljati dinamično prilagajanje potrebam

delovanja v hitro spreminjajočem se okolju. NII se bo razvijala postopoma in po fazah, zajemala pa bo specifična področja in zmogljivosti, ki so navedena v nadaljevanju.
NII sestavljajo osnovna področja, ki so izražena v ciljih sil, in sicer:

- komunikacijsko področje;
- informacijsko področje;
- področje informacijske varnosti.

Na komunikacijskem področju bo vpliv izražen predvsem v tendenci prehoda na IP omrežja, razvoju programsko definiranih radijskih sistemov[6] in razvoju komunikacijskih sistemov v smeri povečanja pasovnih širin taktičnih komunikacijskih sistemov. Trenutno največje težave na komunikacijskem področju predstavljajo povezljivost komunikacijskih sistemov in ob vse večji informatizaciji pasovna širina komunikacijskih sistemov[7] na taktični ravni. Iz tega izhajajo zahteve v cilju sil, ki opredeljujejo potrebne zmogljivosti komunikacijskih sistemov. Tako se v okviru cilja sil »Network enabled communications« zahteva vzpostavitev omrežne infrastrukture, ki bo skladna z zahtevami zmogljivosti omrežnega delovanja. Namesto prenosa podatkov po različnih omrežjih naj bi uporabniki uporabljali eno navidezno omrežje, pri čemer ne bi bili odvisni od prenosnih medijev. Z vojaškega zornega kota gledano bo zagotavljanje t.i. virtualnega omrežja zmanjšalo potrebo po postavitvi različnih vrst komunikacijske infrastrukture na lokacijah, na katerih se izvajajo operacije za potrebe premestljivih sil, saj naj bi le eno virtualno omrežje zagotavljalo prenos različnih vrst signalov. Z ekonomskega vidika bi morala biti aktivnost kot taka cenejša, hkrati pa bo takšno enotno omrežje v taktičnem okolju omogočalo upravljanje s frekvenčnim spektrom in potrebnimi pasovnimi širinami v taktičnem okolju, glede na prioriteto informacij. S ciljem vzpostavitve **naprednih omrežij (Advanced Networking)** se bo za potrebe SV v nacionalnem stacionarnem in taktičnem omrežju TTKS (angl. Deployable Forces Network) vpeljal sistem zagotavljanja kakovosti storitev QoS (angl. Quality of Service). Tovrstna storitev bo zagotavljala najpomembnejšim storitvam prioriteto pri dodeljevanju razpoložljive pasovne širine. Ključne aktivnosti bodo usmerjene na prehod vseh storitev na IP protokol ter na postopen prehod na uporabo IP v 6 protokola.

[6] SDR (Software Defined Radio) – Programsko definirani radijski sistemi.

[7] Uroš Svete, Varnost v informacijski družbi (str. 233–235), kjer so tabelarično prikazane naraščajoče potrebe po pasovnih širinah v oboroženih silah ZDA pri uporabi IKT v ameriško-iraškem konfliktu 2003–2004, ne le na strateški, pač pa tudi na taktični ravni. Na problem pri implementaciji taktičnega interneta pa opozarja tudi več drugih avtorjev in študij.

Ena ključnih zahtev v zvezi z zagotavljanjem različnih zmogljivosti bo tudi zagotovitev vsem NATO-vim deklariranim silam v času njihove uporabe govorno in podatkovno povezavo z nacionalnim obrambnim omrežjem, z NATO-vim komunikacijskim sistemom NGCS (angl. NATO Global Communications system) in z ostalimi taktičnimi omrežji na območju izvajanja operacije. V smislu zagotavljanja večje pasovne širine v taktičnem okolju bo razvoj in nabava usmerjena v zagotovitev širokopasovnih naprednih bojnih radijskih naprav **ACNR** (angl. **Advanced combat network radio**) s kriptografsko zaščito, odpornih na namerno frekvenčno motenje. Razvoj radijskih naprav bo usmerjen v zagotavljanje programsko definiranih radijskih sistemov **SDR (**angl. **Software defined radio)**, ki bodo omogočali vzpostavitev mobilnih omrežij **MANET** (angl. **Mobile Ad-Hoc Networks**) oziroma različico teh omrežij **VANET** (angl. **Vehicular Ad-Hoc Networks**) predvsem v taktičnem okolju, kjer bo prihajalo do hitrih sprememb v taktični situaciji in je onemogočeno postavljanje drugačne komunikacijske infrastrukture.
Za zagotavljanje zmogljivosti komuniciranja na velikih razdaljah **(**angl. **Long Range Communications)** bodo zmogljivosti omrežnega delovanja vplivale na razvoj HF radijskih in satelitskih (SATCOM) sistemov, kar bo povečalo učinkovitost izvajanja ekspedicijskih operacij in zmanjšalo potrebno infrastrukturo ter sile na območju izvajanja operacij.

Na področju zmogljivosti informacijskih sistemov bo vpliv izražen v smeri razvoja in uporabe XML (angl. Extensible Markup Language) kompatibilnih aplikacij/rešitev ter razvoja in integracije sistemov kot servisno orientirane arhitekture SOA (angl. Service Oriented Architecture), kjer je SOA opisana kot IT infrastruktura, ki omogoča različnim aplikacijam izmenjavo podatkov v določenem poslovnem procesu. Informacijski sistemi se bodo razvijali tudi v smeri optimizacije rešitev za delo v taktičnem okolju. Iz tega izhajajo zahteve v okviru cilja sil »Network Enabled Information Systems«, ki so usmerjene predvsem v zagotavljanje zmogljivosti informacijskih sistemov za potrebe premestljivih sil, le-te pa so opredeljene na podlagi identifikacije zahtev poveljevanja in kontrole, predvsem na taktični ravni. Storitve informacijskih sistemov so bile namreč že sedaj na voljo strateškim in operativnim poveljstvom, enote na taktični ravni pa so ostale informacijsko nepovezane. Eden od razlogov zato je tendenca prehoda na uporabo komercialnih COTS (angl. Commercial of the shelf) izdelkov v vojaške namene. Le-ti niso bili ustvarjeni za težke pogoje dela v taktičnem okolju, saj so bile komercialne rešitve precej požrešne glede komunikacijskih virov.

Tako bo potrebno v prvi fazi transformacije povezati nacionalni stacionarni in taktični sistem poveljevanja ter kontrole z NATO-vim sistemom, s čemer bo zagotovljen enoten sistem planiranja in izvajanja operacij na kopnem, morju ter v zraku. Sistem se bo uvajal postopoma po ravneh poveljevanja, najprej v stacionarnem okolju na ravni združenih poveljstev JFC (Joint Force Command), nato pa še v mobilnem do najnižjih taktičnih ravni. Osnovo za izmenjavo podatkov bo predstavljal podatkovni model JC3IEDM (angl. Joint C3 Information exchange Data Model), skladen z MIP (angl. Multilateral Interoperability programme) standardom.
Zahteva se torej ne le povezljivost aplikacij, temveč se zahteva povezljivost na ravni podatkovnih baz. V prehodnem obdobju bo zahtevana povezljivost nacionalnih kopenskih, pomorskih in zračnih sistemov poveljevanja ter kontrole s tovrstnimi NATO-vimi sistemi in njihovimi aplikativnimi rešitvami. Prav tako bo potrebno zagotoviti povezljivost logističnega in obveščevalnega sistema poveljevanja ter kontrole z NATO-vimi sistemi. V okvir modula za spremljanje situacije na bojišču (angl. Situational Awareness) bo potrebno vgraditi zmogljivosti za spremljanje lastnih sil FFT (Friendly Force Tracking) do najnižjih taktičnih ravni in posameznih letalskih platform, ki zagotavljajo vhodne informacije za skupno operativno sliko COP (angl. Common Operational Picture). Težiščno se bodo zagotavljale zmogljivosti za tiste enote SV, ki bodo namenjene popolnjevanju enot NRF. Zmogljivosti bodo nadgrajene do ravni spremljanja sredstev (angl. Asset Tracking), predvsem v času transporta do APOD in SPOD. Napori bodo usmerjeni tudi v zagotavljanje zmogljivosti nacionalnega vojaškega sporočilnega sistema, ki bo kompatibilen z NATO-vim sporočilnim sistemom in integriran v sistem C2.

