Sluttrapport for prosjekt 898 NbF Beslutningsstøtte

Ole-Erik Hedenstad, Anders Eggen, Rolf Rasmussen, Hilde Hafnor og Tommy Gagnes

Forsvarets forskningsinstitutt/Norwegian Defence Research Establishment (FFI)

2. februar 2007

FFI-rapport 2007/00163

898

ISBN 978-82-464-1111-8

Emneord

Nettverksbasert forsvar (NbF)

Tjenesteorientert arkitektur (SOA)

Web Services

Eksperimentering

Informasjonsdeling

Informasjonssikkerhet

Godkjent av

Ole-Erik Hedenstad	Prosjektleder
Vidar S Andersen	Avdelingssjef

Sammendrag

Dette dokumentet gir en oversikt over arbeidet, inklusive resultater og anbefalinger fra FFI-prosjekt 898 *NbF Beslutningsstøtte*. Rapporten er bevisst holdt på et oversiktsnivå og peker på de dokumentene som går mer i dybden på de ulike tema. Prosjektets teknologiske resultater og anbefalinger blir oppsummert i åtte punkter:

- En tjenesteorientert arkitektur (Service-Oriented Architecture - SOA) anbefales fordi dette muliggjør fleksibilitet, hurtighet og dynamisk organisering av kapabiliteter og tjenester.
- Tjenester i Forsvarets informasjonsinfrastruktur (INI) bør som en hovedregel utvikles ved hjelp av Web Services-teknologi. Web Services og XML er teknologier som kan brukes for å realisere en tjenesteorientert arkitektur.
- Etablering av Communities of Interest (COIs) er identifisert som en av kjernefaktorene som ligger til grunn for realiseringen av en nettsentrisk datavisjon. COIs er et organiserings-prinsipp, en samarbeidskonstruksjon, som fremmer økt samarbeid og deling av informasjon mellom mennesker gjennom INI.
- Prosjektet har pekt på at bruk av ”Enterprise Metadata” er en forutsetning for å få realisert økt fleksibilitet i tilgangen til, og gjenfinning av informasjon på tvers i organisasjonen. Ideen er at brukere må ”tagge” (merke) sine dataressurser med informasjon om dataressursen (metadata) for å muliggjøre oppdaging og gjenfinning av ressursene.
- Det er gjort en overordnet vurdering av Semantic Web Services og ulike initiativer som konkurrerer om å bli en akseptert standard. Vesentlig arbeid gjenstår før det blir klart hvordan dette teknologiområdet best kan utnyttes i Forsvaret og når verktøyene vil være modne nok, men utsiktene for denne typen løsninger er svært lovende.
- I prosjektets eksperiment ved Coalition Warrior Interoperability Demonstration 2006 (CWID06) ble det vist at det er mulig å innføre generiske sikkerhetsløsninger i Web Services uavhengig av applikasjonene. Det anbefales at Forsvaret vurderer hvordan ende-til-ende sikkerhetsløsninger kan tas i bruk operativt.
- For å sikre levering av viktig tidskritisk informasjon, er det viktig å etablere en INI med gode gjennomgående mekanismer for å håndtere tjenestekvalitet. Prosjektet har vurdert alternative løsninger for hvordan tjenestekvalitet kan håndteres på mellomvarenivå.
- For å gjøre det mulig å bruke SOA tjenester over nettverk med begrenset datarate, har prosjektet vurdert teknikker for å redusere overhead i XML og Web Services. Ulike alternativer er vurdert, bl.a. komprimering av XML-data og bruk av taktiske profiler i Meldingstjenesten i Forsvaret som bærer.

Prosjektet har gjennomført flere eksperimenter med praktisk utprøving av ulike løsninger for å underbygge resultater og anbefalinger. Fire eksperimenter er gjennomført i samarbeid med eksterne parter i Forsvaret: ”Blue Game 2004”, ”Integrasjon av ressursregister med NORCCIS-II”, ”Battle Griffin 2005” og ”Secure SOA supporting NEC” (SecSOA) ved CWID 06. Videre har prosjektet deltatt i internasjonale aktiviteter og flere internasjonale publikasjoner er utgitt. Prosjektet har også bidratt inn i ulike overordnede prosesser og dokumentutarbeidelser i Forsvaret, bl.a. støtte til utarbeidelse av fremskaffelsesløsninger.

