UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Sašo Vene

# Izzivi omrežno-centričnega bojevanja

Diplomsko delo

Ljubljana, 2014

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Sašo Vene

Mentor: doc. dr. Uroš Svete

# Izzivi omrežno-centričnega bojevanja

Diplomsko delo

Ljubljana, 2014

***Zahvala***

*Zahvaljujem se mentorju za pomoč pri izdelavi diplomske naloge, za vse nasvete in koristne informacije.*

*Še posebej bi se zahvalil mami in bratu, ki sta me skozi študij podpirala tako finančno kot drugače; hvala vama! Zahvalil bi se tudi moji punci Ani, ki me je spodbujala, da sem dokončal svojo nalogo.*
*Hvala lepa vsem!*

**Izzivi omrežno-centričnega vojskovanja**

Sile Združenih držav Amerike (ZDA) so po koncu prve iraške vojne leta 1990 prišle do transformacije, kako z informacijsko dominacijo in z manjšo silo premagati številčno večjega nasprotnika. Ideja, ki temelji na situacijskem zavedanju in omogoča samo-sinhronizirane, je koncept v doktrini omrežno-centričnega vojskovanja. V svoji diplomski nalogi se sem osredotočil na raziskavo tega koncepta, od teorije pa do praktične uporabe v drugi vojni ZDA v Iraku leta 2003. Zanimalo me bo, kako tehnologija in vojaški programi povezovanja vplivajo na ognjeno moč posameznega sistema, zato bom z analizo ognjene moči primerjal oborožitveni sistem v 1. iraški vojni leta 1990 ter v 2. iraški vojni leta 2003. Ker vsaka nova doktrina ni popolna, bom v zaključnem delu diplomske naloge izpostavil izzive omrežno-centričnega vojskovanja. S tem želim pokazati, da je bil koncept v prvih fazah iraške invazije leta 2003 uspešen, ognjena moč se je povečala in da doktrina ponuja veliko priložnosti v prihodnosti bojevanja. Vendar obstajajo ovire, na katere je treba biti pozoren, da ne bo prihajalo do napak in posledično do neuspešnosti misij.

**Ključne besede:** omrežno-centrino vojskovanje, izzivi, programi, načela, ognjena moč.

**The challenges of network-centric warfare**

Forces of the United States of America (USA) as at the end of the first Iraqi war in 1990, came to the transformation, based on information dominance, allowing smaler force to defeat larger opponent. The idea is based on situational awareness which allows self-synchronizetion, and those ideas are the concept in the doctrine of network-centric warfare. In my paper degree I focused on studying of this concept from theory to practical use USA doctrine in Iraq war in 2003. I was interested in how technology and military integration programs affect the firepower of each system, I compared and analys two wepon systems from 1. Iraq war in 1990 and 2. Iraq war in 2003. Since any new doctrine isn't perfect at the first practical use of it, I pointed out the challenges of network-centric warfare. I came to the conclusion, that the concept in the first phases of the Iraqi invasion in 2003 was successful, fire power has increased and that the doctrine offers a lot of opportunities in the future of warfare. However, there are obstacles to which attention must be drawn.

**Keywords**: Network-centrino warfare, challenges, programs, principles, fire power.

## Kazalo vsebine

**Kazalo slik:**



**Kazalo tabel:**

# 1 Uvod

Vojna je produkt svoje dobe in tudi sredstva ter orodja, s katerimi se bojujemo, so se razvijala skupaj s tehnologijo. Živimo v dobi, ko sta tehnologija in način življenja posameznika in družbe napredovala do te mere, da so informacije stalnica našega družbenega povezovanja in obstoja, s katerimi razpolagamo iz dneva v dan in nas obkrožajo pri vsem, kar počnemo. Če lahko te informacije šifriramo in izluščimo iz njih tiste, za katere mislimo, da so za doseganje naših ciljev najbolj pomembne, potem nam to omogoča prednost za dosego teh ciljev v čim krajšem in najbolj efektivnem času.

V celotnem 20. st. so napredki v tehnologiji sovpadali s pomembnimi razvoji v načinu vodenja bojev, ki jih vojske vodijo po svetu. Od uporabe konjeniške enote v izbruhu prve svetovne vojne pa do uporabe zračnih plovil brez posadke (unmanned aerial vehicle ali UAV) je tehnologija omogočala načine, da so se vojaške operacije razvijale. Tako tudi v 21. stoletju tehnologija še naprej igra veliko vlogo pri tem, kako vojske delujejo in se obnašajo v določenih konfliktih po svetu. Vendar pa ne gre le za spremembe novih orožij, letal, vojaških ladij, ampak tudi za načine komuniciranja, s katerimi se širijo informacije, dajejo povelja ter se poroča svojim nadrejenim. Natančneje računalnik, radio in podatkovna omrežja povežejo skoraj vsa vojaška sredstva in rodove ter s tem omogočijo, da se lahko poveljujoči na kopnem v Afganistanu preko komunikacijskih sredstev poveže s podmornico, ki pluje pod vodo Perzijskega zaliva. Bojevanje v informacijski dobi bo neizogibno poosebljajo karakteristike, ki bodo razlikovale to dobo od vseh prejšnjih dob bojevanja.

Zato je tudi na vojaškem področju prišlo do novega koncepta informacijskega tandema. Leta 1990 so Združene države Amerike (ZDA), ki so po izdatkih, namenjenih obrambi, vodilna država na svetu, v okviru ministrstva za obrambo prve govorile o uvedbi nove doktrine network-centric warfare (na omrežjih temelječe bojevanje[1]) ali drugače network-centric operations (omrežno-centrične operacije). Slednje pomeni prenos prednosti informacijskih sistemov in tehnologije na vojaško področje z omrežnim povezovanjem dobro obveščenih, geografsko razpršenih vojaških sil. Ta doktrina si prizadeva dominirati informacijsko prednost z izkoriščanjem informacijske tehnologije.

Za diplomsko delo s to temo sem se odločil, ker je ta koncept bojevanja še relativno mlad. Ta koncept poleg ameriške vojske vpeljujejo tudi druge države (Avstralija, Indija), nekatere ga že imajo ter ga izpopolnjujejo (Velika Britanija). Nedavne vojne ZDA v Iraku in Afganistanu,

[1] V diplomski nalogi bom uporabljal izraz omrežno-centrično vojskovanje

kjer se je bojevanje z novo doktrino prvič pojavilo, so pokazatelj njene prednosti tako v operativni ravni kot na bojiščih. Zanima pa me, kaj prinaša omrežno-centrično vojskovanje ter kakšni so izzivi v prihodnosti, ali se bo trend vojaške doktrine obdržal ali pa ga bo zamenjala nova bolj izpopolnjena in nadgrajena doktrina.

Cilj moje naloge je, da predstavim koncept omrežno-centričnega bojevanja, od zamisli do konca, katere so značilnosti ter katere so povezane tehnologije, sistemi in programi znotraj tega koncepta. Za lažje razumevanje bom v prvem delu diplomske naloge razložil termine in delovanje skozi teoretskih del ter predstavil načela, za katera menim, da so izhodišča za razvoj tega koncepta. V drugem delu bom predstavil programske sisteme, skozi katere deluje omrežno-centrično vojskovanje, primerjal bom tudi ognjeno moč med prvo iraško vojno iz leta 1990 ter drugo iraško vojno leta 2003 (kjer je bila doktrina prvič v uporabi) in pogledal primere delovanja v realnih situacijah ter izkušnje, ki so prinesle prve vidike napak v sistemu.

# 2 Metodološki okvir

## 2.1 Predmet in cilj proučevanja

Kot predmet proučevanja sem izbral sam koncept omrežno centričnega sistema in posledično bojevanja. Za razumevanje koncepta sem se lotil same analize, kaj vse spada pod ta termin in kateri so sistemi, ki so povezani v omrežno-centrični koncept ter kako se to vidi v današnjih spopadih z vidika Združenih držav Amerike (ZDA). V začetku diplomske bom predstavil sistem od uveljavitve leta 1996, ko je avtor, takratni ameriški admiral William Owens, predstavil koncept, pa vse do uporabe sistema današnjega dne. Nato se bom osredotočil na praktično delovanja samega sistema, omenil nova načela, na katerih temelji omrežno-centrični sistem. Prestavil bom tudi cilje, ki jih omrežno-centrično vojskovanje poizkuša zagotoviti. Moje raziskovalno vprašanje je, ali obstajajo nova načela in principi vojskovanja po tej doktrini ter kaj novega nam prinaša omrežno-centrično vojskovanje iz operativne rabe ter kako se to vidi v vojni v Iraku in Afganistanu. V zaključku dela bom podal svoje ugotovitve, sprejel ali zavrgel hipotezo in povezal celotno diplomsko nalogo.

Cilj moje diplomske naloge je analizirati sam sistem in koncept omrežno centričnega bojevanja, predstaviti cilje, katere poizkuša sistem zagotoviti, primerjati ognjeno moč brez in z nadgradnjo, ki temelji na omrežno-centričnem bojevanju, in odkriti slabosti ter napake, ki obstajajo znotraj tega sistema.

## 2.2 Hipoteza

V analizi svoje diplomske naloge sem si postavil hipotezo:

**Hipoteza 1:** Novi vojaški programi oboroženih sil Združenih držav Amerike, ki podpirajo omrežno-centrično vojskovanje, nadgrajujejo sisteme in povečajo ognjeno moč posameznega sistema.

## 2.3 Raziskovalno vprašanje

Za preučevanje izbrane tematike sem si izbral raziskovalno vprašanje: Kakšna so načela nove doktrine omrežno-centričnega vojskovanja in kako to vpliva na vojno v Iraku in Afganistanu.

## 2.3 Metodološki pristop

Moje uporabljene metode v diplomski nalogi bodo predvsem **analiza primarnih in sekundarnih pisnih virov**, s katerimi bom lahko pregledal dogodke, ki so povezani z omrežno-centričnim bojevanjem in se vežejo na sam koncept. Z **deskriptivno metodo** bom opisal sisteme znotraj omrežno-centričnega bojevanja in predstavil vojaške programe, ki vsebujejo elemente modernega vojskovanja. Prav tako bom opisal situacije, v katerih je razvidno delovanje na omrežjih temelječega vojskovanja.

# 3 Definicija temeljnih pojmov

*Informacija*

Po definiciji so informacije podatki, ki so točni in pravočasni, imajo poseben pomen in so temu primerno organizirani, predstavljeni v kontekstu, kateremu dajejo smisel in pomen, in lahko privedejo do povečanja razumevanja in zmanjšanja negotovosti. Informacija je dragocena, saj lahko vpliva na vedenje, odločitev ali izid. Podatki se prenašajo bodisi kot vsebina sporočila ali preko posrednega ali neposrednega opazovanja neke stvari. Informacije so lahko kodirane v različne oblike za prenos in razlago. Lahko so informacije kodirane v znakih in se prenašajo preko signalov (Turk 1987). Sama beseda informacija se pogosto uporablja za sklicevanje na različne točke v okviru informacijskega spektra, od podatka pa do koristnega znanja. Kot primitivni izraz je informacija plod posameznikove zmožnosti opazovanja, ki potem pretvori podatke v nekakšen smiselni kontekst. Podatek je razumljen kot predstavitev posameznih dejstev, konceptov ali navodil na način, primeren za komunikacijo, interpretacijo ali predelavo na človeku razumljivi ravni. Če se zraven besede podatek uporabi termin obdelovan, je mišljena dodatna obdelava samega podatka.