Na področju informacijske varnosti se bodo zmogljivosti razvijale v smeri varne izmenjave informacij (angl. secure information sharing) in ne v ekskluzivni smeri varovanja informacij, saj je tendenca zmogljivosti omrežnega delovanja upoštevanje koncepta operacij, ki temeljijo na učinkih, kjer sodelujejo ne le vojaške sile zavezništva, temveč tudi vladne in nevladne organizacije ter lokalne oblasti in prebivalstvo, s katerim je potrebno izmenjati informacije. Tako bo morala RS v okviru zahtev, ki izhajajo iz cilja sil »Cyber defence and information assurance in the NNEC framework« zagotoviti fleksibilno in varno informacijsko omrežno infrastrukturo (angl. Information Assurance Framework), kjer je težišče usmerjeno v razvoj in zagotavljanje zmogljivosti t.i. protokola SCIP (angl. Secure Communications Interoperability Protocol), ki bo zagotavljal varnost ne glede na

vrsto komunikacijskih sredstev in pasovno širino komunikacijskega kanala, kar je posebej pomembno v taktičnih komunikacijskih omrežjih.
Vpliv na področju informacijske varnosti bo v prehodnem obdobju namenjen zagotavljanju zmogljivosti, ki se nanaša na t.i. prehode za izmenjavo informacij med sistemi, ki obdelujejo, hranijo in prenašajo podatke različne stopnje tajnosti ter delujejo v različnih varnostnih domenah (High Assurance Cross Domain Information Sharing).
V smislu varovanja informacij se v cilju sil zahteva tudi vzpostavitev nacionalne infrastrukture javnih ključev PKI, pri čemer bo infrastruktura zgrajena na istih standardih, s tem pa bo omogočeno medsebojno priznavanje (angl. Cross-certification). Poseben poudarek bo namenjen tudi razvoju sistemov za elektronsko distribucijo kriptografskega materiala in elektronskemu upravljanju s kriptografskim materialom v celoti.
Posebno področje zmogljivosti zajema ustanovitev CIRC (angl. Computer Incident Response Capability) in vzpostavitev CC2 (angl. Cyber Command and Control) zmogljivosti v povezavi z nepravilnim delovanjem in kibernetskimi napadi na NATO-ve in nacionalne KIS.

Na področju informacijskih storitev je zahtevan širok spekter zmogljivosti. Razvoj in zmogljivosti, izražene v cilju sil »Network enabled services«, so usmerjene v nadgrajevanje storitev v sistemu izobraževanja in izvajanje simulacij ter povezovanje nacionalnega izobraževalnega sistema z NATO-vim naprednim izobraževalnim omrežjem ADL (angl. Advanced Distributed Learning) preko zaščitenega NATO-vega in javnega omrežja za vse učne in vadbene centre SV. V tem smislu bo potrebno vzpostaviti osnovne pogoje za izvajanje omrežnega urjenja, s povezavo preko simulacij, z ostalimi NATO članicami. Nadgraditi bo potrebno sistem NETN (angl. NATO Education and Training Network) in v operativno uporabo implementirati omrežno urjenje na konstruktivnih, virtualnih in živih simulacijah LVC (angl. Live Virtual Constructive) in zmogljivosti za izdelavo analiz.

Ena pomembnejših storitev bo tudi storitev zagotavljanja geoprostorskih podatkov, katere namen je pridobiti čim natančnejšo sliko nekega področja REP (angl. Recognised Environmental Picture), integrirano v sistem poveljevanja in kontrole. Storitev je namenjena za štabno odločanje in prostorske analize. Za zagotavljanje geoprostorskih informacijskih storitev bo NATU potrebno posredovati prostorske, meteorološke in oceanografske podatkovne baze po predpisanih standardih, razviti lastno GEOMETOC

podatkovno bazo in aplikativne programske produkte ter razviti vmesnike za mobilni dostop do GEOMETOC podatkov. Zahtevana bo kompatibilnost z NATO-vimi sistemi in možnost distribucije prikaza (REP) kopenskim silam, mornariškim silam in letalstvu. Realizacija cilja in zagotovitev zmogljivosti je tipično medresorska, saj zahteva sodelovanje MORS z Ministrstvom za okolje in prostor ter energetiko (Geodetska uprava RS za prostorske podatke in Agencija RS za okolje za meteorološke podatke) in je v veliki meri odvisna od njihovega sodelovanja.

Za potrebe zagotavljanja vzdržljivosti sil in zagotavljanja zdravstvenih storitev se bodo zmogljivosti razvijale v smeri vzpostavitve zdravstvenega informacijskega sistema MIMS (angl. Medical Information Management System), predvsem za potrebe pripadnikov sil SV, ki se nahajajo na operacijah. Sistem pa bo na varen način z zagotavljanjem vseh varnostnih atributov podatkov sposoben posredovati zdravstvene podatke vsem upravičenim naslovnikom v operativni sestavi, tako na nacionalni kot na večnacionalni ravni in omogočal zdravstveno operativno načrtovanje, spremljanje zdravstvenega stanja, upravljanje z zdravstveno dokumentacijo in zdravstveno oskrbo v celoti. V tem smislu bo potrebno zagotoviti integracijo nacionalnega zdravstvenega informacijskega sistema z NATO-vim MEDICS (angl. Medical Information and Coordination System) in na medresorski ravni ustrezno dopolniti zakonodajo.

Vzpostaviti bo potrebno komunikacijski informacijski sistem za zbiranje, obdelavo in posredovanje podatkov o NRKB dogodkih. Sistem mora biti, kot eno od funkcijskih področij, vključen v informacijski sistem poveljevanja in kontrole ter hkrati omogočati posredovanje podatkov civilnim ustanovam. Sistem bo namenjen delovanju v nacionalnem obrambnem sistemu do operativne ravni poveljevanja in kontrole.

Na področju podatkovne povezljivosti bo potrebno pripraviti okvir, ki bo s formiranjem interesnih skupin uporabnikov za posamezna področja COI (angl. Communities of Interest) in s postavitvijo ustrezne infrastrukture omogočal izdelavo ustreznih nacionalnih podatkov ter vidnost, dostopnost in razumljivost podatkov, dostopnih za NATO (preko ontologij, taksonomij in vzpostavitev metapodatkovnega registra), v skupnem informacijskem omrežju, v katerem je mogoče voditi, urejati, primerjati, povezovati podatke. V nadaljevanju bo potrebno pripraviti vse za uvedbo skupnih NATO taktičnih podatkovnih storitev NTDES (angl. NATO Tactical Data Enterprise Services) v skladu z zahtevami NTDES, kot semantično in podatkovno interoperabilnost.

2.3.2 Vpliv zmogljivosti omrežnega delovanja na spremembe na področju organizacije in kadrov

Zmogljivosti omrežnega delovanja vplivajo na organizacijsko-formacijsko strukturo predvsem z avtomatizacijo posameznih procesov. Organizacija mora slediti funkciji, ki jo ima posamezna zmogljivost, če želimo, da zmogljivost, zgrajena na podlagi zmogljivosti omrežnega delovanja, doseže svoj efekt (potencial). Pri postavitvi organizacijsko-formacijske strukture poveljstev in enot moramo vzpostaviti tesno povezavo med konceptom, procesi, ki se izvajajo in tehnologijo, ki je na voljo. Le na ta način bo organizacijska struktura ustrezala konceptom izvajanja operacije. Organizacijska struktura mora olajšati in pospešiti pretok informacij ter materiala (oskrbe z materialnimi sredstvi), ki so potrebni za izvedbo naloge. Organizacijska struktura mora onemogočiti nastanek organizacijskih ovir ali časovnih zamikov, ki znižujejo učinkovitost realizacije nalog.