English summary

This document describes the work performed by FFI project 898 *NbF Beslutningsstøtte* (Decision Support), including results and recommendations. The report is a summary and points to those documents that give more in-depth descriptions of the various themes. The technological results and recommendations of the project are summarised in eight points:

- A Service-Oriented Architecture (SOA) is recommended as it enables flexibility, agility and dynamic organisation of capabilities and services.
- As a principal rule the services of the Norwegian Defence's information infrastructure (INI) should be developed by means of Web Services technology. Web Services and XML are technologies that can be used to realise a Service-Oriented Architecture.
- The establishment of Communities of Interest (COIs) is identified as one of the main factors for realising the net-centric vision. A COI is an organisation principle, a collaboration structure, which promotes increased collaboration and information sharing between people through the information infrastructure.
- The use of "Enterprise Metadata" is identified as a prerequisite for realising increased flexibility in access to, and retrieval of information across organisational boundaries. The idea is that users must tag their data resources with information about the data resource (metadata) in order to enable discovery and retrieval of the resources.
- An assessment of Semantic Web Services and the various initiatives that compete in becoming an accepted standard has been performed. Substantial work remains before it can be concluded how the Norwegian Defence can utilise this technology and when the tools will be mature enough. However, the prospect of this type of technology is promising.
- In the experiment conducted by the project at the Coalition Warrior Interoperability Demonstration 2006 (CWID 06) it was shown that introduction of generic security solutions independent of the applications is possible. It is recommended that the Norwegian Defence consider adoption of end-to-end security solutions.
- In order to secure delivery of time critical information it is important that mechanisms for Quality-of-Service handling are established at all levels. The project has assessed alternative solutions for how to handle Quality-of-Service at the middleware level.
- In order to enable use of SOA services above Disadvantaged Grids some techniques to reduce overhead in XML and Web Services have been assessed. Among the alternatives assessed are compression of XML data and use of tactical profiles of the Military Messaging Service as bearers.

The project has conducted several experiments in order to support the results and recommendations. Four experiments have been conducted in cooperation with other Norwegian Defence institutions: "Blue Game 2004", "Integration of the Resource Registry with NORCCIS-II", "Battle Griffin 2005" and "Secure SOA supporting NEC" (SecSOA) at CWID 06. Further, the project has participated in international activities and several international publications have been issued.

Innhold

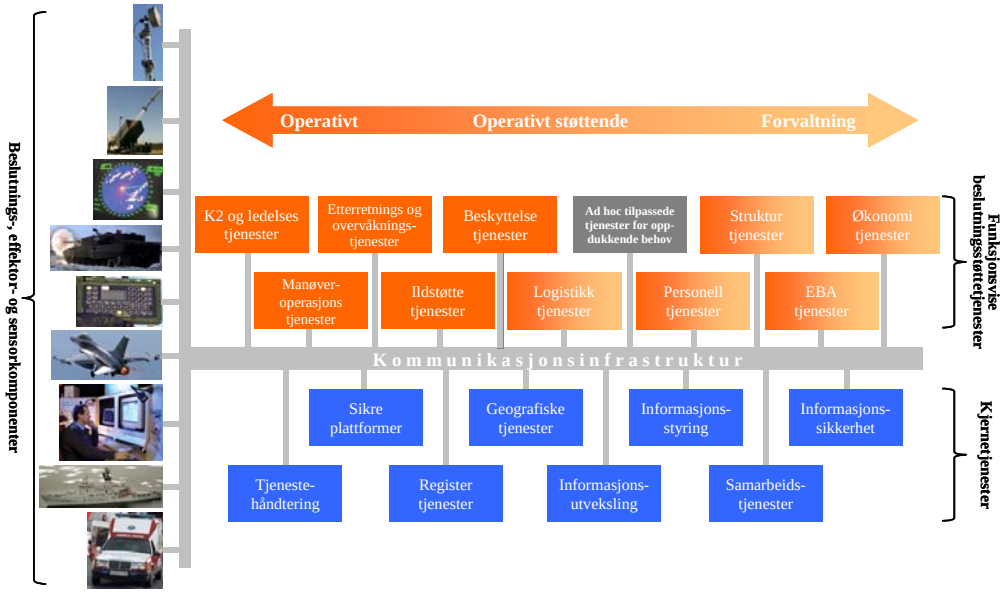
1 Innledning

Dette dokumentet gir en oversikt over arbeidet, inklusive resultater og anbefalinger fra FFI-prosjekt 898 *NbF Beslutningsstøtte*. Prosjektet har vart i tre år fra januar 2004 til og med desember 2006 og det finnes en rekke dokumenter som er utarbeidet underveis i prosjektet. Hensikten med denne rapporten er således ikke å beskrive prosjektets arbeid i detalj, men heller å gi en oversikt over hva prosjektet har utrettet og peke på de dokumentene som går mer i dybden på de ulike tema.