*Preobremenjenost z informacijami*

Pri preobremenjenosti z informacijami gre za stres, ki ga povzroči sprejemanje več informacij, kot jih pa potrebujemo, da sprejmemo odločitev. Shenk izrazu informacijska preobremenjenost dodaja izraza, kot sta »informacijska zasičenost« in »podatkovni smog« (Shenk 2003, 387). Pojem se je začel uporabljat pri psihologiji. Gre za to, da je človeški um omejen na to, koliko informacij lahko sprejme v danem času. Če je subjekt izpostavljen preveliki obremenjenosti z informacijami, pozablja dele ključnih informacij ter posledično preživi in izgubi preveč, ko se skuša spomniti, kaj je pozabil. Ko pride subjekt do te mere, je njegova sposobnost, da deluje normalno, bistveno reducirana (Shenk 2003, 395–398).

*Situacijsko zavedanje*

Situacijsko zavedanje je sposobnost prepoznavanja, procesiranja in razumevanja ključnih elementov informacij o tem, kaj se dogaja v okolici. Gre za dojemanje elementov v okolju znotraj obsega časa in prostora, razumevanje njihovega pomena in projekcijo njihovega statusa v bližnji prihodnosti. Za ohranjanje situacijskega zavedanja moramo neprekinjeno črpati okolijske informacije ter povezati te informacije s predznanjem, da tvorimo mentalno sliko ter to sliko uporabimo za usmerjanje nadaljnjega zaznavanja in predvidevanja prihodnjih dogodkov (Salas in drugi 1995, 124–125). Če pride do nezavedanja in dezorentiranja v okoliškem sektorju, pride do stopnje ne sigurnosti, kar posledično poveča možnost za človeške napake. Situacijsko zavedanje je močno dinamično, težko se ohrani in enostavno ter hitro se izgubi zavedanje o tem, kaj se dogaja v okolici.

*Samostojna sinhronizacija*

Gre za izraz uporabljen v omrežno-centričnem konceptu. Izraz sinhronizacija izhaja iz grške besedne zveze (syn; skupaj in chronos; čas), kar pomeni skupni čas. Fenomen sinhronizacije se je proučeval na različnih področjih, od matematike, fizike, biologije kot tudi na področjih strojništva in elektrotehnike. Za nas najbolj pomembno je področje obrambne sfere, kjer je izraz prišel v ospredje že pred pojavom koncepta omrežno-centričnega vojskovanja. Kaufman poudarja, da je bila sinhronizacija temelj vojskovanja po vsej zgodovini, saj so bile zaradi sinhroniziranega vedenja različnih enot vojaške operacije uspešne (Kaufman 2000, 45). Izraz sinhronizacija se uporablja v različnih nacionalnih doktrinah za opis postopka usklajevanja ali dirigiranja enot na bojišču. Koncept samo-sinhronizacija je bil opredeljen s Cebrowskim in Gartsko (1998): »Samo-sinhronizacija je sposobnost dobro poučene vojaške sile za

organizacijo in sinhronizacijo kompleksne borbene dejavnosti od spodaj navzgor. Gre za doseganje ciljev organizacije, brez ali z manj voditelji kot v hierarhični organizaciji. Pri samo-sinhroniziranju gre za komunikacijo informacij, preden nastane situacija«. To predhodno znanje posamezniku omogoča samostojno delovanje in odločanje, saj ima skupno razumevanje položaja z ostalimi subjekti.

Situacijsko zavedanje je ključnega pomena za samostojno sinhronizacijo. To je razvidno iz popolnega in točnega znanja o drugih enotah, ki so prisotne na operativnem področju, ali pa iz seznanjenosti z viri in potrebami koalicijskih partnerjev z vidika morebitnih prihodnjih dogodkov. Ozaveščenost o zmogljivostih in strokovno znanje sta pomembna za maksimaliziranje učinkovitosti in uspešnosti misije. Tehnologija omrežno-centričnega vojskovanja pomaga izboljšati zavedanje o razmerah, kar posledično ustvari boljšo vizualizacijo bojnega prostora.

*Bojni prostor*

Bojni prostor (Battlespace) je izraz, ki označuje enotno vojaško strategijo z namenom integracije in združitve oboroženih sil za vojaško operacijo, ki vključujejo dimenzije, kot so zrak, informacija, kopno, morje, vesolje, in z namenom dosega vojaških ciljev. Bojni prostor zajema okolje, dejavnike in pogoje, ki jih je treba razumeti, da bi lahko uspešno uporabili bojno moč. Razumevanje le-teh je pomembno tudi za zaščito in obrambo svojih sil ali pa za dosego svojih ciljev in dokončanje dodeljene misije (Vega 2007, 4). V ta prostor so vključene naše oborožene sile, sovražnikove oborožene sile, infrastruktura, vreme, teren in elektromagnetni spekter znotraj operativnih območjih ter v območjih interesa.

*Bojno prostorska agilnost*

Bojno prostorska agilnost (Battlespace agility) se nanaša na hitrost, s katero vojaška organizacija spreminja znanje v dejanja z namenom doseči želene cilje v bojnem prostoru. Bistvo agilnosti v bojnem prostoru je, da moramo biti boljši od opozicije pri delanju pravih stvari v pravem prostoru in času. Če hočemo doseči nekaj v bojnem prostoru, se ne smemo osredotočati samo na hitrost, ampak moramo pozornost nameniti tudi izvedbi najbolj učinkovitih akcij, najbolj učinkovitemu načinu glede na željen dosežek učinka na sistem (Phister in drugi 2000). Koncept je razvil dr. William Mitchell z raziskovanjem v nadzorovanih poizkusih kot tudi z opazovanjem dejanskega bojevanja danskih sil v Afganistanu.

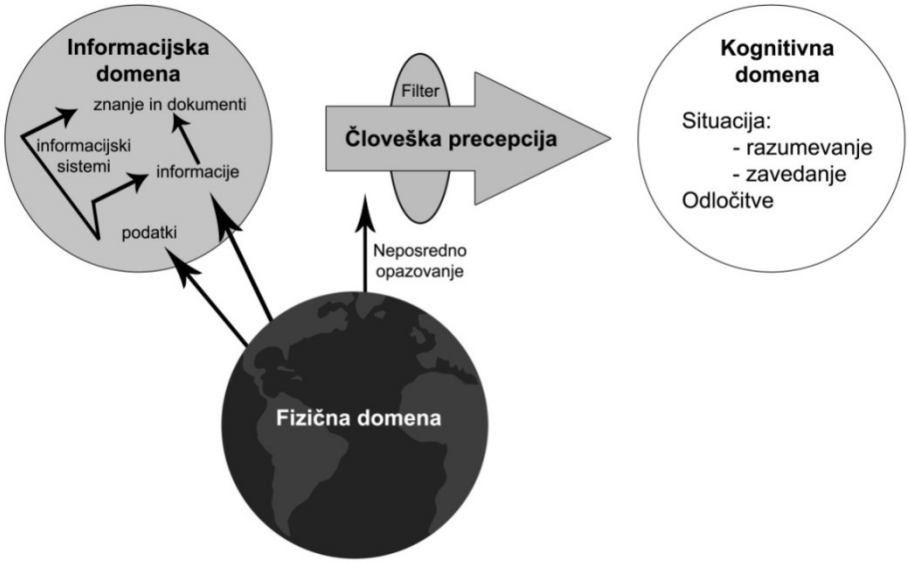
*Bojno prostorska zavednost*

Pri bojno prostorskem zavedanju gre za prakso vojaške filozofije, ki se uporablja kot koristno sredstvo, ki vključuje skupne komponente in poveljnike sil, z namenom predvidevati potek dejavnosti še pred namestitvijo vojakov na določeno območje operacij. To predvidevanje lahko dosežemo z uporabo obveščevalnih podatkov, katere ima na voljo poveljujoči in katere mu omogočajo zavedanje nedavnih, sedanjih in bližnje prihodnjih dogodkov v njegovem bojnem prostoru (Phister in drugi 2000, 8).

# 4 Domene

V tem delu bom predstavil domene, ki so osrednjega pomena za razumevanje narave in vpliva informacij, ki so temeljni kamen za razvoj omrežno-centričnega vojskovanja. Da bi razumeli, kako informacija vpliva na našo sposobnost, da lahko opravljamo vojaške operacije, moramo razmišljati o treh domenah, katerih se ta pojem tiče. Prva domena je fizična domena, druga je informacijska domena in tretja je kognitivna domena.

Slika 4.1: Domene




Vir: Albert in drugi (2001).

## 4.1 Fizična domena

Fizična domena je kraj, kjer obstaja situacija, na katero poizkuša vojska vplivati. To je domena, kjer potekajo napad, obramba in manever preko vseh vrst fizičnega okolja, na tleh, v morju, zraku in vesolju. Gre za domene, kjer prebivajo fizične platforme in komunikacijska omrežja, katera jih povezujejo. Elementi tega področja so primerjalno najlažje izmerljivi in posledično se je bojna moč tradicionalno merila predvsem na tem področju. Zato se v večini virov fizična domena označi kot realnost (Alberts in drugi 2001, 12). Pomembni merilci za merjenje bojne moči v tem področju vključujejo smrtnost in preživetje.

## 4.2 Informacijska domena

Je območje, kjer se nahajajo informacije. To je domena, kjer se ustvari informacija, se manipulira in deli z drugimi. Ta domena omogoča sporočanje informacije med bojevniki in poveljujočimi. Informacije, ki obstaja v informacijski domeni, lahko ali pa ne odražajo realnost. Za primer, senzor opazuje realni svet in nam pošilja podatke, ki obstajajo v informacijski domeni. Zato z izjemo neposrednega senzoričnega opazovanja vse informacije o svetu prihajajo skozi in so pod vplivom naše interakcije z informacijsko domeno. Preko informacijske domene nam je omogočeno komuniciranje z ostalimi (telepatija je izključena). Posledično je prav ta domena tista, katero je treba zaščiti in obraniti z namenom, da bi se omogočalo pridobiti bojno moč kot odgovor na ofenzivne akcije sovražnika. V vseh pomembnih bitkah za informacijsko premoč je prav informacijska domena tisti »ground zero« (ničelno ozemlje) (Alberts in drugi 2001, 12).