Organizacijska struktura se v SV nenehno spreminja. Ali se spreminja v smeri strukture, ki bo sposobna na podlagi konceptov in opredeljenih procesov nadgraditi ter udejaniti zmogljivosti, ki jih nudi koncept in zmogljivosti omrežnega delovanja? Dvomim, da smo trenutno na pravi poti. Na bazi zmogljivosti omrežnega delovanja zgrajena organizacijska struktura bo veliko agilnejša (gibčna, okretna) od trenutnih. Zmogljivosti omrežnega delovanja bodo omogočale t.i. virtualno operativno organiziranost, ki bo formirana le za izvedbo določene naloge ali za izvedbo nalog v določenem časovnem obdobju (t.i. task force), NATO pa se bo ta t.i. virtualna organizacija vrnila v okvir obstoječe strukture. Zaradi večjih zmogljivosti, ki jih dosegajo enote z zmogljivostjo omrežnega delovanja, se lahko struktura posameznih enot zmanjšuje. Zmogljivosti omrežnega delovanja prav tako omogočajo zmanjševanje strukture poveljstev, saj se procesi, za katere je bilo nekoč potrebno veliko korakov in ljudi, potrebnih za njihovo realizacijo, skrajšujejo ter avtomatizirajo. Če želimo dejansko in uspešno pristopiti k transformaciji sil SV, moramo usmeriti vse napore k formiranju organizacijske strukture, ki ne bo politično motivirana. Tako umetno ohranjamo strukturo posameznih poveljstev in enot, ki ne prispevajo k uspešni transformaciji SV.

Tudi strukturo in infrastrukturo izobraževalnih ustanov je potrebno uskladiti in nadgraditi zahtevam, ki izhajajo iz koncepta omrežnega delovanja. Večjo pozornost je potrebno nameniti organizacijskim enotam v SV, ki se ukvarjajo z eksperimentiranjem, raziskavami ter razvojem konceptov in zmogljivosti. Jasno bo potrebno, ne ločiti, pač pa uskladiti vlogo

CDR v procesu izobraževanja in v procesu razvoja doktrinarnih dokumentov. Smatram, da je potrebno vlogo predavatelja oz. učitelja opredeliti v okviru posameznih kateder za vsebine, ki naj bi se izvajale v okviru PDRIU oz. posameznih izobraževalnih ustanov v okviru SV, ta segment pa tesno povezati s pripadniki, ki se nahajajo v CDR.

Ko govorimo o spremembah strukture na strateški in operativni ravni, je potrebno transformacijo gledati z vidika procesov, ki se odvijajo na teh ravneh, in strukture, ki te procese izvaja. Iz prakse lahko ugotovimo, da se procesi na strateški ravni podvajajo, prav tako je s strukturo, ki je izvajalec teh procesov. Tako imamo na Generalštabu, kot najvišjem organu SV, in MORS-u podvojene strukture, ki se ukvarjajo z istimi procesi, podprocesi in nalogami, ki naj bi bile v okviru pristojnosti posameznih organizacijskih enot. Podobno lahko ugotovimo tudi med strateško in operativno ravnjo poveljstev SV. Zaradi neusklajenosti prihaja do podvajanj, v nekaterih segmentih do prekrivanja pristojnosti in odgovornosti, na drugih področjih pa ni ustreznih segmentov, ki naj bi naloge ter aktivnosti iz posameznega procesa ali podprocesa izvajali.

Ljudje so osnovni in najpomembnejši del zmogljivosti, saj so le-ti ključni elementi, ki koncepte pretvarjajo v realnost. Ljudje morajo razmišljati v duhu zmogljivosti, ki jih prinaša in zagotavlja omrežno delovanje. Zato so potrebna informiranja in izobraževanja, ki bodo omogočila udejanjanje koncepta omrežnega delovanja. Omrežno delovanje zahteva spremembo doktrine tako, da bo le-ta podpirala procese, ki se izvajajo. Omrežno delovanje zahteva spremembo miselnosti ljudi in veliko večje razumevanje informacij, ki so odločevalcem na voljo, procesov in orodij za obdelavo podatkov ter senzorjev, ki omogočajo zbiranje podatkov. Vse skupaj se pretvarja v zavedanje situacije na bojišču. Pri tem govorimo o doseganju »Superiornosti odločanja«, ki ga lahko opredelimo kot stanje, pri katerem se boljše odločitve distribuirajo in izvajajo hitreje, kot lahko nasprotnik reagira. »Superiornost odločanja« je kritično povezana in odvisna od doseganja informacijske prevlade, boljšega pregleda nad situacijo na bojišču med izvajanjem vseh faz operacije, ki omogoča boljše poznavanje situacije na bojišču, kot jo ima nasprotnik. To zagotavlja večjo usklajenost in učinkovitost izvajanja operacij ter skrajšanje faz odločanja. Posamezniki morajo poznati bojno polje kot celoto in tudi vlogo ostalih na bojnem polju. Razviti moramo doktrino oz. modificirati/poudariti principe, ki so neločljivo povezani z omrežnim delovanjem, opredeliti novo vlogo posameznih akterjev na bojišču in njihove medsebojne povezave.

Večji poudarek je potrebno nameniti zagotavljanju zaupanja ljudi v sisteme C4ISR in informacije, ki jim jih sistem daje na voljo, ter v orodja, ki jih pripadniki uporabljajo pri obdelavi podatkov.

Izhajajoč iz miselnosti hladne vojne, je še vedno dominantno razmišljanje, povezano z varovanjem informacij. Koncept omrežnega delovanja, skupaj s konceptom operacij, ki temeljijo na učinkih EBO (angl. Effects Based Operations), kjer je ključen poudarek namenjen izmenjavi informacij vseh, ki prispevajo k realizaciji zastavljenih ciljev, mora spremeniti razmišljanje ljudi in nagibati tehtnico v smer potrebe ter želje po izmenjavi informacij, upoštevajoč tudi varnostne atribute informacij. Pretiravanje v segmentu varnosti informacij onemogoča njihovo izmenjavo, to pa je v nasprotju s konceptom omrežnega delovanja.

V smislu razvoja kadrov bo prišlo do sprememb predvsem tudi na izobraževalnem področju.

V smislu sodelovanja in urjenja posameznikov, poveljstev in enot s poveljstvi ostalih članic NATA, zmanjševanju stroškov ter poenostavljanja in poenotenja postopkov je potrebno zagotoviti večje število izobraževanj na združenih distribuiranih računalniško podprtih vajah NATA, kjer se preverja izvedljivost konceptov in zagotavlja sodelovanje naših pripadnikov v različnih vlogah (vadbenci, nadzorne skupine …) in predstavljajo edinstveno in cenovno najugodnejšo obliko izobraževanja kadra, ki bo v takih strukturah sodeloval. Zaradi majhnosti oboroženih sil Slovenija namreč nima izkušenj v izvedbi združenih operacij na strateški ter operativni ravni, kot članica NATA pa bo s svojimi pripadniki prav gotovo sodelovala v NATO-vih poveljstvih na najvišjih ravneh. Zaradi sodelovanja pri določenih aktivnostih se bodo lahko skupaj urila poveljstva in enote SV ter enote NATA in ostalih članic zavezništva ter partnerskih držav. Sistem mora omogočati dostop do standardiziranih izobraževalnih vsebin, ki jih lahko države članice uporabljajo za izobraževanje lastnega kadra ter pripravo za misije.