I dag har Forsvarets informasjonsinfrastruktur (INI) en lav grad av å være en nettsentrisk omgivelse fordi man har relativt få ressurser som er tilgjengeliggjort gjennom nettverket. Likefullt opererer Forsvaret med en fremtidsvisjon for INI som er nettsentrisk. Kort sammenfattet er denne visjonen å:

- Fasilitere (sømløs) tilgang til og deling av tjenester og ressurser.
- Muliggjøre flere typer arbeidsprosesser (planlagte og uforutsette) på tvers av organisatoriske skillelinjer, brukerkontekster, kommandonivåer og forsvarsgrener samt at kunnskap skal ivaretas og kunne gjenbrukes.

I prosjektet har vi i hovedsak arbeidet med teknologiske problemstillinger og undersøkt hvilke egenskaper og tjenester INI bør ha for å muliggjøre denne visjonen, samt hvordan vår nåværende infrastruktur best kan migreres i den retningen. Prosjektets arbeidsområde har vært funksjonsvise beslutningsstøttetjenester og i enda større grad kjernetjenester, se Forsvarsdepartementets referansemodell for INI i Figur 1.1. I dette dokumentet benyttes *tjenesteinfrastruktur* som en samlebetegnelse på funksjonsvise beslutningsstøttetjenester og kjernetjenester.



Figur 1.1 FDs referansemodell for INI

Kort oppsummert har prosjektet sett på grunnleggende elementer i tjenesteinfrastrukturen i et fremtidig nettverksbasert forsvar (NbF) og undersøkt hvilke muligheter ny teknologi gir. Videre er dette anvendt på informasjonstilgang og -deling i omgivelser som krever fleksibel organisering av informasjonsflyt. En viktig ramme for arbeidet var at tjenesteinfrastrukturen i størst mulig grad skal baseres på hyllevare (Commercial Off The Shelf - COTS) teknologier og åpne standarder.

Resultatmål for prosjektet er formulert innenfor tre områder:

A. *Grunnleggende elementer i tjenesteinfrastrukturen.* Målet var å gi råd og anbefalinger om hvordan kommende COTS teknologier og åpne standarder kan brukes for å bygge en tjenesteinfrastruktur som dekker militære behov. Prosjektet hadde også som målsetting å bistå Forsvaret i å utarbeide en nettsentrisk strategi for bruk av *metadata* for publisering av informasjonsressurser i tjenesteinfrastrukturen.
B. *Informasjonstilgang og -deling.* Målet var å undersøke hvilke egenskaper og tjenester en fremtidig tjenesteinfrastruktur bør ha for å understøtte en fleksibel tilgang til og deling av informasjon, og ut fra dette formulere krav til fremtidig funksjonalitet i INI. Dette gjelder både krav til informasjonsdeling (distribuert bildeoppbygging) og krav til behovstilpasset tilgang til informasjon. Et annet viktig mål var å utrede krav til samspillet med underliggende kommunikasjonssystemer, inklusive løsninger for bruk av mellomvare over taktiske nett. Arbeidet ble understøttet både av teoretiske studier og eksperimentering med ulike løsninger.
C. *Sikkerhet og neste generasjons meldingstjeneste.* Målet var å ta frem sikkerhetsløsninger som kan integreres i mellomvare, samt delta i NATOs arbeider med neste generasjons militære meldingstjeneste og relaterte distribusjonsmekanismer som Instant Messaging.

I mai 2005 ble det foretatt en endring i prosjektet ved at et delprosjekt i NbF Grid, ett av de andre prosjektene innenfor NbF programmet ved FFI Avdeling Ledelsessystemer, ble flyttet til NbF Beslutningsstøtte. Dette ble gjort for å samle miljøene ved avdelingen som arbeider med mellomvare. Dessuten var det en fordel at utvikling av sikkerhetsløsninger og gjennomføring av eksperimenter med sikkerhetsfunksjonalitet kunne skje som en integrert del av et bredere sammensatt miljø.