## 4.3 Kognitivna domena

Kognitivna domena se nahaja v mislih udeležencev. To je kraj, kjer se dojemanje, zaznavanje, razumevanja, prepričanja in vrednote nahajajo znotraj posameznika in kot posledica smisla se sprejemajo odločitve. V tej domeni se bitke dobivajo ali izgubljajo. To je domena nepredmetnih sredstev, kot so: vodstvo, morala, kohezija enote, raven izobrazbe in izkušnje, poznavanje razmer in javnega mnenja. V tej domeni se nahaja razumevanje poveljnikovega namena, nauki, taktike, tehnike in postopki. O tej domeni se je skozi zgodovino že veliko pisalo, vendar so ključne značilnosti tega področja sorazmeroma ostale iste še od Sun Tzujevega dela Art of war (umetnost vojne). Atributi na tem področju so zelo težko izmerljivi in vsaka pod-domena (vsak individualni um) je edinstvena in ima svoje lastnosti ter vidik za razumevanje stvari. Iz slike je razvidno, da vse vsebine kognitivne domene prihajajo skozi filter ali lečo, ki je označena kot človeško dojemanje. Ta filter je sestavljen iz

posameznikovega pogleda na svet, osebnega znanja osebe, ki ga ta oseba prinese do situacije, njegovih izkušnje, njegovih treningov, izobraževanj, vrednot ter individualne sposobnosti (inteligenca, osebni slog, sposobnosti dojemanja dogajanja, itd.). Ker je ta leča človeškega dojemanja unikatna za vsako posamezno osebo, vemo, da je posameznikovo zaznavanje (razumevanje, ipd.) prav tako edinstveno. Obstaja le ena realnost ali fizična domena. Ta se pretvori v izbrani podatek ali informacije ter služi kot znanje v sistemu znotraj informacijske domene. Zato se z usposabljanjem in skupnimi izkušnjami v vojski poizkuša kognitivne dejavnosti narediti čim bolj podobne, da bodo odločevalci imeli čim bolj iste odločitve pri zelo podobnih ali pa istih situacijah (Alberts in drugi 2001, 13). Kljub temu ostajajo individualne osebe edinstvene s svojim mišljenjem. Te razlike so bolj opazne pri posameznikih, ki prihajajo iz različnih rodov, generacij in držav.

# 5 Temelji in razvoj omrežno-centričnega vojskovanja

## 5.1 Transformacija oboroženih sil Združenih držav Amerike

Razprava o spremembah v obrabnem sektorju oboroženih sil ZDA so se začele z razpravo o informacijskem bojevanju, ki je od leta 1990 bila ena izmed najpomembnejših tem nacionalne varnosti v ZDA še posebej v okviru obrambnega oz. vojaškega podsistema. Tako so leta 1994 ustanovili šolo za informacijsko bojevanje in strategijo, z namenom usposabljanje častnikov za bojevanje v informacijskih operacijah. Prav tako so se razvijali novi koncepti, ki so temeljili na vojno v informacijski dobi. »Joint vision 2010« je usmerjevalni koncept, kateri je bil sprejeti 1996 z novim pogledom na bojevanje, ki ni temeljilo na ognjeni moči, ampak se je osredotočalo na znanje, kot obliko moči. Ker »Joint Vision 2010« ni bil dovršen novim smernicam, je leta 2000 prišlo do nadgradnje in je nastal dokument »Joint Vision 2020«. »Potreba po večji interoperabilnosti ter informacijskem pretoku znotraj ameriškega obrambnega ministrstva je bila sicer izpostavljena že v dokumentu Joint Vision 2010, ki je zagotavljal osnovo prihodnjega razvoja ter izboljšanje obveščevalnih in poveljniško-nadzornih zmogljivosti v informacijski dobi, na ta način pa poudarjal tehnološke inovacije kot sredstvo.« (Svete 2005, 128). Vse to je omogočalo interakcije znotraj ministrstva za obrambo ZDA ter izmenjavanje ključnih informacij med platformami, katere so izvajale operacije. Novi dokument Joint Vision 2020 je poudaril pomen po novih tehnološko izboljšanih sistemih, ter prav tako potrebo po interoperabilnosti v združenih in multinacionalnih silah ter operacijami, ki bi potekale med različnimi varnostnimi instrumenti, v katerih bi sodelovale oborožene sile, kot ene izmed njih. Temeljne v teh dokumentih so torej inovacije, katere pa

nebi smele biti omejene le na tehnološki vidik, ampak moramo biti pozorni še na ostala področja doktrine kot so manever, natančno delovanje, usmerjeno logistiko ter lastno zaščito. Če se zagotovijo ti pogoji, lahko govorimo o popolni prevladi na vseh področjih, kar je tudi glavna ideja Joint Vision 2020 (Svete 2005, 128-130).

## 5.2 Temelji omrežno-centričnega vojskovanja

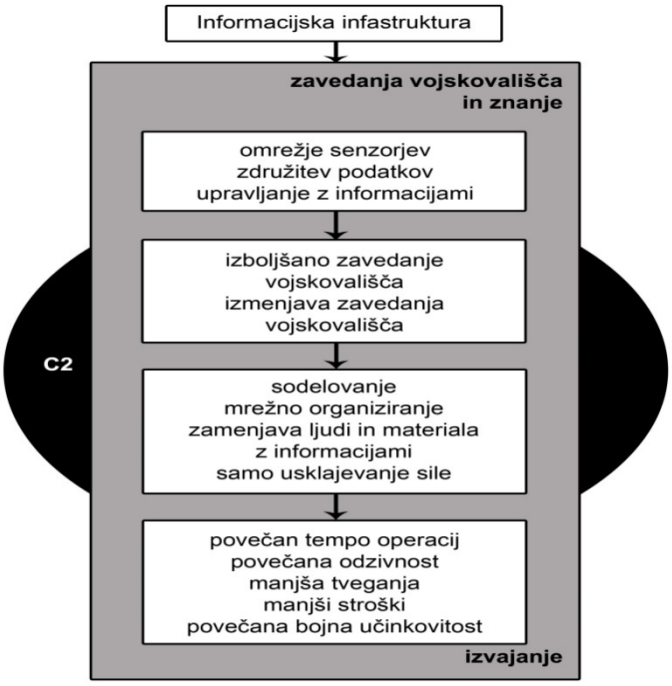
Omrežno-centrično vojskovanje je vojskovanje. Da bi razumeli, kaj je drugačnega pri omrežno-centričnem vojskovanju, se moremo hkrati osredotočiti na tri področja bojevanja ter na interakcije med njimi. Omrežno-centrično vojskovanje vključuje povezovanje vseh treh domen. V svoji popolnoma zreli obliki ima omrežno-centrično vojskovanje naslednje karakteristike:

- Fizična domena: vsi elementi sile so robustno povezani v omrežje in s tem se doseže varna povezljivost in interoperabilnost.
- Informacijska domena: elementi sile imajo sposobnost, da dostopajo, delijo in varujejo podatke do mere, da se lahko vzpostavi in vzdrži informacijska prednost nad nasprotnikom. Sila ima sposobnost za sodelovanje v informacijski domeni, s tem je omogočeno izboljšanje njenega informacijskega položaja skozi procese korelacije, fuzije in analize.
- Kognitivna domena: sila ima sposobnost, da razvije visoko kakovostno ozaveščenost in da deli z ostalimi situacijsko zavedanje. Prav tako ima sposobnost, da razvije skupno razumevanje, vključno z razumevanjem poveljnikovega namena. Prav tako lahko sila samo sinhronizira in odloča o svojih operacijah (Alberts in drugi 2001).

Sila mora biti sposobna voditi informacijske operacije po vseh teh področjih, da se doseže sinhroniziran učinek v vsaki izmed prej naštetih področjih (fizične, informacijske in kognitivne). Iz tega izhaja, da je osrednji namen omrežno-centričnega vojskovanja ta, da bo sila s temi lastnosti in zmogljivostmi imela večjo bojno moč z boljšim sinhroniziranim učinkom na bojnem prostoru, dosegala večje in hitrejše sposobnosti oddajanja in sprejemanja poveljstva ter povečanje smrtonosnosti, preživetja in odzivnosti. Do danes je razmišljanje o eksperimentiranju z omrežno-centričnim konceptom večinoma osredotočeno na taktično in operativno raven vojskovanja, vendar pa ne samo, da velja za vse ravni vojskovanja, temveč tudi za vse vrste vojaške dejavnosti, od taktične do strateške. Ko se koncept o omrežno-centričnem vojskovanju apelira na operacije drugačne od vojne, se uporablja termin omrežno-centrične operacije. Na operativni ravni omrežno-centrične operacije poveljnikom

zagotavljajo zmožnost natančnih in učinkovitih bojevniških efektov pri izjemnem operativnem tempu in s tem ustvarjanje pogojev za hitro osamitev sovražnikovih možnosti ukrepanja. Omrežno-centrični koncept dramatično izboljša sposobnost sile za hiter, učinkovit in uspešen prenos vseh svojih razpoložljivih sredstev za izpolnitev dodeljenih nalog. To izboljšano vojskovanje s svojimi zmogljivosti izhaja deloma od sile z namenom, da bi dosegla visoko stopnjo integracije čez številne dimenzije, sposobnost nadomestitve informacije namesto masovnega števila ter sposobnost, da se po bojišču premikajo informacije namesto ljudi in materiala. Omrežno-centrično vojskovanje omogoča sili, da se hitro in učinkovito prilagodi hitremu dinamičnemu okolju (Alberts in drugi 2001, 66–72).

Slika 5.1: Vojaška organizacija kot mrežna organizacija




Vir: Albert in drugi (2001).

Koncept se je razvijal v času informacijske dobe, ko je bila informacija pomembna iz večih vidikov. Hitro sprejemanje in filtriranje pomembnih informacij je bil cilj, h kateremu stremi vsaka vojska za lažje obvladovanje nasprotnika. S tem bi imeli veliko prednost, ki bi bila ključnega pomena pri izpeljavi operacije. Kaj sploh je omrežno-centrično vojskovanje? Gre

za nastajajočo teorijo vojne v informacijski dobi. Gre za koncept, ki je na najvišji ravni po odzivu vojske do bojevanja v informacijski dobi. Izraz omrežno-centrično vojskovanje splošno opisuje kombinacijo strategij, taktik, tehnik in postopkov ter organizacije, ki v celoti ali delno izrabljajo prednosti, ki jih nudi sistem, za ustvarjanje odločilne premoči pri bojevanju.

Po zalivski vojni leta 1991 so se ameriške oblasti zavedale nastale krize na vseh območjih obrambnih sil, še posebej zaradi razpada Sovjetske zveze in spoznanja, da za opravljanje prihodnjih nalog ne potrebujejo številčno tako velike vojske. Zato so iskali rešitve in to je spodbudilo sprejetje koncepta združevanja rodov. Razvoj je danes prišel do te mere, da je skupno bojevanje osnova za bojne operacije, in te smernice so sedaj prevladujoča zahteva za usmerjanje in razvoj sistemov, s katerimi se bodo izvajale prihodnje operacije, v katerih bodo sodelovale sile Združenih držav Amerike.