Transformacija in zmogljivosti omrežnega delovanja zahtevajo tehnično bolj izobražen in ozaveščen kader. Pri tem ne govorimo le o tistih, ki se bodo ukvarjali z upravljanjem komunikacijskih in informacijskih sistemov, pač pa o uporabnikih storitev tega sistema. Od uporabnika se več ne zahteva le poznavanje vmesnika, preko katerega prihaja do želenih podatkov in gumbov na posameznih napravah, ki jih uporablja. Zahteva se globlje poznavanje sistema kot celote. Pri mnogih ključnih posameznikih v sistemu je čutiti odpor do sprememb in novosti, ki jih prinašajo tehnološke rešitve. Zato je potrebno večje napore usmeriti v informiranje vseh pripadnikov o rešitvah, ki učinkovito pripomorejo k reševanju

nalog, za katere so odgovorni v okviru posameznega procesa in ustvariti zaupanje v tehnološke rešitve. Ključni problemi običajno ne nastajajo zaradi tehnologije, ampak zaradi neurejenih procesov in neustreznih podatkov v sistemu, za katere so odgovorni uporabniki in upravljavci posameznega procesa. Vzpostaviti je potrebno tesno povezavo med pripadniki, ki se ukvarjajo z operativnim delom, razvojem tehnoloških rešitev in tistimi, ki se ukvarjajo z razvojem doktrin ter konceptov.

Za zagotavljanje zmogljivosti omrežnega delovanja in doseganja informacijske prevlade se vse enote in poveljstva ter oborožitveni sistemi opremljajo z različnimi komunikacijskimi in informacijskimi sistemi. Sistemi postajajo kompleksnejši, razen prilagoditve strukture pa zahtevajo tudi večje število ustrezno usposobljenega kadra za upravljanje teh sistemov. Pri pridobivanju kadra ustreznega profila, s kadrovskim menedžmentom in z zadrževanjem tega kadra v strukturi SV se srečujemo, tako kot tudi vse ostale članice in NATO, z velikimi težavami. V zvezi s tem sta možni dve rešitvi: prva se nanaša na zagotavljanje posameznih storitev pri zunanjem izvajalcu (t.i. outsourcing) ali pa pristopiti k ustreznejšemu načinu reševanja zgoraj omenjenih problemov v SV. Samo kupljena tehnika namreč še ne pomeni zmogljivosti, SV pa se ravno na ta način loteva uvajanja novih zmogljivosti na tem področju. NATO namenja temu področju izjemno pozornost, tudi pri zagotavljanju kadrovskih virov, saj se zaveda pomembnosti prispevka pri zagotavljanju bodočih zmogljivosti zavezništva pri transformaciji kot celoti.

2.3.3 Vpliv zmogljivosti omrežnega delovanja na doktrinarnem področju

Spremembe v konceptu izvajanja operacij morajo zagotoviti usklajenost načina izvajanja operacij z dejanskimi zmogljivostmi, ki jih prinašajo zmogljivosti omrežnega delovanja. Da bi videli, ali je koncept izvajanja operacij dejansko usklajen z zmogljivostmi omrežnega delovanja, moramo videti, ali dosega vse učinke in prednosti, ki bi jih informacije ter zmogljivosti (senzorjev, oborožitvenih sistemov, enot …) lahko dosegle v zahtevanem časovnem obdobju izvajanja operacije. Koncept, ki je usklajen z zmogljivostmi omrežnega delovanja, mora biti usmerjen v identifikacijo, izbor in uporabo tistih zmogljivosti lastnih sil, ki prinašajo največji možni učinek in nadvlado nad nasprotnikom ter doseganje želenega cilja.

V NATU je za področje transformacije odgovorno poveljstvo ACT (angl. Allied command Transformation). MORS v svojih usmeritvah, kljub zavezam, ne omenja transformacije v smeri zmogljivosti omrežnega delovanja. V SV je za področje transformacije odgovorno

Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje (PDRIU), v njegovi sestavi pa je več organizacijskih enot, pristojnih za to področje, med njimi Center za doktrino in razvoj ter ORIS (CORSA), ki pa se tem vprašanjem ne posvečajo v ustrezni meri. Lahko bi celo dejal, da njihovo delo ni težiščno usmerjeno v preučevanje tega področja in iskanje ustreznih rešitev. Za zagotovitev njihovega delovanja in doseganja ustreznih rezultatov bo to področje potrebno kadrovsko okrepiti ali pa spremeniti težišče izvajanja njihovih aktivnosti. V smislu zagotavljanja skladnosti razvoja vseh področij transformacije je potrebno posebno pozornost nameniti izdelavi doktrinarnih in konceptualnih dokumentov, ki bodo podpirali koncept omrežnega delovanja. Tako bo potrebno razvijati lastne koncepte, ki bodo usklajeni z NATO-vimi koncepti. Večine področnih doktrin SV prav tako še vedno nima. Pospešiti bo potrebno izdelavo ustreznih doktrinarnih in konceptualnih rešitev, saj so le-te podlaga za implementacijo na ostalih področjih transformacije. Brez njih se transformacija izvaja stihijsko, brez pravega kompasa, kriterijev in pokazateljev, ki bi kazali, ali transformacijo peljemo v pravo smer.

Tudi v procesu poveljevanja in kontrole, gledano z vidika bodočih konceptov in zmogljivosti enot, oborožitvenih sistemov, senzorjev ter komunikacijskih in informacijskih sistemov, ki obdelujejo podatke in se odzivajo v skladu z definiranimi procesi ter odločitvami poveljnika lahko pričakujemo spremembe, predvsem pri spremljanju procesa poveljevanja in kontrole skozi časovno determinanto. Zmogljivosti omrežnega delovanja namreč omogočajo znatno skrajšanje odzivnosti posameznih sistemov in enot, hkrati pa v skoraj realnem času omogočajo kontrolo realizacije aktivnosti. Tako se praktično do sedaj časovno ločeni aktivnosti v procesu poveljevanja in kontrole združujeta, pojavi pa se nov, pomembnejši vidik v tem procesu – sinhronizacija oz. koordinacija, ki postane veliko pomembnejša in kompleksnejša. Če govorimo o kontroli kot časovni determinanti, ki je vsebinsko zajemala nadzor realizacije odločitve poveljnika, se je le-ta z uvedbo zmogljivosti omrežnega delovanja izjemno skrajšal, saj zmogljivosti omrežnega delovanja zagotavljajo kontrolo realizacije aktivnosti in odločitev v skoraj realnem času, da je zaradi dinamike izvajanja operacije pomembneje zagotoviti sinhronizacijo in koordinacijo na območju izvajanja operacije. Zaradi dinamike izvajanja aktivnosti, odzivnosti enot in oborožitvenih sistemov bo potrebno segmentu sinhronizacije in koordinacije v okviru procesa poveljevanja in kontrole nameniti veliko več pozornosti. Tako lahko skozi zmogljivosti, ki jih prinaša omrežno delovanje v prihodnosti razmišljamo o spremembah iz koncepta poveljevanja in kontrole v koncept poveljevanja ter koordinacije oz. sinhronizacije.

Izvajanje ekspedicijskih operacij zahteva visoko dinamiko premeščanja poveljstev in poveljniških mest, prav tako pa zmanjšanju potrebnih sil (poveljstva), potrebnih za realizacijo nalog oz. izvajanja procesa poveljevanja in kontrole. Da bi dosegli ustrezno raven, potrebno za izvajanje ekspedicijskih operacij, je potrebno v okviru zmogljivosti omrežnega delovanja zagotoviti robusten KIS, ki bo zanesljiv in bo omogočal, da se del analitičnih aktivnosti izvaja v poveljstvih ter zmogljivostih v domovini. Zaradi tega bo potrebno ugotoviti, kateri procesi ali deli procesa se lahko oz. morajo izvajati v domovini in na ustrezen način spremeniti ter prilagoditi štabne postopke in koncept poveljevanja ter kontrole.