Med dette som bakteppe er rapporten bygget opp som følger. Prosjektets teknologiske resultater og anbefalinger oppsummeres i seksjon 2. Prosjektet har gjennomført flere eksperimenter med praktisk utprøving av ulike løsninger for å underbygge disse resultatene og anbefalingene. En gjennomgang av disse eksperimentene finnes i seksjon 3. Videre gis det en oversikt over prosjektets deltagelse i internasjonale aktiviteter og internasjonale publikasjoner i henholdsvis seksjon 4 og 5. Til slutt gis en gjennomgang av andre bidrag fra prosjektet, blant annet støtte til utarbeidelse av fremskaffelsesløsninger.

2 Teknologiske resultater og anbefalinger

Kapitlet oppsummerer teknologiske resultater og anbefalinger fra prosjektet.

2.1 Tjenesteorientert INI

En tjenesteorientert informasjonsinfrastruktur (INI), det vil si en INI hvor tjenesteinfrastukturdelen er realisert som en tjenesteorientert arkitektur, muliggjør fleksibilitet, hurtighet og dynamisk organisering av kapabiliteter og tjenester. Den tillater at informasjonsressurser tilgjengeliggjøres som tjenester som brukere kan aksessere direkte gjennom nettverket. I FFI-rapporten [1] som ble utarbeidet i forbindelse med 'P9268 – Variantbegrensing av Operative Beslutningsstøttetjenester', beskrev prosjektet en konseptuell løsning for operative beslutningsstøttetjenester både på kort sikt (målbilde 2008) og lang sikt (målbilde 2014). En tjenesteorientert arkitektur anbefales for begge målbildene. I tillegg kan nevnes at dette er en anbefaling som er i tråd med NATO Network Enabled Capability Feasibility Study (NNEC FS), se [2]. I resten av dette avsnittet begrunnes vår anbefaling, samt at det gis en kort beskrivelse av hva en tjenesteorientert arkitektur er.

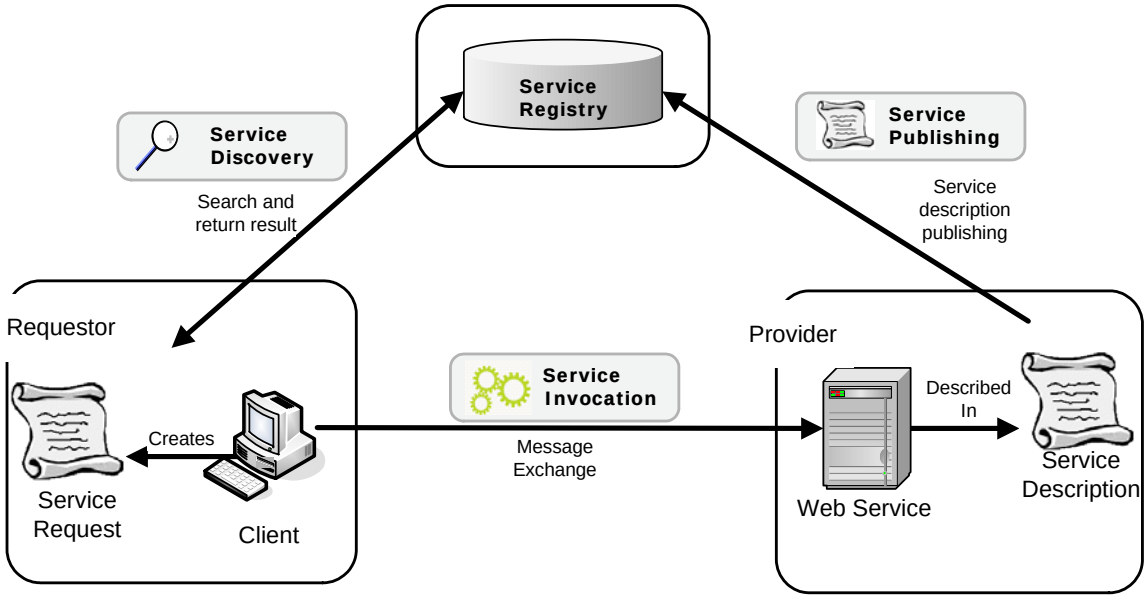
Forsvaret har behov for en løsning for operative beslutningsstøttetjenester som understøtter alliansetilpassede styrker. Støtte skal gis i forhold til det situasjonen krever, noe som kan være vanskelig å forutse. En fremtidig løsning må speile organisasjonens behov og ønske om organisk tilpasningsdyktige strukturer. Nye kapasiteter (eksempelvis sensorer) må kunne plugges inn, og interoperabilitet med logistikk- og støttevirksomhet vil også bli stadig viktigere. Vi står dermed overfor en transformasjon av dagens løsninger, slik at informasjon (både strukturert og ustrukturert) kan deles mellom langt flere enheter enn i dag, og også på tvers i organisasjonen.