Sam razvoj mrežno-centričnega vojskovanja se je začel leta 1996, ko je ameriški admiral William Owens uvedel pojem »sistem sistemov« v isto imenskem delu in takrat predstavil vizijo prihodnosti, v katero bo šla vojska ZDA. V tem delu je Owens opisal razvoj sistema obveščevalnih senzorjev, sistemov poveljevanja in kontrole, natančnost orožji, ki so omogočila izboljšane situacijskega zavedanje s tem, da so hitro ocenile ciljno razdaljo. Isto leto so v kabinetu Joint Chiefs of Staff (skupno združeno poveljstvo) izdali vizijo, ki je predstavila koncept »Full-spectrum dominance« (dominacija na vseh spektrih). Pri dominaciji na vseh spektrih gre za dosežek vojaškega subjekta za nadzor nad vsemi razsežnostmi na bojevališču. Učinkovito posreduje prevladujočo raznolikost sredstev na področju kopenskega, letalskega, pomorskega, podzemeljskega, zunajzemeljskega, psihološkega, biološkega ali informacijsko tehnološkega bojevanja. Vključuje tako fizično bojevališče, kot so zrak, teren ter podvodno bojevališče, pa tudi elektromagnetski spekter in informacijski prostor. Nadzor na teh področij bi pomenil, da je svoboda nasprotnikovih sil za raziskovanje sovražnih in svojih enot, terena in drugih bistvenih elementov na področju bojevališča v celoti omejena, kar pomeni, da bi sovražnim enotam s tem onemogočili možnost za preučevanje terena in vseh njegovih kompetenc (Joint Vision 2010). Skupni učinek prevladujočega položaja v zraku, na tleh, pomorskega ter vesoljskega in informacijskega okolja omogoča izvajanje skupnih operacij brez učinkovite opozicije ali motenj.

## 5.3 Cilji in načela omrežno-centričnega vojskovanja

Doktrina omrežno-centričnega vojskovanja za oborožene sile Združenih držav Amerike črpa svoje smernice iz pojma »ekipno vojskovanje«, kar pomeni usklajevanje in povezovanje vseh ustreznih enot in zmogljivostih na področju različnih storitev, ki segajo od enot kopenske vojske, letalstva pa vse do obalne straže ZDA. To ne vključuje delovanja enot le na določenem območju operacij, temveč tudi usklajevanje razpršenih sil na globalni ravni. Glavni cilj in namen tega koncepta je, da zagotovi prihod kritične informacije do tistih, ki jo hitro potrebujejo, kakor tudi do tistih, ki so na bojišču, ali pa za osebe, ki sprejemajo odločitve. David S. Albert, bivši pomočnik sekretarja za obrambo na področju omrežja in informacijsko integracijo, navaja štiri cilje oziroma prednosti, ki jih nudi omrežno-centrični sistem:

1. robustna mrežna povezanost izboljšuje informacijsko izmenjavanje,
2. izmenjavanje informacij in sodelovanje, izboljšanje kakovosti informacij in skupno zavedanje o razmerah,
3. deljeno situacijsko zavedanje omogoča samostojno sinhronizacijo,
4. če so ti cilji zagotovljeni, se s tem dramatično poveča učinkovitost misije (Alberts in drugi 2001, 85–90).

Samo izvajanje omrežno-centričnega vojskovanja je v prvotnem namenjeno obnašanju posameznikov znotraj omrežnega sistema povezovanj. Gre za iskanje vzorca obnašanja vojakov, mornarjev in pilotov v sistemu nenehnega komuniciranja in povezovanja. S tem povezovanjem in sodelovanjem rodov lahko marinci, ki izvajajo vojaške operacije na taktični in operativni ravni vojne, pridobijo pomembno prednost pred nasprotniki, saj so del skupnega situacijskega zavedanja. Teorija o omrežno-centričnem vojskovanju se lahko uporablja (in tudi se) na vseh treh ravneh vojskovanja: strateškem, operativnem in taktičnem. Prav tako zajema celotno območje vojaških operacij; od večjih bojnih operacij z dolgoročno kampanjo do operacij za ohranjanje miru in stabilnosti (Manthorpe 1996, 305).

Obstaja vrsta principov ter načel, po katerih se ravna in razvija sama teorija omrežno-centričnega vojskovanja. Sama načela so v konstantnem razvoju in so predmet izboljšanja ter smernica omrežno-centričnega vojskovanja v nastajajoči teoriji. To pomeni, da postavljajo pravila, po katerih omrežno-centrično vojskovanje organizira, trenira, simulira in deluje. Prvo načelo je **bojevanje za informacijsko superiornost**. Pri tem načelu gre za to, da si ustvarimo informacijsko prednost s pravočasnostjo, točnost in ustreznostjo podatkov. Za prednost pred

sovražnikom nas to načelo vzpodbuja, da povečamo sovražnikovo potrebo po informacijah, ob tem je potrebno zmanjšati njegovo sposobnost za dostop do informacij in dvigniti sovražnikovo negotovost. Zagotavljati si moramo lasten dostop do informacij prek dobro omreženih in interoperabilnih sil ter si zaščititi svoje informacijske sisteme, vključno s senzorskimi sistemi. Zagotavljati si moramo zmanjšanje lastne potrebe po informacijah, predvsem v količini podatkov, s povečanjem naših sposobnosti, da izkoristimo vse naše sisteme za zbiranje informacij. Drug tak princip omrežno-centričnega vojskovanja je **skupno zavedanje**. Gre za redno prevajanje in izluščanje informacij in znanja za zagotavljanje skupnega razumevanja in poznavanja razmer v celotnem spektru udeležencev v skupnih in združenih operacijah. Za zagotavljanje tega načela se mora zgraditi kolaborativna mreža mrež, ki vsebuje kvalitetne podatke, da lahko sile v skupnih operacijah hitro in enostavno uporabijo te informacije za uspešno opravljanje misij. Tisti, ki uporabljajo informacije, morajo prav tako postati ponudniki informacij, ki so odgovorni za objavo informacij brez odlašanja. Omogočiti morajo dostop do podatkov ne glede na lokacijo, na kateri se nahajajo. Visokokakovostno skupno zavedanje zahteva varnostne protokole, ki omogočajo varovanje takšne mreže pred napadi ali vdori sovražnika v sistem. Tretje načelo je **hitrost poveljstva in odločanja**. Poveljujoči mora prepoznati informacijsko prednost in zagotoviti, da bodo prednostne informacije v najkrajšem času prišle do enote, ki potrebuje to informacijo in je ključnega pomena. S čim hitrejšim posredovanjem informacij na bojišču se naredi blokada sovražnika in ga pušča brez možnosti presenečenja in s tem omogoča prevlado zavezniških in naših sil na bojišču. Četrto je načelo **samo-sinhronizacije**. Načelo samo-sinhronizacije (samostojne sinhronizacije) nam poveča možnost, da lahko sile, ki so na nižji stopnji (to pomeni, da so lažje oboroženi in v manjšem številu), delujejo skoraj samostojno in da si po opravljeni nalogi samostojno določijo novo nalogo z izkoriščanjem informacij iz skupnega zavedanja in z namerami vodje skupine. Načelo poveča vrednost pobude podrejenih za smiselno povečanje operativnega tempa in odzivnosti. To načelo pomaga poveljujočemu pri izvedbi njegove namere z izkoriščanjem prednosti visoko izurjene, profesionalne enote in omogoča hitro prilagajanje, če pride do nenadnih sprememb na bojišču. Če pride do spremembe, ki se tiče ostalih udeležencev, morajo ostale sile informirati druge znotraj bojišča o teh dogodkih ter poskrbeti za vnaprejšnje sporočanje o namenih enot. Naslednje načelo je načelo o **razprševanju sil**. To načelo govori o premiku bojnih sil iz nelinearnega bojevališča do nestičnih operacij in s tem premik ravnotežja sil na točko predora, ki bi povzročil zlom nasprotnikovih sil. Da bi to omogočili, mora biti konstantna kontrola fizičnega bojevališča in dogajanja na njem ter nenehnega sporočanja o tem dogajanju. Ko je to omogočeno, se lahko

na bojišču prenese učinkovita bojna moč na pravem mestu ob pravem času. To nam omogoča, da delujemo konstanto na nelinearnem položaju in v razpršeni formaciji, ampak ko se pojavi priložnost in pride do povelja, se lahko v hitrem časovnem obdobju združijo sile in nastane gosta ognjena moč z večjim številom sil. S tem moramo povečati tesno spajanje obveščevalnih podatkov, operacij in logistike, za doseganje natančnih učinkov in začasnega prednostnega položaja z razpršenimi silami. 6. načelo je načelo **demasifikacije**. Premik iz pristopa, ki je zagovarjal stik več manjših enot v večje velike sile in formacije ter uporabo teh sil na manjšem geografskem območju. Če uporabimo informacije in s tem pridobimo znanje o sovražnikovi sili in njegovi nameri, se lahko z manjšo enoto zoperstavimo in dosežemo cilj v hitrejšem času, kot pa bi ga porabili za združevanje z ostalimi enotami z namenom pridobiti večjo ognjeno moč (ki bi bila potrebna, če ne bi imeli informacije o dogajanju na bojevališču). S tem se omeji poraba fizičnih sil, zmanjšata se logistika in drugi stroški premikanja. Ostale enote, ki opravljajo svoje dolžnosti, lahko nadaljujejo z opravljanjem svojih dolžnosti na svojih položajih. S tem bi se pridobilo na času in uspešnosti operacij. Manjše enote se hitreje in lažje gibajo po bojevališču, kar spet pomeni pridobitev na času in hitrosti premika sil, s čimer se sovražniku oteži ciljanje in lociranje naših enot. 7. je načelo o **globokem senzorskem dosegu**. Gre za to, da bi se razširile uporabe premostljivih, distribuiranih in mrežnih senzorjev v globoko geografsko oddaljenost z namenom odkrivanja informacij o elementih našega interesa na operacijsko pomembni razdalji, katerega cilj bi bil, da se dosežejo odločilni učinki. S tem bi se razširila in izkoristila bolj obstojna obveščevalna dejavnost, povečal bi se nadzor nad večjim območjem in se okrepilo izvidništvo globoko v notranjosti. Senzorji bi se uporabili kot manevrski element, s katerim bi si pridobili in vzdržali informacijsko premoč. Načelo stremi k temu, da se omogoči, da vsaka oborožitvena platforma postane senzor za odkrivanje informacij, pa če je to posamezni vojak ali pa tehnološko dovršeni satelit (Cebrowski 2005, 7–12). Ta načela ne nameravajo izpodrinit ostalih starejših načel ameriške vojske, kot so:

- Cilj: usmerite vsako vojaško operacijo proti jasno opredeljenim in dosegljivim ciljem. Končni vojaški namen vojne je uničevanje oboroženih sovražnih sil ter odvzeti jim voljo do boja.
- Ofenziva: pridobiti, ohraniti in izkoristi pobudo.
- Masa: preusmeriti veliko skoncentrirane ognjen sile na odločilnih krajih ob odločilnem času.
- Manever: postaviti sovražnika v slabšalni položaj s prilagodljivo uporabo bojne moči.

- Presenečenje: napasti sovražnika v času, kraju ali načinu, na katerega ni pripravljen.
- Varnost: nikoli ne dovoliti, da bi sovražnik pridobil nepričakovano prednost (Headquarters Department of the Army 1993).

# 6 Združljivost vojaških programov z omrežno-centričnim vojksovanjem in ognjena moč

## 6.1 Vojaški programi

V nadaljevanju je seznam nekaterih tehnologij in programov, ki so kompatibilni in omogočajo izvajanje omrežno-centričnega vojskovanja v vojski Združenih držav Amerike. Omrežno-centrično vojskovanje je samo koncept, kako pridobljene informacije čim bolj efektivno preoblikovati v uspešnost misije. Vendar je za zagotovitev informacij potrebno uporabiti različne senzorje za zaznavo. Ko imamo informacijo, jo preko zvez in komunikacije prinesemo do osebe ali enote, ki to informacijo potrebuje. Za to, da bi čim hitreje prava informacije prišla do pravega naslovnika, so potrebni različni sistemi in programi povezovanja v omrežja.