Na podlagi razvitih konceptov in uvajanja novih tehnologij je potrebno spremeniti ali dopolniti obstoječe programe usposabljanj, ne le za uporabo in upravljanje posameznih komunikacijskih in informacijskih sistemov.

2.3.4 Vpliv zmogljivosti omrežnega delovanja na proces uvajanja zmogljivosti

Vsi dejavniki, ki vplivajo na razvoj želenih zmogljivosti enot SV, se morajo razvijati istočasno (koncepti, sistem PINK, organizacija, doktrina, oborožitveni sistemi, omrežna in informacijska infrastruktura ter kadrovski menedžment) v enoten, nedeljiv sistem zmogljivosti SV. V tem procesu sodelujejo vsi segmenti MORS in SV, skupaj z vsemi ostalimi dejavniki, ki lahko pripomorejo k zagotovitvi želenih zmogljivosti omrežnega delovanja. V te dejavnike sodijo ostala ministrstva, izobraževalne ustanove, industrija, oborožene sile ostalih članic zavezništva in drugi. Industrija, domača in tuja, neposredno vpliva na razvoj ter uvajanje zmogljivosti, kot ponudnik določenih rešitev v zvezi z zagotavljanjem zmogljivosti. Z oboroženimi silami ostalih članic je potrebno izmenjevati izkušnje pri uvajanju posameznih zmogljivosti in rešitev, ki so bile uspešno uvedene. V tem smislu se izvajajo bilateralne aktivnosti s posameznimi članicami ali pa pristopimo k sodelovanju na vajah, ki so namenjene preizkušanju povezljivosti ali certifikaciji (potrjevanju ustreznosti oz. skladnosti) posameznih sistemov ali rešitev. V tem smislu se izvajajo vaje, kot so Combined Endeavour, CWID[8], Steadfast Cathode ipd. Sodelovanje ministrstev in organov v njihovi sestavi seveda ne zajema le segmenta, vezanega za uvajanje zmogljivosti. Razna ministrstva in organi v njihovi sestavi z različnimi

[8] CWID (angl. Coalition Warrior Interoperability Demonstration) je dogodek, namenjen preverjanju zmogljivosti komunikacijskih in informacijskih sistemov ter skladnost teh sistemov z zahtevami in kriteriji, ki jih izpostavijo bojni poveljniki. Na dogodku se preverjajo zmožnosti sistemov C4I za izmenjavo informacij.

strokovnjaki s posameznih področij aktivno sodelujejo pri izvajanju operacij kriznega odzivanja (CIMIC, OMLT …), izvajanju skupnih nalog pri predsedovanju EU, souporabi komunikacijske infrastrukture pri izvajanju skupnih nalog ipd. V procesu uvajanja zmogljivosti pa ministrstva sodelujejo pri zagotavljanju posameznih storitev, kot so zagotavljanje potrebnega frekvenčnega spektra (APEK), uvajanje IS za potrebe zdravstvene zagotovitve pripadnikov na operacijah, zagotovitev GIS podatkov, prilagajanje zakonodaje in posodabljanje strateških dokumentov, ki so bili omenjeni v uvodnem delu.

Zmogljivosti omrežnega delovanja imajo velik potencial, ki nas lahko pripelje do sprememb v našem pristopu k izvajanju operacij in ki zagotavlja večjo učinkovitost naših enot. Vsekakor se moramo zavedati, da se ta napredek ne dosega z enostavnim zagotavljanjem in uvajanjem omrežne ter informacijske infrastrukture v obstoječi sistem, kar si mnogi predstavljajo. Zaradi neustrezne sinhronizacije vseh aktivnosti in razvoja na vseh omenjenih področjih lahko pride do dejanskega zmanjšanja zmogljivosti, nezaupanja in malodušja. Da bi zagotovili uspešno uvajanje zmogljivosti omrežnega delovanja, je potrebno izdelati celovit pristop, ki bo opredeljeval spremembe na vseh področjih in posledice teh sprememb na vse elemente ali komponente SV.

Kot navaja Alberts (1999: 199) obstajata dva predpogoja za uspešno uvajanje zmogljivosti omrežnega delovanja. Le-ta sta:

- razvoj konceptov, ki bodo podpirali izvajanje sodobnih operacij, kot so koncept operacij, ki temeljijo na učinkih[9] in koncept za NATO-ve odzivne sile[10];
- sposobnost transformacije teh konceptov v realnost oz. zagotavljanje dejanskih zmogljivosti omrežnega delovanja, ki jih ne ovirajo trenutno veljavni koncepti ter zakonodaja.

Zgodovina in naša praksa sta polni primerov organizacijskih neuspehov, kjer organizacija ni bila uspešna pri zagotavljanju prednosti, ki jih zagotavlja nova tehnologija ali pa so bili ti uspehi le delni, mnogo manjši od dejanskih zmožnosti. Razlog neuspeha leži predvsem v asinhronosti zgoraj navedenih dejavnikov. Velik problem predstavljata predvsem prevelik razkorak med organizacijo in tehnološkim napredkom, pri čemer se predvsem velike organizacije, kot je ministrstvo in SV v njegovi sestavi ne morejo na adekvaten način pravočasno spremeniti ter slediti spremembam tehnologije. Tako imamo v veliki organizaciji, kot je naša v uporabi tehnološke rešitve različnih generacij, kar še veča

[9] EBO (angl. Effects Based Operations) predstavlja kratico za koncept operacij, ki temeljijo na učinkih.
[10] NRF (angl. NATO Response force) predstavlja kratico za NATO-ve odzivne sile.

razkorak med zgoraj navedenimi dejavnostmi, predvsem pa zmanjšuje interoperabilnost/povezljivost in znižuje varnost.

Informacijska doba vpliva na vodenje operacij predvsem v smislu:

- izredno visoke stopnje tehnološkega napredka in uvajanja novih tehnologij;
- prednosti, ki jih prinaša nova tehnologija, so večje, kot jih lahko izrazimo z znanimi operativnimi zahtevami in veljavnimi postopki;
- spremembe v vojski na ostalih področjih ne dohajajo sprememb v tehnoloških ciklih, zato prihaja do vse večje neusklajenosti, vojska pa ima vse manj časa za izvajanje ustreznih sprememb;
- nove zmogljivosti, ki so razpoložljive na tržišču (COTS), so dosegljive tudi našemu eventualnemu nasprotniku.

Medtem ko imamo v SV težave z uvajanjem tehnologije, pri čemer je uvajanje v teoretičnem smislu opredeljeno, imamo v praksi veliko težav z nedorečenimi pristojnostmi organizacij in posameznikov v procesu uvajanja, hkrati pa so zahteve, izhajajoče iz sprejetih ciljev sil izjemno visoke. V MO in SV se sicer izvajajo spremembe ter reforme, ki naj bi delovale v smeri skrajšanja časa od načrta do zagotovitve zmogljivosti in njihove operativne uporabnosti, vendar samo to ni dovolj za zagotovitev celovitih zmogljivosti SV. Eden od razlogov je vsekakor razkorak med tehnološkim razvojem in zmogljivostmi, ki jih prinaša nova tehnologija, ter razvojem področnih doktrin in konceptov. Zato je potrebno zagotoviti predvsem usklajenost med doktrinarnim razvojem in tehnološkim razvojem oz. zmogljivostmi, ki jih nudi uvajanje novih tehnologij. Hitrost uvajanja novih tehnologij namreč prinaša veliko težav. Zamislimo si, da uvedemo novo tehnologijo z vsemi svojimi zmogljivostmi, ne da bi pri tem spremenili procese, ki se izvajajo na poveljniškem mestu in s tem povezanimi operativnimi zmogljivostmi oborožitvenih sistemov in senzorjev. Koliko zmogljivosti, ki jih tehnologija nudi, bo dejansko uporabnih? Zelo malo. Ta scenarij se bo ponavljal ves čas, saj bodo spremembe v tehnologiji vedno prednjačile pred ostalimi potrebnimi spremembami.