Forsvaret trenger en virksomhetsarkitektur som ivaretar disse behovene. I tillegg bør systemet støtte endring i virksomhetsprosesser på en enkel måte. Et arkitekturparadigme som er ment å skulle forenkle slike utfordringer er tjenesteorientert arkitektur. Basert på behovene vi ser Forsvaret vil få i fremtiden, samt retningen på teknologi og forskning, anbefaler vi at Forsvarets operative løsning bør gå i retning av en tjenesteorientert arkitektur basert på åpne standarder. En tjenesteorientert arkitektur basert på åpne standarder gjør oss best mulig rustet for stadig endring i samarbeidspartnere og operasjoner, og dermed krav til systemet.

Tjenesteorientert arkitektur er det norske begrepet for det som på engelsk kalles for Service-Oriented Architecture (SOA). En SOA er en arkitektur som består av en samling løst koblede tjenester, som igjen er en samling av funksjonalitet. Tjenester kan sammenlignes med komponenter, da disse også er basert på et klart definert grensesnitt, samt en datamodell for informasjonsutveksling. I tillegg kan tjenester utføres over et nettverk, noe som muliggjør distribusjon. Tjenester kan konfigureres sammen, slik at systemet utfører den ønskede funksjonalitet til enhver tid, basert på de virksomhetsprosesser som systemet skal støtte. Det er viktig at tjenester er basert på åpne standarder, slik at interoperabel kommunikasjon kan oppnås

til tross for forskjellige maskinvareplattformer, operativsystem og programmeringsspråk.

SOA er illustrert i Figur 2.1. Tjenestetilbydere publiserer sine tjenester i et tjenesteregister. Tjenestebrukere kan finne aktuelle tjenester ved å slå opp i tjenesteregisteret, og dersom brukeren finner en passende tjeneste vil denne tjenesten kunne tas i bruk (service invocation). Se for øvrig [3] for en mer utførlig beskrivelse av SOA.



Figur 2.1 Service-Oriented Architecture

2.2 Web Services

Web Services og XML er teknologier som kan brukes for å realisere en tjenesteorientert arkitektur (SOA). Fordelen med bruk av Web Services er at det er en standardisert, interoperabel mekanisme for å transportere XML-meldinger. Basisen for Web Services består av åpne standarder, og er også plattformuavhengig på samme måte som XML. Vi anbefaler at tjenester i INI som en hovedregel utvikles ved hjelp av Web Services-teknologi. Dette er utdypet i [1].

XML-basert teknologi og semantisk teknologi vil trolig bli viktig i fremtiden. Dette er avhengig av en felles datamodell som informasjonselementene trekkes ut fra. XML og Web Services ligger an til å bli den mest populære måten å få til kommunikasjon mellom forskjellige systemer på. Leverandører av utviklingsverktøy, mellomvareprodukter og konsulentfirmaer har omfavnet SOA som et arkitekturprinsipp, og spesielt er det SOA realisert med Web Services og XML som er gjenstand for mye oppmerksomhet. Videre vil en rekke viktige teknologier som utfyller basisteknologiene i Web Services bli tilgjengelige i perioden frem mot 2008. Det er også et poeng at forskning på teknologier innen SOA og semantisk interoperabilitet bygger videre på XML og Web Services, slik at dette vil utgjøre et godt fundament å bygge en dynamisk INI på. Mer om forskning på semantiske teknologier i 2.5.

For transport av XML er basisstandarden i Web Services, SOAP, forholdsvis moden. Det finnes videre et mangfold av såkalte WS-* spesifikasjoner. Disse er utvidelser av basisstandardene, og på noen områder finnes flere initiativer. For å beskrive tjenester benyttes i dag standarden Web Services Description Language (WSDL). WSDL beskriver grensesnittet og meldingene som en tjeneste leverer, men ikke hva den leverer. I tillegg kan Universal Description, Discovery & Integration (UDDI) benyttes som et tjenesteregister for å muliggjøre oppdagelse av tjenester (”service discovery”). UDDI kan benyttes både i design-time (som et tjenesteregister for utviklere) og i run-time (dynamisk binding til instanser av en tjeneste). Et UDDI-register er ikke en nødvendig bestanddel i en SOA, men kan gi større robusthet, siden erstatningstjenester kan finnes. Alle disse standardene er i benyttet i demonstratoren som ble utviklet for SecSOA-eksperimentet ved CWID 2006 (se seksjon 3.4).