### 6.1.1 Link 16

Taktične podatkovne povezave (Tactical data link ali TDL) zagotavljajo sredstva za razširjanje in pošiljanje informacij, pridobljenih od sistemskih radarjev, sonarjev, elektronskega bojevanja, samo-poročanja ter vizualnega opazovanja. Vsak TDL uporablja standardno podatkovno povezavo, da se zagotovi komunikacija preko radijskih valov ali podatkovnih kablov. Ti vojaški standardi (MIL-STD) so postavili standarde za pošiljanje in sprejemanje sporočil z namenom zagotoviti interopabilnost podatkovnih zvez. Link 16 so vojaška taktična omrežja za izmenjavo podatkov, ki jih uporabljajo vojaške sile Združenih držav Amerike, še posebej letalstvo. Ta omogoča, da lahko vojaška letala kot tudi ladje in kopenske sile med sabo izmenjujejo svojo taktično sliko v realnem času. Link 16 uporablja skupne taktične informacijsko-distributivne sisteme (Joint Tactical Information Distribution System (JTIDS)) ter multifunkcijske informacijsko-distributivne sisteme (Multifunctional Information Distribution System (MIDS)). Gre za 16 frekvenčno proti moteno in visoko zmogljivo podatkovno povezavo. Link 16 vsebuje elemente Link 11 / link 11B in Link 4A / link 4C, zagotavlja veliko novih in izboljšanih zmogljivosti, vključno z glasovnim sporočanjem. Prav tako podpira tudi izmenjavo tekstovnih sporočil, podatkov, slik in nudi dva kanala digitalnega glasu (2.4 kbit/s ali 16 kbit/s) (National Research Council 2013).

### 6.1.2 Globalna informacijska mreža

Globalna informacijska mreža (Global Information Grid (GIG)) je komunikacijska infrastruktura, ki podpira sorodne sisteme znotraj ministrstva za obrambo sile ZDA. Omogoča izmenjavo informacij med vsemi vojaškimi oporišči, mobilnimi platformami ter napotenih skupin na terenu. Ministrstvo za obrambo Združenih držav Amerike je pooblastilo, da bo globalna informacijska mreža primarni tehnični okvir, ki bo podpiral bojevanje/delovanje omrežno-centričnega vojskovanja. V skladu s to direktivo so vse napredne oborožitvene platforme, senzorski sistemi ter centri poveljevanja in nadzora v končni fazi združeni in povezani med sabo preko globalne informacijske mreže. Zato se izraz sistem sistemov pogosto uporablja in nanaša na opis rezultatov tovrstnih masivnih informacijskih integracij. Zmožnost globalne informacijske mreže je tudi, da zagotavlja komunikacijske vmesnike za koalicijske sile Združenih držav Amerike, zaveznikov ter za uporabnike in sisteme, ki niso znotraj ministrstva za obrambo ZDA (National Security Agency 2012). Ključne storitve omrežne arhitekture za izvajanje zmogljivostne omrežno-centrične operacije preko sistema globalne informacijske mreže so sistemi različni zvrsti, tako na primer sistem Air Force C2 Constellation, mornariški sistem ForceNet ter sistem kopenske vojske LandWarNet (Cummings 2010).

### 6.1.3 Napredno taktično ciljna tehnologija zračnih sil

Air Force Advanced Tactical Targeting Technology (AT3) sistem združuje in kombinira informacije, ki jih v zračnem prostoru zaznavajo in prepoznavajo senzorji, da bi natančno locirali sisteme sovražnikove zračne obrambe. Sistem temelji na usklajevanju informacij iz različnih sistemov na krovu večkratnih letal. AT3 sistem ima zmožnost, da lahko zračna plovila pasivno najdejo sovražnikove zračne protisisteme z medsebojno izmenjavo podatkov preko taktičnih omrežij. Program AT3 bo pilotu in upravljavcu oborožitvenih sistemov omogočil prednost zaradi zmogljivosti zaznavanja večkratnih ciljev (Hampton 2003). Tehnike, ki so uporabljene v tem sistemu, omogočajo ločeno hkratno informiranje o posameznem sistemu sovražnikovega protizračnega orožja in s tem omogočijo, da se bo orožje usmerilo na več ciljev in povzročilo hkrati uničenje večih tarč.

### 6.1.4 Mornariška kooperativna zmogljivost

Navy Cooperative Engagement Capability (CEC) sistem povezuje mornariške ladje in zračna plovila, ki delujejo na določenem območju, in jih nato poveže v enovito zračno obrambno mrežo, v kateri radarsko pridobljeni podatki, ki so bili zbrani iz vsake platforme na območju,

posredujejo naprej drugim enotam, oziroma oborožitvenim sistemom v realnem času. Vsaka enota v CEC omrežju združi svoje lastne radarske podatke s podatki, ki jih je prejela od drugih enot. S tem pridobijo večjo sliko prostorske ozaveščenosti in dogajanja na področju. CEC omogoča ladjam, da izstrelijo zračno obrambne rakete (air-defense missiles) na bližajoče se proti ladijske rakete in to iz razdalje, kjer same nimajo virtualnega in ne fizičnega pogleda na bližajoče se izstrelke. Dejavniki te funkcije so podatki, ki so zbrani od drugih enot in v mreži tvorijo celoto ter omogočajo sliko prihajajočih izstrelkov ter jih preoblikujejo v premikajoče tarče. Prav tako lahko ladje izstrelijo svojo raketo, namenjeno za obrambo, ter obvarujejo in uničijo izstrelke namenjene drugi ladji v omrežju (O'Rourke 2005).

### 6.1.5 Army Force XXI Battle Command Brigade and Below (FBCB2)

FBCB2 se uporablja z računalniško opremo in tehnologijo modrega sledenja sil (Blue Force Tracker), ki je glavni digitalni sistem Ameriške vojske. Le-ta uporablja taktični internet za pošiljanje podatkov bitke v realnem času in vsem svojim silam na bojišču. Med operacijo v Iraku je bil ta sistem uporabljen v nekaterih bojnih vozilih Bradley in tankih M1A1 Abrams ter tako zamenjal papirnate zemljevide in rutinsko poročanje o položajih preko radijskih komunikacij kot v prvi zalivski vojni. Računalniške slike in GPS zmogljivosti so dovolile tankovskim posadkam, da so z uporabo modrega slednja sil izsledili svoje in prijateljske položaje tudi sredi Iraške peščene nevihte, podobno kot to storijo piloti letal z uporabo instrumentov za letenje v slabem vremenu (Tiboni in French 2004). Modro sledenje sil omogoča tudi uradnim osebam iz Pentagona ter tistim daleč stran od bojišča, da lahko spremljajo in nadzorujejo napredek svojih sil po bojišču.

### 6.1.6 Army WIN-T in JNN

Informacijsko omrežje Warfighter (WIN-T) je visoko zmogljivostni omrežni sistem, ki omogoča enoti in poveljniškim centrom komunikacijo med sabo, med tem ko so na premiku. Gre za nadgradnjo prejšnjega sistema Mobile Subscriber Equipment system (MSE) (General Dynamics C4 Systems). Joint Network Nodes (JNN) je most med novejšo in starejšo tehnologijo, ki je bila v uporabi med hladno vojno in ima 30 letno zapuščino MSE ter današnjega WIN-T sistema. JNN trenutno daje brigadam ter bataljonskim poveljniškim postojankam zmožnost za neposreden stik z bazami v domačih ZDA oziroma drugih globalnih lokacijah (Headquarters Department of the Army 2006). JNN zagotavlja znatno povečanje zmogljivosti do vojske modularnih enot, ki jih zagotavljajo satelitske širokopasovne komunikacije vse do bataljonske ravni.

Zgoraj omenjena tehnologija se osredotoča na hitrostno širjenje informacije in s tem omogoča povečanje bojne moči in prednost ozaveščanja in sodelovanja med posameznimi silami. Zagotavlja komunikacijo, ki je bistvo sporazumevanja med enotami na bojišču ter poveljniškimi centri, katerim posreduje podatke v čim hitrejšem času, in s tem daje možnost hitrejšega reagiranja na nastale situacije. Informacije, poslane od teh sistemov in tehnologij, so le podlaga za samostojno sinhronizacijo, kjer usklajevanje le-teh koristi. Posledica je, da imajo enote skupne miselne modele ter večjo usklajenost in učinkovitost.

## 6.2 Ognjena moč doktrine omrežno-centričnega vojskovanja

Da bi lahko preveril, če nova doktrina vojskovanja z novo tehnologijo doprinaša večjo ali manjšo ognjeno moč, bom primerjal ognjeno moč podobnega oborožitvenega sistem iz prve iraške vojne leta 1990 ter oborožitveni sistem iz druge iraške vojne leta 2003. Za primerjavo sem si izbral Havbice model M109A2, ki je bil uporabljen v prvi vojni, ter model M109A6 »Paladin« iz vojne leta 2003. Za izračun ognjene moči bom uporabil formulo: *teoretična hitrost streljanja za posamezno orožje v minuti x masa naboja za posamezno orožje v kilogramih = ognjena moč.* S tem bom dobil količino, koliko kilogramov svinca lahko sistem izstreli v eni minuti. Havbica modela M109 je ameriška 155 mm havbica na lasten pogon, prvič predstavljena v začetku leta 1960. Zaradi analize se bom osredotočil le na karakteristike, ki me zanimajo za izračun ognjene moči.

*M109A2*

Posadka havbice modela M109A2 sestavlja 6 članov (za izračun bom za njihovo primarno oborožitev uporabil jurišno puško M16A1): poveljujoči vozila, voznik, strelec, pomočnik strelca ter dva vojaka namenja za rokovanje s strelivom. Strelec ima nalogo, da cilja top po horizontali levo in desno, medtem ko pomočnik strelca po vertikali gor in dol. Za izračun potrebujem maksimalno hitrost streljana ter posamično orožje posadke in njeno maksimalno hitrost. Primarna oborožitev havbice je 155 mm top, njeno sekundarno orožje pa je mitraljez M2 kalibra 12.7×99 mm, efektivni domet havbice je 18.000 metrov (Headquarters Department of the Army 2003; Military analysis network 2000).

Tabela 6.1: Ognjena moč posadke havbice M109A2

| naziv sredstva | št. sredstev | št. max. izstrelkov na minuto | št. izstrelkov/min | masa izstrelka (v kg) | masa v kg/min |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 155 mm top | 1 | 4 | 4 | 44,5 | 178 |
| M2 mitraljez | 1 | 550 | 550 | 0,045 | 24,75 |
| jurišna puška M16A1 | 6 | 950 | 5700 | 0,004 | 22,8 |
| ognjena moč | 8 | | 6245 | | 226 |

Vir: Headquarters Department of the Army (2003); Military analysis network (2000).