Drugi razlog za neuspešno uvajanje zmogljivosti je neupoštevanje vpliva posameznih zmogljivosti, ki sicer predstavljajo samostojen cilj sil, pri zagotavljanju celotnih zmogljivosti, izraženih v kompleksnejših ciljih sil (primer L 0035). V teh ciljih se zahtevajo integrirane zmogljivosti z različnih področij. To ne zajema le nabave posameznih sredstev in sistemov ter popolnjevanja mest strelcev v npr. motoriziranem bataljonu, ampak zajema tudi ostala področja, predvsem usposobljene kadre na ostalih področjih in enotah v sestavi bataljona, sistem upravljanja, vzdrževanja, izobraževanja,

spremembe formacije itd., kar tvori celoto zmogljivosti posamezne enote. Najpogosteje pademo na izpitu pri kadrovskih vprašanjih, saj za ustrezno zmogljivost nismo sposobni zagotoviti ustreznega števila usposobljenega kadra, prav tako pa so postopki nabave in uvajanja tako zapleteni ter nepregledni, da se uvajanje zamakne v nedoločeno prihodnost.
Kaj je potrebno narediti? Povezati moramo procese in realizirati aktivnosti, ki:

- podpirajo razumevanje združevanja različnih zmogljivosti;
- omogočajo razvijanje novih konceptov, zagotavljajo testiranje in izboljšavo teh konceptov;
- usklajujejo želeno stopnjo zmogljivosti z viri, ki so na voljo;
- se osredotočajo na aktivnosti, ki zagotavljajo razvoj in uvajanje različnih zmogljivosti v operativno uporabo.

Da bi zagotovili realizacijo tega, moramo prilagoditi in sinhronizirati naše obstoječe zahteve, planske ter investicijske dokumente, vire in procese tako, da bodo pravočasno zagotovili rezultate ter zagotovili uvajanje zmogljivosti omrežnega delovanja v operativno uporabo. Trenutna praksa, ne le v Sloveniji, je popolnoma ločila procese planiranja zahtev, zagotavljanja virov, načrtovanja arhitekture ter razvoja in nabave posameznih segmentov zmogljivosti. S tem, namesto, da bi se procesi medsebojno dopolnjevali in nadgrajevali naše zmogljivosti, dobimo ravno nasproten učinek.
V procesu izvajanja nabav novih sistemov se še vedno oklepamo tradicionalnega pristopa (angl. waterfall), ki se je izvajal korak za korakom, od priprave operativnih zahtev, ki so bile potrjene, NATO pa so daljši čas razvijali sistem, ki so ga predali v operativno uporabo popolnoma drugim uporabnikom. V fazi transformacije se priporoča uvajanje novega sistema nabave, pristop k t.i sistemu razvojnega pridobivanja/nabave (angl. evolutionary acquisition). Ta sistem izvajanja nabav je bil razvit na podlagi stalnega nezadovoljstva z rezultati nabave in uvajanja posameznih zmogljivosti v operativno uporabo. Najpogosteje je bil sistem uveden prepozno, z ogromnimi stroški. Kar je še slabše, ko je bil sistem uveden, ni več ustrezal operativnim zahtevam in ni zagotavljal funkcionalnosti, ki so bile izpostavljene na začetku procesa nabave. Pred uvedbo novega sistema razvojnega pridobivanja/nabave so verjeli, da so za slabe rezultate krive slabo napisane operativne zahteve. A pripravljavci razvojnega sistema nabave so ugotovili, da izdelovalci operativnih zahtev niti niso mogli dovolj natančno specificirati svojih zahtev, saj sistema in njegovih zmogljivosti niso poznali. Šele takrat, ko je bila uvedena, so videli zmogljivosti in njihov vpliv na procese, ki so jih zmogljivosti podpirale. Tako moramo v sistemu razvojnega pridobivanja/nabave izbrati pristop po strategiji malo ali del zmogljivosti izgradi/izdelaj,

malo testiraj, malo uvedi s ponavljanjem in prekrivanjem ciklov, pri čemer je potreben poseben poudarek nameniti tesni povezavi uporabnikov, razvijalcev zmogljivosti in tistih, ki zmogljivosti uvajajo v celotnem obdobju. Ob tem ne smemo pozabiti na istočasen razvoj ustreznih konceptov, pri izdelavi katerih morajo sodelovati strokovnjaki iz operativnega in tehničnega področja.

Izjemno pomemben dejavnik v fazi uvajanja je tudi standardizacija, kot postopek sprejemanja standardov in uporabe le-teh v uvedenih rešitvah. S tem se izognemo nepotrebnim stroškom in hkrati zagotovimo povezljivost oz. uporabnost uvedenih rešitev. Mnogi standardi, ki so zahtevani v ciljih sil, še niso razviti, saj se predvideva dolgotrajen razvoj zmogljivosti omrežnega delovanja. Zato ni potrebno hiteti z uvajanjem rešitev, ki morda ne bi bile v skladu s standardi, ker le-ti trenutno še ne obstajajo.

2.4 PREDLOGI SPREMEMB V ZVEZI S TRANSFORMACIJO, IZHAJAJOČI IZ VPLIVOV OMREŽNEGA DELOVANJA

Predlogi, ki sledijo v nadaljevanju, so plod dosedanjih izkušenj, pridobljenih na različnih funkcijah v SV in preučevanja različne literature ter dokumentov, povezanih z zagotavljanjem zmogljivosti omrežnega delovanja. Ena ključnih nalog na najvišji ravni je posodobiti vse strateške dokumente, vključno z zakonskimi dokumenti, ki morajo na ustrezen način omogočati in podpirati razvoj zmogljivosti omrežnega delovanja ter odražati dejanske zmožnosti družbe za uresničitev posameznih ciljev in zmogljivosti. Nerealne usmeritve, ki predstavljajo »seznam želja« in nimajo realne osnove, zamegljujejo zahteve po želenem končnem stanju v določenem obdobju, hkrati pa omogočajo raznoliko tolmačenje izhajajočih aktivnosti in izbiranje prioritet. S tem onemogočajo sinhronizacijo aktivnosti za doseganje skupnih ciljev, navedenih v strateških dokumentih.

Implementacijo zmogljivosti omrežnega delovanja in zavez, ki jih je dala RS, je potrebno dvigniti na višjo raven, saj zmogljivosti, ob upoštevanju novih konceptov, presegajo raven obrambnega resorja. V zvezi s tem je potrebno dvigniti na višjo raven tudi medresorsko usklajevanje, saj so za doseganje posameznih zmogljivosti v določenih segmentih pristojna različna ministrstva. Za medresorsko usklajevanje je potrebno identificirati nosilca na ravni ministrstva.

Pripraviti je potrebno pregled zmogljivosti in vseh ciljev sil, na katere neposredno ali posredno vplivajo zmogljivosti, ki se gradijo v okviru ciljev sil s področja omrežnega delovanja. Le na ta način bomo dobili relevantne podatke o potrebnih virih (finančnih in

kadrovskih), ki jih je potrebno v okviru teh ciljev zagotoviti za doseganje zmogljivosti omrežnega delovanja.

Zagotoviti je potrebno skladnost razvoja tehnoloških zmogljivosti z razvojem konceptualnih rešitev in zmožnostjo zagotavljanja virov za realizacijo, kar je trenutno v velikem razkoraku. Pri realizaciji teh aktivnosti morajo sodelovati vsi sektorji, odgovorni za planiranje in zagotavljanje zmogljivosti kakor tudi virov. Proces je potrebno izvajati skupaj, ne pa ločeno, v okviru sektorjev, kot se to izvaja v okviru trenutne prakse.