Vi har vi identifisert noen mangler ved UDDI-standarden. Selv om flere UDDI-registre kan koples sammen for å gi et distribuert register, så er det fortsatt en sentralisert arkitektur for tjenesteoppdagelse (”service discovery”). En desentralisert tjenesteoppdagelse, kjent fra “peer-to-peer” systemer og andre, vil ofte være mer egnet i dynamiske omgivelser [4].

Det er en del utfordringer knyttet til bruk av Web Services der man har begrensninger i terminaler eller i kommunikasjonssystemene (såkalte Disadvantaged Grids). Mulige begrensninger kan eksempelvis være datarate, prosessering, batterikapasitet, monolittiske terminalløsninger, tidskrav og trafikkmengde. Disse begrensningene kan føre til et skille mellom der systemene kan benytte XML og Web Services, og der disse teknologiene ikke kan benyttes. Se avsnitt 2.8 for en oppsummering av prosjektets arbeid på dette området.

2.3 Communities of Interest (COIs)

Communities of Interest (COIs) er et organiseringsprinsipp, en samarbeidskonstruksjon, som fremmer økt samarbeid og deling av informasjon mellom mennesker gjennom INI (nettbasert samarbeid). Det kan også betraktes som et informasjonsstyringsprinsipp for å håndtere enormt store mengder av data i en mer kompleks IKT-verden. Prosjektet har identifisert etablering av COIs som en av kjernefaktorene som ligger til grunn for realiseringen av en nettsentrisk datavisjon, se [5].

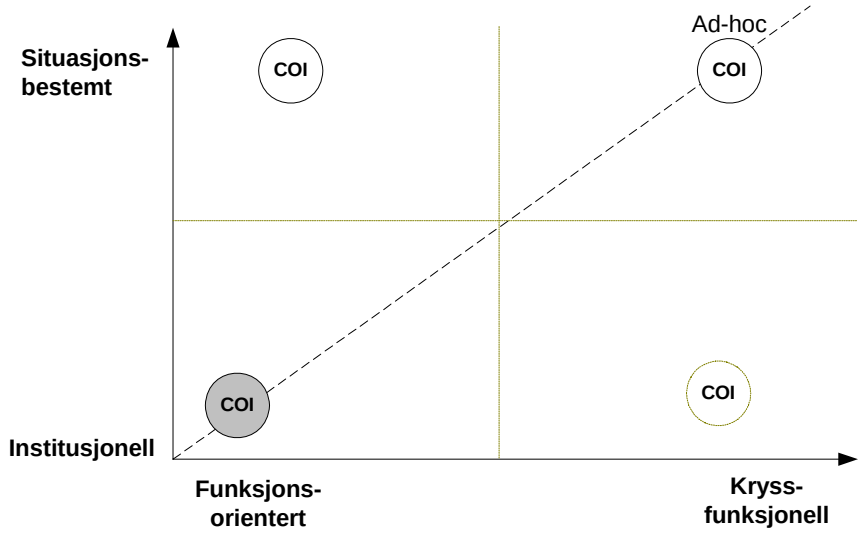
Begrepet COI dukker opp i forbindelse med litteratur som omhandler bruk av metadata i en militær kontekst. I denne konteksten brukes begrepet som følger:
En COI er en hvilken som helst samarbeidende gruppe av brukere som har behov for å utveksle og dele informasjon i arbeid som har felles mål, interesser, oppgaver eller oppdrag og som derfor må ha et felles språk (vokabular) for informasjonen som utveksles.

Det er ingen begrensninger eller regler for dannelser av COIs. Enhver gruppe av brukere som har behov for å utveksle informasjon kan betraktes som en COI. Det være seg innenfor spesifikke fagområder, fagmilitære domener eller på tvers av disse. Eller det kan være innenfor eller mellom

kampgrupper/enheter, innsatsgrupper, prosjekter eller arbeidsgrupper[1].

I en COI deler man informasjon både internt (mellom COI-medlemmene) og eksternt (mellom COIs). Eksempler på COIs i vår sammenheng kan være grupper innenfor situasjonsbildebygging som har behov for å samarbeide, ISAF[2] (deling av informasjon mellom nasjoner), kommando- og kontroll (K2) eller i forbindelse med ikke-operative virksomhetsprosesser av ulike typer (f.eks. stab/støtte funksjoner).