*M109A6 Paladin*

Artilerijski sistem Paladin opravlja posadka 4 članov (za primarno oborožitev posadke bom uporabil jurišno puško M16A3): poveljnik, voznik, strelec ter rokovalec s strelivom. Sposobnost Paladina je, da lahko deluje brez zunanje tehnične pomoči, posadka sprejme poslanstvo preko varnega glasovnega in digitalnega komunikacijskega sistem, računalniški sistemi izračunajo podatke za ognjeno delovanje, samodejno odklepajo topove med premikom, imajo možnost delovanja »shoot and move« (streli in premakni), kar pomeni večjo zaščito posadke pred sovražnikovim povratnim ognjem. Primarna oborožitev še vedno ostaja 155 mm top, vendar se je hitrost streljanja povečala. Top deluje z avtomatskim sistemom za nadzor ognja z balističnim računalnikom, opremljenim z optično rezervo. Sekundarna oborožitev ostaja mitraljez M2, efektivni domet havbice je 24.000 m (Headquarters Department of the Army 2003; Army-technology 2014). Paladin se je prvič uporabil kot podporno orožje v operaciji Iraška svoboda, marca leta 2003.

Tabela 6.2: Ognjena moč posadke havbice M109A6 Paladin

| naziv sredstva | št. sredstev | št. max izstrelkov na minutov | št. izstrelkov/min | masa izstrelka (v kg) | masa v kg/min |
|---|---|---|---|---|---|
| 155 mm top | 1 | 8 | 8 | 44,5 | 356 |
| M2 mitraljez | 1 | 550 | 550 | 0,045 | 24,75 |
| jurišna puška M16A3 | 4 | 900 | 3600 | 0,004 | 14,4 |
| ognjena moč | 6 | | 4158 | | 395 |

Vir: Headquarters Department of the Army (2003); Army-technology (2014).

Iz primerjave lahko vidimo, da se je v 13 letih proti istemu sovražniku ognjena moč povečala za več kot 60 %. Med tem se je število živih sil za upravljanje z istim oborožitvenim sistemom zmanjšalo iz 6 na 4 članov posadke. Če dodamo še povečan domet izstrelka iz Paladinove havbice, nov način komuniciranja in širjenja informacije, je očitno, da se nova tehnologija navezuje na avtomatizacijo sistemov in povezanosti, ki omogoča hitrejše streljanje in samostojno delovanje sistema.

## 7 Praktična uporaba omrežno-centričnega vojskovanja in izzivi v prihodnje

Iz same teorije je razvidno, da ta doktrina prinaša nove načine izvajanja vojskovanja na področju oboroženih sil Združenih držav Amerike. Če so v drugi svetovni vojni bili v osredje postavljeni tanki in njihova sposobnost, je zdaj področje bojevanja usmerjeno na hitrost zbiranja, analize in predstavljanja podatkov; strojna in programska komponenta informacijsko-komunikacijske tehnologije (posebno »umetne inteligence«) ter stopnja njihove integracije v različnih mrežah strateškega, operativnega in taktičnega interneta. Od začetka ideje pa do praktične uporabe so ameriške sile posredovale v dveh vojnah in tako preizkusile ideje doktrine v vojni z Afganistanom ter Irakom. Po tej teoriji je informacijska superiornost ter mrežna povezanost enot bolj pomembna od številčnosti sile. Omrežno-centrično vojskovanje omogoča, da se potreba po rezervah ali okrepitvah zmanjšuje in v prihodnje ne bo potrebna. Prav tako se bo logistična podpora kalibrirala in zmanjšala do te mere, da se bodo potrebščine dostavljale točno takrat, ko bo to potrebno. Tehnologija se obravnava ne kot pomoč pri bojevanju, ampak kot ključni del bojevanja, vse ostalo se smatra kot podrejeno sistemu (Vega 2007, 175–185).

V prvi zalivski vojni, ko še koncept omrežno-centričnega vojskovanja ni bil razvit, so bile zavezniške sile 1,5 krat številčnejše od armade Iraške vojske. Torej bi to pomenilo, da bi v vojni v Iraku leta 2003, kjer je vojska štela okrog 400,000 vojakov, morale zavezniške sile posredovati s silo, ki bi štela okrog 600,000 vojakov. Na koncu je v začetni fazi operacije sodelovalo le 30,000 enot (v končni fazi pa več kot 150,000) in je bilo razmerje sil 1,57:1 v korist branilca. Navkljub tako neugodnemu številčnemu razmerju sil so zavezniške sile uspele v dvajsetih dneh prodreti do središča Bagdada in razbiti iraško glavnino kopenske vojske, vključno z enotami Revolucionarne garde (Svete in Žabkar 2006). Kar je pozitiven kazalnik, ki nakazuje na to, da lahko s koriščenjem informacij in močnim povezovanjem sil z manjšimi enotami premagamo številčnejšega nasprotnika.

*Scenarij delovanje omrežno-centričnega vojskovanja*

Za primerjavo bi podal scenarij, ki omogoča ciljanje na velike razdalje, kar ponazarja potrebo po skupnih mrežnih operacijah ter poudarja kompleksnost za tehnične potrebe v uspešnosti te misije.

Satelitski posnetki nam prikažejo povečano aktivnost v bazi teroristične celice, ki je oddaljena od 40 kilometrov do zavezniškega ozemlja. Satelitski posnetki so preko programa morske informacijske strukture (NCII) predstavljeni mornariškem bojnemu poveljniku, ki se odloči, da bo spremljal dogajanje. Če pride do sovražne aktivnosti, bo tudi posredoval. Tako se uporabi sistem JSTARS (Joint Surveillance and Target Attack Radar System), ki zbira nadaljnje informacije ter določa natančno zemljepisno dolžino, širino in višino fiksnih ciljev v teroristični bazi. Podatki se vpišejo v avtomatiziran sistem načrtovanja, katerega uporablja poveljnik, in se pripravi vse potrebno za zračno misijo F-18, ki je oborožen JSOW-GPS raketami. Po petih dneh zračnega opazovanja indikator premičnih tarč (MTI), radar na JSTAR, zaznava bistveno premikanje na območju teroristične baze. Slike iz Global Hawk UAVja potrjujejo, da gre za gibanje terorističnih sil in da ne gre za signale zaradi dejavnosti komercialnega prometa. Podatki iz JSTAR in Global Hawka so takoj predloženi poveljniku bojne skupine, ki se odloči za odreditev napada na teroristične baze in vozila. Medtem se na letalonosilki F-18 naložijo rakete na letalo in vpišejo koordinate GPS za odobrene cilje v teroristični bazi. Med poletom F-18 se zagotovi točnost GPS podatkov, ker bi sovražniki lahko imeli tehnologijo za motenje delovanja. Ko so JSOW rakete izstreljene in potujejo proti cilju, pride do ugotovitve, da se njeni inercialni navigacijski sistem (INS) ter GPS koordinate razlikujejo v več kot dovoljenih mejah zaradi učinkov motenja. INS prevzame nadzor in je programiran, da vodi izstreljene rakete do željnega cilja in uniči tarče v teroristični bazi. Ker so teroristična vozila v premiku, ne morejo biti usmerjena z GPS orožjem. Specialne sile se zaradi predhodnega opozorila vkrcajo v helikopterski transport in so odložene na sovražnikovo ozemlje z namenom laserskega markiranja vozila, ki je namenjen iz teroristične baze. Poveljujoče se odloči, da se napade vsako premikajoče vozilo z Maverick raketami iz F-18. F-18 leti v sovražno območje in izstreli AGM-65C rakete, ki nato sledijo do lasersko dodeljene tarče (National Research Council 2000, 60–61).

Tehnični elementi predstavljeni v tem scenariju, ki so ključni do uspeha, so:

- satelitska obveščevalna,
- natančna lokalizacija ciljev z dodajanjem podatkov iz JSTAR radarjev,

- natančna lokalizacija F-18 z GPS sistemom ter prenos podatkov do raket,
- samo-lokalizacija JSOW projektila z uporabo INS sistema, ko je GPS bil onemogočen,
- MTI radar za identifikacijo premikanja,
- validacija podob potencialnih premičnih ciljev z uporabo UAV,
- ter najbolj pomembne so bile instantne informacije o dogajanjih, ki jih je prejel poveljnik bojne skupine preko NCII.

Čeprav je to šolski scenariji, nam pokaže, v kakšni obliki so sistemi povezani in kako omogočajo hitro reakcijo na spremembe, ki jih zaznajo senzorji. Prav tako prikaže pomembnost satelitske slike, ki je pomemben segment za uspešno operativno rabo omrežno-centričnega vojskovanja. S pomočjo mreže senzorjev in platform so GPS pametna orožja primerna za fiksne, nepremične tarče.

*Praktična uporaba tehnologije*

Naslednji primeri pa prikazujejo, kako se uporaba omrežno-centričnega vojskovanja vidi z vidika praktičnih primerov na bojiščih Iraka in Afganistana. Eden izmed takšnih primerov je bližnja podpora iz zraka (close air support). To je omogočilo vojaku specialnih sil, da iz svojega prenosnega računalnika zahteva posredovanje B-52 bombniku, ki je z bombami tipa Joint Direct Attack Munition (JDAM) lahko uničil celotno množico talibanskih ali iraških sil v roku 20 min. Specialne sile so na terenu uporabljale daljnoglede, opremljene laserskimi daljinomeri za določitev tarčne točne lokacije, in v takojšnem času poslale natančne koordinate bombniku, ki je letel nad njimi. Ko je bombnik pridobil podatke, jih je takoj programiral v rakete JDAM, ki so bile le minuto po prejetju podatkov sprožene in zadele tarče. Ta sposobnost omrežja je omogočala sposobnost manevriranja v realnem času. Obseg senzorjev od vojaka do letalonosilke in posadke letala je dajal vso potrebno znanje o nasprotniku in prijateljskih silah, da so lahko letala nudila natančno in hitro ognjeno podporo koalicijskim enotam. Zato je v veliko primerih prišel sovražnik pod ognjeno močo, ki ni izhajala iz oklepnih enot ali številčne masivne sile, ampak od peščice vojakov, ki so prenašali podatke letalu. Misije z uporabo UAV-ije za dolge razdalje so omogočale strateško izvidovanje in nadzor. Letenje na višinah do 60,000 metrov z veliko hitrostjo ter nudenje stalno pokritih širokih območji, so ključni elementi Global Hawka, ki nudi dodatne informacije, pridobljene iz satelitskih posnetkov ali pa podatkov, pridobljenih od drugih zračnih plovil. S svojim sintetično podprtim radarjem, elektro-optičnimi kamerami ter infrardečimi in drugimi senzorji je Global Hawk nudil dodatno oko na bojišču ter zavzemal

tisoče slik za ocenjevanje bombnih napadov, nudenje ognjene pomoči ter slike za izvidovanje (Houghton 2004). Iz mrežnega vidika je Global Hawk pokazal dve edinstveni zmogljivosti. 1. je bil nadzorovan prek komunikacijskega omrežja, kjer je upravitelj več 1000 kilometrov oddaljen od bojevališča (ali v Evropi ali pa v Kaliforniji). 2. pa ni letel samo po vnaprej določeni poti letenja, ampak se je prilagodil uporabam za ostale misije. Global Hawk še vedno nadzoruje meje Iraka in Afganistana ter zagotavlja tesnejše spremljanje območjih, ko druga sredstva opozarjajo na sumljiva dogajanja. Med tem ko Global Hawk posreduje slike in nadzira območja, ima nižje leteči Predator večjo vlogo pri manevriranju sil. Radarji ter IR sistemi znotraj Predatorja omogočajo, da lahko spremlja in pošilja slike tako v slabem vremenu kot tudi ponoči. Njegova video sposobnost mu omogoča snemanje in pošiljanje posnetkov drugim letalom, poveljniškim centrom ter taktičnim kontrolorjem na kopnem. Te lastnosti so se izkazale za neprecenljive v izvidovanju in manevriranju sil, ki so v bojnem delovanju s premikajočim sovražnikom. Marca 2002 so specialne sile v operaciji Anaconda v Afganistanu bile neposredno povezane s Predatorjem, ki so ga uporabili za ugotavljanje morebitnih sovražnikovih lokacij, kar jim je nakazovalo, če je bila pot naprej varna za napredovanje (Luddy in Fellow 2005). Tako so se lahko sile premikale hitreje, kot če bi bilo to potrebno raziskovat po tradicionalni metodi z uporabo izvidniških sil za odkrivanje groženj na svoji poti.