Spremembe v sistemu nabave sistemov za zagotavljanje zmogljivosti omrežnega delovanja so nujne. Sprejeti je potrebno filozofijo in sistem razvojnega pridobivanja, ki je edini učinkoviti mehanizem za uspešno uvajanje teh sistemov v operativno uporabo. V tem procesu je potrebno jasno definirati pristojnosti in odgovornosti posameznih dejavnikov, ki sodelujejo v tem procesu, predvsem pa tesno povezati razvijalce rešitve, ki so v večini primerov ponudniki izdelkov domače ali tuje industrije in uporabnikov.

Senzorski sistemi so neposredno povezani s komunikacijskimi in informacijskimi sistemi. Na to povezanost nakazuje tudi kratica C4ISR. V SV je ta segment razdrobljen na različna funkcijska področja, zaradi tega pa neustrezno usklajen. Vsekakor uporabniki, ki pripravijo operativne zahteve, sodijo na različna področja. Tehnološki segment pa bi kazalo združiti v strokovnem organu, odgovornem za C4ISR. Temu je potrebno prilagoditi tudi strukturo strokovnega organa.

Izobraževalni sistem SV je potrebno prilagoditi zahtevam in zmogljivostim omrežnega delovanja. Rešitve, ki jih nudijo zmogljivosti omrežnega delovanja, je potrebno približati pripadnikom SV na način, da zmogljivosti ne bodo predstavljale dodatnega bremena in izgube časa, ampak koristen pripomoček pri realizaciji nalog. Vsebine, izhajajoče iz zmogljivosti omrežnega delovanja, je potrebno redno dopolnjevati v vseh programih VIU. Posodobiti je potrebno tudi izobraževalno infrastrukturo, ki bo omogočala pridobivanje novih znanj.

Vse obstoječe področne doktrine in koncepte je potrebno dopolniti, nadgraditi oz. uskladiti tako, da bodo v največji meri omogočali uporabo zmogljivosti omrežnega delovanja in tistega, kar nudi omrežna in informacijska infrastruktura pri zagotavljanju teh zmogljivosti.

Velikost in strukturo SV je potrebno prilagoditi virom ogrožanja in poslanstvu, ki ga ima SV v okviru zagotavljanja nacionalne in mednarodne varnosti. Struktura mora biti prilagojena konceptom uporabe in zmogljivostim, ki jih želimo doseči z implementacijo sprejetih ciljev sil. Vsak razkorak med zgoraj navedenimi elementi v povezavi z viri, ki so nam na voljo, ter prilagajanje velikosti in strukture dnevnopolitičnim interesom in

interesom posameznikov, predstavlja vse večji prepad med načrtovanim in dejanskim stanjem. Vse to vodi v nenehne spremembe in nestabilno strukturo, ki onemogoča kvalitetno realizacijo ciljev in nalog v zvezi s transformacijo.

3. ZAKLJUČEK

Republika Slovenija in Slovenska vojska se nahajata v procesu zagotavljanja zmogljivosti omrežnega delovanja. Na tej poti so bili izvedeni mnogi koraki. Ker je doseganje zmogljivosti dolgotrajen proces, ki vsebuje mnoge spremenljivke, ni dovolj, da se izdelajo strateški in usmerjevalni dokumenti, ki naj bi veljali za vse večne čase. Potrebno je spremljati spremembe in jih vgrajevati v temeljne razvojne usmeritve. Ugotovili smo, da RS ni primer ažurnega spremljanja situacije. Ustreznega odziva še ni na vidiku. Prav tako ugotavljam, da zagotavljanje zmogljivosti omrežnega delovanja ni zastopano na ustrezno visoki ravni, saj se težišče aktivnosti odvija v okviru struktur MO in SV, ki so odgovorne za vzpostavitev omrežne in informacijske infrastrukture. V okviru naloge smo se seznanili s področji transformacije in operativnimi zahtevami, ki iz njih izhajajo. Ugotovili smo, da ta področja ne zajemajo le sprememb komunikacijske in informacijske infrastrukture, kljub temu, da je le-ta eden ključnih dejavnikov transformacije in zagotavljanja zmogljivosti omrežnega delovanja. V okviru zahtev, ki izhajajo iz ciljev sil, je evidentno izražena potreba po medresorskem sodelovanju. Ugotovljeno je, da ostale strukture državne uprave niso na ustrezen način seznanjene in v praksi zastopane v procesu transformacije SV. To sodelovanje tudi ni opredeljeno v nobenem dokumentu.

Kljub temu, da je eden ključnih področij transformacije namenjen omrežni in informacijski infrastrukturi, ki predstavlja ključen pogoj za uspešno izvedbo transformacije v smislu ustvarjanja želenih bodočih zmogljivosti, se temu področju ne namenja dovolj pozornosti v SV. V okviru poglavja o vplivu zmogljivosti mrežnega delovanja na transformacijo SV smo ugotovili, kateri so tisti dejavniki, ki na transformacijo vplivajo. Razen zagotavljanja zmogljivosti komunikacijskih, informacijskih in senzorskih sistemov je vpliv izražen tudi na področjih organizacije in kadrov, na doktrinarnem področju ter v procesu uvajanja novih zmogljivosti. Na ta način lahko potrdimo tudi hipotezo, predstavljeno v uvodnem delu, v kateri trdimo, da se transformacija in zagotavljanje zmogljivosti omrežnega delovanja ne nanašajo le na področje komunikacijskih in informacijskih sistemov, kar bi mnogi želeli prikazati.

Razen potrditve teze je ena ključnih ugotovitev te naloge potreba po sinhronizaciji vseh dejavnikov, ki vplivajo na zagotavljanje zmogljivosti in uspešno transformacijo. Med vsemi bi osebno, razen na zagotavljanje omrežne in informacijske infrastrukture, dal največji poudarek še kadrom in doktrinarnemu področju. Ugotovljeno je, da izdelava doktrinarnih dokumentov in kadrovska politika v SV ne sledita uvajanju novih tehnoloških

rešitev, zahtevam transformacije in zagotavljanju zmogljivosti omrežnega delovanja in bi lahko predstavljala glavne dejavnike neuspešne transformacije SV. Učinkovito upravljanje s kadri je namreč ključ do uspeha vsake vojske. Ugotovljeno je, da kadrovskih virov, ki bi ustrezali zahtevam transformacije, ni ali pa so nepravilno porazdeljeni. Zaradi tega je vprašljiva uspešnost transformacije. Odločevalci se morajo zavedati, da SV ne predstavlja le bojevnikov in da so v različnih enotah potrebni različni izobrazbeni profili (logistika, zveze, informatika, raketni sistemi, inženirstvo, radarska tehnika, vozniki …). V tem smislu je potrebno spremeniti sistem pridobivanja kadrov. Prav tako se vojska ne more razvijati brez ustreznih doktrinarnih dokumentov. V okviru procesa uvajanja novih zmogljivosti pa je kot ena večjih pomanjkljivosti ugotovljeno slabo sodelovanje uporabnikov in tistih, ki posamezne zmogljivosti za uporabnike razvijajo. Tako je vprašljivo, ali operativne zahteve dejansko predstavljajo tisto, kar si uporabnik želi v okviru novih zmogljivosti.