COIs kan fremvise en rekke karakteristikker avhengig av interessefellesskapets mål eller oppgaver og oppdrag. I Figur 2.2 nedenfor illustreres de mest alminnelige COI-typene, som gjennom begrepene situasjonsbestemt, institusjonell, funksjonsorientert, kryssfunksjonell [6] brukes for å karakterisere COIs.



Figur 2.2 En COI kan være institusjonell (fast) eller dannes mer spontant (ad hoc)

En situasjonsbestemt COI er behovsdrevet og vil typisk utnytte eksisterende ressurser i nettverket produsert og synliggjort for hele organisasjonen for gjenfinning og gjenbruk. Dette gjelder ressurser som inkluderer vokabularer, applikasjoner og andre informasjonsressurser. Eksempel på en situasjonsbestemt COI vil kunne være en ”Joint Task Force” som bruker dataressurser tilgjengelig gjennom nettverket for å generere ny etterretning og planleggingsscenarier. Eller en COI som opprettes i forbindelse med et spesifikt oppdrag. For at en situasjonsbestemt COI skal kunne dannes og være ”operativ” relativt raskt (f.eks. i forbindelse med et oppdrag) forutsettes det at det allerede er etablert COIs som tilbyr informasjonsressurser.

Institusjonelle COIs er de ”tradisjonelle” COIs som er mer ”faste” og varige enn de situasjonsbestemte og krever mer tid på å bygge seg opp. Denne type COIs har typisk ansvar for utvikling av vokabularer for å kunne tilrettelegge for felles forståelse av begreper brukt innenfor

[1] Det betyr ikke at alle prosjekter og arbeidsgrupper nødvendigvis defineres som COIs.
[2] International Security Assistance Force

fellesskapet. Det vil også være denne type COI som har ansvar for å utvikle logiske datamodeller, registrere COI-spesifikke metadata for sin COI i metadataskjemaer samt identifisere eller utvikle andre relevante datarelaterte ressurser. Systemutviklere og andre teknologiske ekspertiser vil naturlig ha større representasjon i medlemsmassen til denne type COI enn til andre og mer "flyktige" COIs. Disse vil i samarbeid med de andre COI-medlemmene ha ansvar for å utvikle COI-relaterte ressurser. Institusjonelle COIs kan betraktes som en mekanisme for, eller som et organisatorisk grep for, å institusjonalisere samarbeid på i organisasjonen. Eksempel på en institusjonell COI kan være innenfor et allerede etablert sentralt militært funksjonsområde som f.eks. etterretning og overvåking eller logistikk.

Ved å styre organisasjonen i en nettsentrisk retning tillater det oss (på sikt) å gå utover institusjonelle og "statiske" COI-dannelser til å legge til rette for mer dynamiske COI-dannelser på kryss og tvers (ad-hoc). Denne dynamikken forutsetter imidlertid at man klarer å oppnå semantisk interoperabilitet.

2.4 Bruk av "Enterprise metadata" for "Discovery"

I tillegg til at man bør bruke en tjenesteorientert arkitektur basert på åpne standarder (Web Services og XML), har prosjektet pekt på at bruk av "Enterprise Metadata" er en forutsetning for å få realisert økt fleksibilitet i tilgangen til, og gjenfinning av informasjon på tvers. Ideen er at brukere (og applikasjoner)[3] må "tagge" (merke) sine dataressurser med informasjon om dataressursen (metadata) for å muliggjøre oppdaging og gjenfinning av ressursene ("Discovery"). Videre må brukere poste alle sine dataressurser til såkalte delte informasjonsrom ("shared spaces") slik at de kan bli tilgjengelig gjennom hele organisasjonen. Dette er en type brukeratferd som må stimuleres gjennom bruk av insentivstrukturer (belønningssystemer), trening og utdanning i nettsentrisk datapraksis.

Det er i hovedsak to hovedkategorier av metadata: 1) Strukturelle og relasjonelle metadata, og 2) det som vi her har valgt å kalle for "nettsentriske" metadata. På dette nivået er det viktigst å forstå den prinsipielle hovedforskjellen mellom disse to typene.

De strukturelle og relasjonelle metadataene definerer datastrukturer og relasjoner mellom data (f.eks. datamodeller) for å støtte utviklingen av databaser og applikasjoner. Dette gjøres typisk av systemutviklere (eksperter). Disse metadataene er helt nødvendig for å kunne utvikle teknologiske løsninger som bygger opp under en nettsentrisk datastrategi.