## 7.1 Izzivi omrežno-centričnega vojskovanja

Čeprav so uspehi in znaki potenciala omrežno-centričnega vojskovanja vidni v vojni na bližnjem vzhodu, so še vedno slepe točke in vrzeli v zmogljivosti in napake, ki se pojavljajo v obliki neodkritih in zgrešenih tarč, civilne in kolateralne škode ter streljanje na zavezniške enote in lastne sile (freindly fire). Izpostavil bi tri področja, kjer se ti problemi najbolj zavedajoči in ki vplivajo na sam potek operacij. 1 področje je področje človeškega nadzora v omrežno-centričnih operacijah. 2. področje se dotika prevelike odvisnosti od tehnologije in 3. uporabe sistemov omrežno-centričnega vojskovanja z ostalimi zavezniškimi silami Združenih držav Amerike.

*Človeški nadzor v sistemu avtomatiziranega omrežno-centričnega vojskovanja*

Premik od platfatformno-centričnega vojskovanja do vojskovanja, temelječega na omrežjih, predstavlja premik v vlogi človeka, tako pri načrtovanju misije kot tudi pri dejanskem

delovanju. Kot je razvidno že od razvoja visoko tehnoloških avtomatiziranih sistemov raket in letal, imajo vojaški operaterji čim manj neposrednega ročnega krmiljena sistemov ter so postavljeni v višjo raven planiranja ter odločanja. Gre za proces človeškega komuniciranja z računalnikom, kjer človek prejema povratne informacije in zagotavlja ukaze nadzorovane naloge, ki je priključena na sistemski del računalnika. Medtem ko je avtomatizacija pomemben aspekt za hitro menjavo informacij, pa se lahko zaplete pri odkrivanju tistih informacij, ki so ključne in sploh pomembne za posamezno operacijo. Avtomatiziran sistem ne bo mogel sam izpeljati naloge, če bo prišlo do nenadne spremembe na operacijski shemi. To pomeni, da če se prepusti vse sistemu, da postori sam, lahko pride do izgube situacijskega zavedanja in neustrezne povratne informacije, kar lahko ogrozi misijo (Parasuraman in Riley 1997). Iz Afganistana prihajajo poročila, da posamezne enote, ki so uporabljale robotizirane sisteme brez posadke, niso našle zaupanja v robotih, pa čeprav je sistem dokazal, da deluje in da je sposoben zagotovit prave informacije. V nasprotju pa lahko pride do obratne zmešnjave, kadar pilot zaupa avtomatizaciji preveč ali kadar sistem ne deluje pravilno. Kadar piloti čutijo časovno stisko in so v situaciji z visokimi vložki in negotovostjo, se lahko odločijo zaupati avtomatiziranemu sistemu v preveliki meri in namesto, da bi uporabili svoje zavedanje, se odločijo, da bo računalnik opravil zadeve po svoje. To lahko privede do škode celotne misije (Skitka 2000). Omrežno-centrične operacije povečujejo število razpoložljivih virov informacij, hitrejši operacijski tempo, kar za seštevek daje večji stres za kognitivno domeno operaterja. Sprejeta načela omrežno-centričnega vojskovanja so problematična za tiste, ki bodo odločali in izvajali nadzor ter kontrolo preko kompleksa porazdeljenih omrežnih sistemov z visoko stopnjo negotovosti. Omrežno-centrične operacije dodajajo število informacij kot tudi hitrejši pretok informacij. Zato mora napredek te doktrine stremeti k temu, da omeji ta pretok in da ne bo prihajalo do preobremenjenosti z informaciji. Da bi lahko upravljali s povečanjem informacij preko omrežja, bi bila potrebna večja stopnja avtomatizacije, kar pa posledično spet uvede dodatne probleme človeške zmogljivosti.

*Odvisnost od GPS tehnologije*

Oborožene sile se močno nanašajo na tehnologijo, še posebej na infrastrukturo, ki jim omogoča omrežno-centrično vojskovanje. Obstajajo pa različni razlogi, zakaj prav zanašanje na tehnologijo prinaša visoka tveganja. Kakršna koli prevelika odvisnost vojske od tehnologije lahko postane »primarno težišče«, katerega bo nasprotnik hotel izkoristiti, kar je še posebej nevarno, če sistem nima alternativnega drugega načina. Če bo omrežno-centrično vojskovanje postalo tako ključnega pomena za vojskovanje v silah ZDA, da se vojaki ne bodo

znašli v okolju brez omrežno-centričnega modela, bi to lahko imelo katastrofalne posledice in bi potencialno lahko onesposobilo vojsko. Sovražniki se že zdaj prilagajalo in izkoriščajo napake v sistemu ter izkoriščajo že znane slabosti. Eden takih primerov so GPS jammerji (motilci GPS). Poveljnik ameriških zračnih sil vesoljskega poveljstva je ugotovil, da so ameriške sile v zelo veliki meri odvisne od vesolja in da je GPS temelj za vojaške operacije. GPS je tudi osnova za večino delovanja znotraj sistema omrežno-centričnega vojskovanja. V zadnjih letih so zato motilci GPS za blokiranje signalov postali cenejši in posledično razširjeni v veliki meri prav z namenom oslabiti sisteme, temelječe na GPS (Robb 2014). Z uničenjem GPS v določenem območju delovanja bi se prav tako uničili sistemi za natančno usmerjene izstrelke. Iz tega vidika je izguba GPS signala velik problem v ameriški vojski in podobno bi se zgodilo tudi z velikimi silami drugih držav, ki uporabljajo sisteme GPS. Še posebej bi bil problem škodljiv za tiste sile, ki se opirajo na omrežno-centrične navigacijske sisteme. Zato mora Ameriška vojska razvijati alternativne sisteme bojevanja v območju, ki ne dovoljujejo omrežno-centrične povezanosti. Prav tako se morajo sile še vedno uriti v situacijah brez omrežne povezanosti, da bi, ko bi prišlo do takih situacij, vedele, kako odreagirati in se prilagoditi. Do zdaj so le pripadniki specialnih sil tisti, ki so še vedno vešči v vseh oblikah bojevanja, ampak če se bo trend motilcev GPS povečal, bi se podobno urjenje moralo prenesti še na ostale pripadnike oboroženih sil.

*Omrežno-centrična povezanost z ostalimi koalicijskimi silami*

Ameriška vojska je s svojimi izdatki edina na svetu, ki lahko do popolnosti izvaja omrežno-centrične operacije. Sistem in prehod na ta način bojevanja je bil v veliko državah pod vprašanjem, še posebej glede njegove učinkovitosti. Ravno zato nobena vojska ni hotela tvegati takšne nadgradnje, ne da bi videla, kaj lahko prinaša ta način bojevanja in če je sploh uspešen. ZDA so glede stroškov, namenjenih za obrambo, vodilna sila na svetu, ki je leta 2004 zapravila 466 bilijonov, na drugem mestu je Kitajska s 65 bilijoni stroškov in Rusija s 50 bilijoni (podatki so za leto 2004) (Mitchell 2006, 63–66). Ameriška vojska je po koncu hladne vojne v vojni z Irakom in Afganistanom v glavnem delovala z zavezniškimi silami. Tukaj se pojavi slabost, kajti zavezniške sile, ki ne morejo učinkovito komunicirati, imajo napačne situacijske informacije in druge podatke, kar je slabo za delovanje celotne zavezniške sile. Za primer je delovanje med Američani ter Kanado in Avstralijo, ki so širjenje informacij med ZDA ocenili kot zadovoljivo, saj jim je bilo zadosti, da so lahko opravili svoje operacije.

Vendar so obstajali primeri, kadar podatki niso bili ujemajoči. Tako je prišlo do incidenta, ko bi Avstralske in Kanadske sile skoraj uničile specialne enot Navy SEAL, ker so bili zaradi neobveščenosti in slabega komuniciranja in zmešnjave ne sigurni, ali gre za prijateljske sile ali pa za nasprotno tarčo. Šele koordinacija preko radija je lahko razrešila ta problem, ker omrežno-centrično povezovanje z ZDA ni bilo učinkovito (Mitchell 2006, 53–60). Zato sile ZDA pritiskajo na ostale sile, da preidejo na omrežni način vojskovanja. Evropske države in NATO so zato izdelale podoben princip imenovan Network Enable Operations (NEO). Ta sistem še ni povsem dovršen in tudi razlika v tehnologiji je prevelika (vrzel med tehnologijo ZDA in ostalimi je nekje 10 let in še več), da bi lahko oba sistema delovala v popolnosti. Sodelovanje z zavezniki spet onemogoča prosto širjenje informacij, še posebej tistih, ki so »občutljive« z vidika obveščevalne, prav tako informacije »skrite misije«, ki se navezujejo na delovanje specialnih sil.

To so le nekateri izzivi, ki se pojavljajo v zvezi z omrežno-centričnim vojskovanjem. Iz teh izzivov izhajajo problemi, ki so usmerjeni k napakam in neuspehom na vojaško-operativnem področju. V vojni v Afganistanu in Iraku so se pokazali problemi, kot so ubijanje nedolžnih žrtev, ponavadi civilistov, ki so bili zaradi napačnih informacij ali napak v sistemu označeni kot tarče. Seveda se sovražnik prilagaja in zato je tudi način bojevanje oblikovan tako, da čim v večji meri zmede sisteme in tako povzroča žrtve na civilnih straneh, kar posledično vpliva na rekrutiranje več ekstremno islamističnih ljudi in tako na neuspeh kampanje v boju proti terorizmu. Problematičen je tudi problem prijateljskega ognja, katerega bi povezave in pretok informacij morali omejit ali celo onemogočiti. Kljub temu še vedno prihaja do spopada ali bombardiranja lastnih sil (včasih je za to kriva tehnologija, ampak v večini primerov nepravilnost v informiranju).