4. LITERATURA IN VIRI

1. ALBERTS, David S., GARSTKA, John J., STEIN Frederick P. (1999) Network centric warfare: Developing and leveraging information superiority 2nd edition (Revised). CCRP publication series.
2. BARTOLOMASI, P. (2005) NATO Network enabled capability, Feasibility study, Volume I, Overwiev of NATO Network Centric Operational Needs and Implications for the Development of Net-Centric Solutions, Version 2.0.
3. BOOTH M. (2005) NATO Network enabled capability, Feasibility study, Volume II, Detailed Report Covering a Strategy and Roadmap for realizing an NNEC Networking and Information Infrastructure (NII), Version 2.0.
4. Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008, Dostopno na http://www.NATO.int/docu/pr/2008/p08-049e.html (24.07.2008).
5. Buckman T. (2005) NATO Network enabled capability, Feasibility study, Executive summary, Version 2.0.
6. Compendium of NNEC Related Architectures, (27 November 2006), Enclosure 3 to 3000 SC-6 SER: NU0644.
7. Comprehensive Political Guidance Endorsed by NATO Heads of State and Government on 29 November 2006, Dostopno na http://www.NATO.int/docu/basictxt/b061129e.htm (24.07.2008).
8. E-2780 Network enabled communications (2008), Cilj sil
9. E-2781 NNEC Information assurance framework (2008), Cilj sil
10. E-2860 Network enabled information systems (2008), Cilj sil
11. E-2861 Network enabled services (2008), Cilj sil
12. JANKOVIČ, Zoran, ŠTERBENC, Marko, KOLBEZEN, Sandi, LIČAR, Saša, Koncept delovanja informacijskega sistema poveljevanja in kontrole (IS PINK), Verzija 1.0, številka 4301-79/2006-13 (01.04.2008).
13. JANKOVIČ, Zoran, ŠANTELJ, Stanislav, KOLBEZEN, Sandi, ŠTERBENC, Marko, KOLARIČ, Srečko, GOGALA, Aleš, Koncept uporabe in razvoja zmogljivosti C4I v MOTB in BBSK, Verzija 1.0, številka 4301-63/2007-69 (22.04.2008).
14. MC 477, Military Concept for the NATO Response Force (2003).

15. NATO Network enabled capability (NNEC), Business Case (2007), Enclosure 1 to 2000 SC-6 SER: NU0137.
16. NATO Network enabled capability (NNEC), Roadmap (2007), Enclosure 2 to 2000 SC-6 SER: NU0137.
17. NATO Network enabled capability (NNEC), Vision & Concept (2006), Enclosure 1 to 5000 SC-6 SER: NU0065.
18. NATO Network enabled capability, Feasibility study, (2005), Annex C to Volume II; Communication Technology for NII.
19. NATO Network enabled capability, Feasibility study, (2005), Annex D to Volume II; Information and Integration Services (IIS) for NII.
20. NATO Network enabled capability, Feasibility study, (2005), Annex E to Volume II; Information Security for NII.
21. NATO Network enabled capability, Feasibility study, (2005), Annex F to Volume II; Service Management Control Technology for NII.
22. Networked operations, The Netherlands Defence organisations steps into the future with Network Enabled Capabilities, (2006), NEC steering group of the Netherlands Ministry of Defence in Cooperation with TNO Defence, Security and Safety, Netherlands Ministry of Defence.
23. PEŠEC, Mojca; (2007) Koncept na učinku temelječih operacij (Primer ZDA in zveze NATO), Magistrsko delo, Univerza v Ljubljani, FDV.
24. Prague Summit Declaration, Press Release (2002)127, 21 Nov. 2002, Dostopno na http://www.NATO.int/docu/pr/2002/p02-127e.htm .(24.07.2008).
25. Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske (ReDPROSV), Uradni list RS, št. 89/2004.
26. Resolucija o strategiji nacionalen varnosti, Uradni list RS, št. 56-2957/2001.
27. Riga Summit Declaration, Press Release (2006)150, 29 Nov. 2006 Dostopno na http://www.NATO.int/docu/pr/2006/p06-150e.htm (24.07.2008).
28. Splošni dolgoročni program razvoja in opremljanja SV, Uradni list RS, št. 97/2001.
29. Srednjeročni obrambni program, Ljubljana, številka 803-2/2006-58 z dne 27.11.2006.
30. SVETE, Uroš, (2005) Varnost v informacijski družbi, Knjižna zbirka Varnostne študije, Ljubljana.

SEZNAM UPORABLJENIH KRATIC IN OKRAJŠAV

ACNR	Advanced Combat Network Radio
ACT	Allied Command Transformation
APEK	Agencija za pošto in elektronske komunikacije
APOD	Air Port of Debarkation
C4I	Command, Control, Communications, Computers, Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance
CDR	Center za doktrino in razvoj
CIMIC	Civil Military Cooperation
COI	Community of Interest
COP	Common Operational Picture
CORSA	Center za operacijske raziskave, simulacije in analize
CWID	Coalition Warrior Interoperability Demonstration
EBO	Effects Based Operations
FFT	Friendly Force Tracking
FP	Force Proposal
IS PINK	Informacijski sistem poveljevanja in kontrole
ISLOG	Informacijski sistem logistike
ISTAR	Intelligence, Surveillance, Target Acquisition, Reconnaissance
JC3IEDM	Joint Command Control Consultation Information Exchange Data Base
MANET	Mobile Ad Hoc Network
MIP	Multilateral Interoperability Programme
MEDICS	Medical Information and Coordination System
MIMS	Medical Information Management System
MMHS	Military Message Handling System
NAC	North Atlantic Council
NC3B	NATO Command Control Consultation Board
NC3O	NATO Command Control Consultation Organisation
NCW	Network Centric Warfare
NGCS	NATO Global Communications System
NII	Networking and Information Infrastructure
NNEC	NATO Network Enabled Capability

NRF	NATO Response Forces
NRKB	Nuklearno radiološko kemično biološko
NTDES	NATO Tactical Data Enterprise Services
PDRIU	Poveljstvo za doktrino razvoj izobraževanje in usposabljanje
PINK	Poveljevanje in kontrola
PKI	Public Key Infrastructure
POVC	Poveljniški center
QoS	Quality of Service
REP	Recognised Environmental Picture
SATCOM	Satellite Communications
SC	Strategic Commands
SCIP	Secure Communications Interoperability Protocol
SDPRO	Splošni dolgoročni program razvoja in opremljanja
SDR	Software Defined Radio
SOPR	Srednjeročni obrambni program
SPOD	Sea Port of Debarkation
TST	Time Sensitive Targeting
TTKS	Taktični telekomunikacijski sistem
VANET	Vehicle Ad Hoc Network
VTC	Video Telekonferenca
XML	Extensible Markup Language

IZJAVA O AVTORSTVU ZAKLJUČNE NALOGE

Slušatelj podpolkovnik Zoran Jankovič izjavljam, da sem avtor zaključne naloge z naslovom »VPLIV ZMOGLJIVOSTI OMREŽNEGA DELOVANJA NA TRANSFORMACIJO SLOVENSKE VOJSKE«, ki sem jo napisal pod mentorstvom dr. Uroša Svete.

S svojim podpisom zagotavljam da:
- je zaključna naloga izključno rezultat mojega lastnega dela,
- so vsa dela in mnenja drugih avtorjev, ki jih uporabljam v zaključni nalogi, navedena oziroma citirana v skladu s Postopkovnikom za izdelavo in ocenjevanje zaključne naloge na PŠŠ,
- se zavedam, da je plagiatorstvo kaznivo po Zakon o avtorskih in sorodnih pravicah, (Uradni list številka 21/1995, 9/2001), prekršek pa podleže tudi ukrepom disciplinske odgovornosti v skladu s Pravili službe v Slovenski vojski,
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo zaključno nalogo in moj status v Slovenski vojski.

S podpisom se odrekam vsem materialnim pravicam v zvezi z zaključno nalogo in dovoljujem uporabo zaključne naloge v študijske namene za potrebe Slovenske vojske.

V Poljčah, dne 21.08.2008 Podpis:_____