# 8 Zaključek

V svoji diplomski sem s predstavitvijo teoretičnega dela predstavil koncept doktrine omrežno-centričnega vojskovanja in kako pomembna je informacija v moderni dobi vojskovanja ter kako se informacija iz fizičnega sveta pretvori v informacijo v informacijski domeni ter kako to osebe razumevajo v kognitivni domeni. Ameriška vojska s svojo transformacijo sledi načelom novodobnega vojskovanja, ki temeljijo na principih na omrežju temelječega vojskovanja. Nekateri avtorji trdijo, da gre pri tem za revolucijo na področju vojskovanja (Lonsdale 2005, 4). Pritrdilno temu je, da so v dveh vojnah, v katerih so sodelovale ZDA s svojo novo doktrino vojskovanja, prišli do izjemnih uspehov. Kot odgovor na moje

raziskovalno vprašanje sem naštel nova načela; bojevanje za informacijsko superiornost, skupno zavedanje, hitrost poveljstva in odločanja, samo-sinhronizacija, razprševanje sil, demasifikacija, globoko senzorski doseg**.** Seštevek vseh načel lahko vidimo kot rezultat operacij in delovanja ter uspehov v vojni z Irakom in Afganistanom. Rezultat je bila hitra, učinkovita in uspešna kampanja v prvi fazi vojne. Po teh načelih ni več linearnega bojevanja po določenih frontah, ampak prihaja do razprševanja sil, ki se v ključnih trenutkih združijo in tvorijo zgoščeno ognjeno moč. To je možno zaradi tehnologije, ki omogoča mreženje sistemov, posledično prihaja do situacijskega zavedanja ter nato do samo-sinhronizacije. Tako lahko nova načela primerjam s kampanjo v prvi iraški vojni iz leta 1990 in pa zadnjo kampanjo za osvoboditev Iraka 2003. Prednosti se vidijo na večkratnih področij. Od hitrejše kampanje do dosega boljših rezultatov proti številčnejšemu nasprotniku in to na nasprotnikovem ozemlju.

Svojo hipotezo: novi vojaški programi oboroženih sil Združenih držav Amerike, ki podpirajo omrežno-centrično vojskovanje, nadgrajujejo sisteme in povečajo ognjeno moč posameznega sistema, lahko v celoti sprejmem. Iz primerjave havbice M109A2 ter havbice M109A6 »Paladin«, ki sta sodelovali v vojni proti iraškim silam, le da s 13 letno razliko, je razvidno, da se ne le ognjena moč poveča, pač pa se tudi število operaterjev sistema zmanjšuje, kar je posledica avtomatizacije in robotizacije, kateri se prek programskih sistemov, kot so Link 16 ali globalne informacijske strukture, povezujejo in pošiljajo informacije o sovražnikovih enotah v realnem času ter tako uspešno dobivajo ciljne koordinate tarč in možnost hitrega posredovanja. Prav tako se poveča bojna moč, kar je omogočilo številčno manjšim silam, da so lahko prodrle obrambo številčno močnejšega iraškega sovražnika.

Kljub uspešni ofenzivni kampanji je še veliko napak, ki jih sistem pušča odprte. Tako kot vsak na novo predstavljen način delovanja ima tudi ta v začetnih fazah slabosti, ki se šele v praktični uporabi lahko odkrijejo. Tudi obe vojni nista bili hitro zaključeni in še vedno trajajo spopadi, pa tudi normalizacija razmer še ni vzpostavljena. Izpostavil sem le nekatere temeljne napake na treh področjih, ki bi z odpravljanjem omogočile sistemu boljše delovanje ter zmanjšanje napak. Nelinearno bojevanje omogoča sovražniku napad na boke, če nimamo podpornega kritja teh delov. Če bi se Iraške sile bolj aktivno vključevale v spopad, bi na tem segmentu imele oborožene sile ZDA resne težave. Kljub manjšemu številu sil, ki so posledično lahko hitreje prišle na bojišče kot večje sile ter hitro posredovala v spopadih, ki bi na daljši rok eskalirali in bi bila potrebna večja številčnost vojakov, je to bilo možno zaradi tega, ker so bile sile Iraka in Talibanov močno pasivne in nekompetentne. Če bo res prišlo do

revoluciji ali le evolucije na vojaškem področju, bomo videli čez določeno periodo časa, ko bo prišlo do spopada med dvema tehnološko približno enako razvitima nasprotnikoma. Vizija omrežno-centričnega vojskovanja je preveč fokusirana na informacijo ter tehnologijo. Informacije igrajo pomembno in včasih tudi ključno vlogo pri odločanju ter posledično dobivanju vojn. Vendar uspeh vojne ni samo zaradi informacijske dominacije, pomembni so še tudi drugi faktorji. Še posebej človeški dejavnik, ki bo tudi v prihodnjih vojnah imel ključno vlogo pri zmagah. Za enkrat so edino ZDA s svojim finančni primatom nad izdatki za obrambna sredstva zmožna dokončno razviti tak sistem delovanja.

# 9 Literatura


1. Alberts, S. David, Jonh J. Gartska in Richard E. Hayes. 2001. *Understanding information age warfare*. Washington: CCRP Publication Series. Dostopno prek: www.dodccrp.org/files/Alberts_UIAW.pdf (25. avgust 2014).
2. --- 2014. *Army-technology*. Dostopno prek: http://www.army-technology.com/projects/paladin/ (28. avgust 2014).
3. Cebrowski, K. Arthur. 2005. *The Implementation of Network-Centric Warfare*. Washington: Department of Defense. Dostopno prek: http://www.carlisle.army.mil/DIME/documents/oft_implementation_ncw%5B1%5D.pdf (25. avgust 2014).
4. Cebrowski, K. Arthur in John J. Gartska. 1998. Network-Centric Warfare: Its Origin and Future. *Proceedings Magazine* 124 (1–1). Dostopno prek: http://mattcegelske.com/wp-content/uploads/2012/04/ncw_origin_future.pdf (25. avgust 2014).
5. Cummings, L. Mary. 2010. Human Supervisory Control Challenges in Network-Centric Operations. *Human Factors and Ergonomic* 6 (34). Dostopno prek: http://web.mit.edu/aeroastro/labs/halab/papers/Cummings_UVS.pdf (25. avgust 2014).
6. --- 2014. *General dynamics c4 systems*. Dostopno prek: http://www.gdc4s.com/warfighter-information-network-tactical-(win-t).html (25. avgust 2014).
7. Hampton, Stephens. 2003. *USAF Will Begin Air-Defense Targeting Demonstration In FY-04*. Dostopno prek: http://www.idga.org/iowa-robot/document.html?topic=196&document=30568 (25. avgust 2014).
8. Headquarters Department of the Army. 1993. *Field Manual 100–5: Operations*. Dostopno prek: http://www.bits.de/NRANEU/others/amd-us-archive/fm100-5(93).pdf (25. avgust 2014).

9. --- 2003. *Field Manual FM 3-22.9 Rifle Marksmanship M16A1, M16A2-3, M16A4, and M4 Carbine*. Dostopno prek: https://archive.org/details/milmanual-fm-3-22.9-rifle-marksmanship-m16a1-m16a2-3-m16a4-and-m4-carb (28. avgust 2014).
10. --- 2006. *Field Manual 6-02: Tactics, Techniques, and Procedures (TTPs) for the Joint Network Node-Network (JNN-N).* Dostopno prek: http://fas.org/irp/doddir/army/fmi6-02-60.pdf (25. avgust 2014).
11. Houghton, Peter. 2004. *Potential System Vulnerabilities of a Network Enabled Force*. Dostopno prek: http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/131.pdf (25. avgust 2014).
12. --- 1995. *Joint Vision 2010*. Washington: Joint Chiefs of Staff. Dostopno prek: http://www.dtic.mil/jv2010/jv2010.pdf (25. avgust 2014).
13. Lonsdale, J. David. 2005. *The nature of war in the information age, Clausewitzian Future.* London: F. Cass.
14. Luddy, John in Adjunct Fellow. 2005. *The challenge and promise of network-centric warfare*. Arlington: Lexington Institute. Dostopno prek: http://www.lexingtoninstitute.org/wp-content/uploads/challenge-promise-network-centric-warfare.pdf (25. avgust 2014).
15. Manthorpe, H. J. William Jr. 1996. The Emerging Joint System of Systems: A Systems Engineering Challenge and Opportunity for APL. J*ohn Hopkins Apl Technical digest* 17 (3): 305–313.
16. --- 2000. *Military analysis network.* Dostopno prek: http://fas.org/man/dod-101/sys/land/m109.htm (28. avgust 2014).
17. Mitchell, T. Paul. 2006. *Network centric warfare, Coalition operations in the age of US military primacy*. London: Routledge.
18. --- 2012. *National Security Agency*. Dostopno prek: http://www.nsa.gov/ia/programs/global_information_grid/index.shtml (25. avgust 2014).
19. National Research Council. 2000. *Network-centric naval forces: a transition strategy for enhancing operational capabilities.* Dostopno prek: http://www.nap.edu/openbook.php?record_id=9864&page=R1 (25. avgust 2014).
20. --- 2013. *Northrop Grunman: Understanding voice and data link Networking*. Dostopno prek: http://www.northropgrumman.com/Capabilities/DataLinkProcessingAndManagement/Documents/Understanding_Voice+Data_Link_Networking.pdf (25. avgust 2014).

21. O'Rourke, Ronald. 2005. *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress*. Dostopno prek: http://www.history.navy.mil/library/online/navy_ network.htm (25. avgust 2014).
22. Parasuraman, Raja in Victor Riley. 1997. Humans and Automation: Use, Misuse, Disuse, Abuse. *Human Factors* 39 (2): 230–253.
23. Phister, Paul, Timothy Busch in Igor G. Plonisch. 2004. *Joint Synthetic Battlespace: Cornderstone for Predictive Battlespace Awareness*. Dostopno prek: www.dodccrp.org/events/8th_ICCRTS/pdf/005.pdf (25. avgust 2014).
24. Robb, Jonjo. 2014. *Modern Militaries and a Network Centric Warfare Approach*. Dostopno prek: http://www.e-ir.info/2014/01/09/modern-militaries-and-a-network-centric-warfare-approach/#_ftn19 (25. avgust 2014).
25. Salas, Eduardo, Carolyn Prince in David P. Baker. 1995. Situation awareness in team performance implications for measurement and training. *Human factors* 37 (1): 123–136.
26. Shenk, David. 2003. *Information overload. Encyclopedia of international media and communications*. (2). Dostopno prek: http://davidshenk.com/webimages/ Encyclopedia.PDF (25. avgust 2014).
27. Skitka, J. Linda. 2000. Automation Bias and Errors: Are Crews Better Than Individuals? *The International jurnal of aviation psychology* 10 (1): 85–97.
28. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: Hermina Krajnc.
29. --- in Anton Žabkar. 2006. Irak – poligon za preizkušanje novih vojaških doktrin. *Teorija in praksa* 43 (1–2): 285-302.
30. Tiboni, Frank in Matthew French. 2004. Blue Force Tracking Gains Ground. *Federal Computer Week* 18 (7): 49–55.
31. Turk, Ivan. 1987. *Pojmovnik poslovne informatik.* Ljubljana: Društvo ekonomistov poslovne informatike.
32. Vega, N. Milan. 2007. *Joint operational warfare: theory and practice*. Newport: Naval War College.