"Nettsentriske" metadata benyttes til å publisere dataressurser og viktige attributter og aspekter knyttet til disse i nettverket, slik at ressursene blir tilgjengelige for alle i nettverket. Dette gjøres typisk av vanlige brukere innenfor et interessefellesskap (en COI - Communities of Interest). Det er denne type metadata som sørger for at de andre potensielle brukerne av ressursene ikke trenger å ha fullstendig med forhåndskunnskaper om ressursens eksistens eller karakteristikker for å oppdage den. Det er også disse metadataene som danner grunnlaget for at vanlige brukere skal

[3] "Brukere" i denne konteksten er både mennesker og applikasjoner.

kunne gjøre søk og gjøre ”enterprise discovery” av informasjonsressurser på tvers av ekspertdomener og virksomheter. Dette er metadata som blir kalt for ”Enterprise metadata”. Bruk av ”Enterprise Metadata” er mer utførlig behandlet i [5].

For å imøtekomme dagens problemer med tilgang til og gjenfinning av informasjon, trenger vi også en strategi for å håndtere dette bedre i fremtiden. Dette kalles en nettsentrisk datastrategi og representerer et paradigmeskifte fra “prosessorientering” til “dataorientering”. Det innebærer at man fokuserer på data som fundament for organisasjonen heller enn på prosesser. I dette ligger det at man skiller dataene fra applikasjonene, eller sagt på en annen måte: Skiller informasjonsressursene fra systemene. En datavisjon for en militær nettsentrisk omgivelse er skissert i NATO NEC Data Strategy [6]. Vi vurderer NATOs strategi å være en farbar vei å gå ut fra teknologiutviklingen i et 10-års perspektiv.

Hovedmålet med en nettsentrisk datastrategi er å øke datamengden som blir synlig gjennom hele organisasjonen - ”Enterprise Wide”. Dvs mer ”Enterprise” data, mer COI-data og mye mindre ”private” data, samt sikre at data er tilgjengelige og brukbare for både forutsette og uforutsette brukere og applikasjoner. Spesielt uforutsette brukere refererer til en type ønsket fleksibilitet som krever aksesskontroll på objektnivå basert på sikkerhetsmerking og brukerprivilegier [1].

Realiseringen av en nettsentrisk datavisjon baserer seg på tre kjernefaktorer, se [5]:

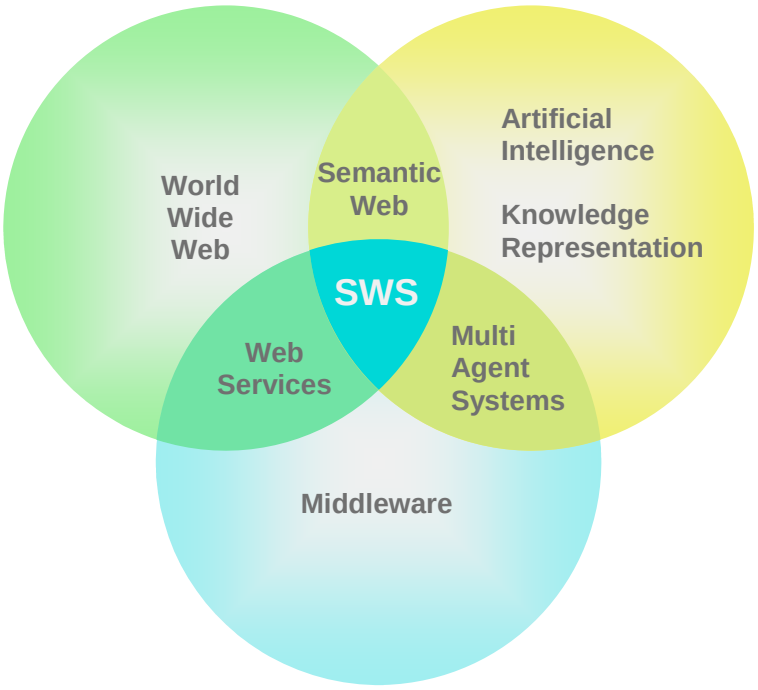
1. *”Communities of Interest”* (COIs) for å adressere organisasjonen (virksomheten) og vedlikeholdet av dataressursene. COIs introduseres fordi COI er en konstruksjon for nettbasert samarbeid (utveksling av dataressurser gjennom INI), se seksjon 2.3.
2. *Metadata*, som tilbyr en måte å beskrive dataressurser på samt bruken av metadata- og tjenesteregistre (”Discovery” registre) samlet i ”Shared Spaces” (felles informasjonsrom) i nettverket.
3. *INI-kjernetjenester (”Core Services”)* som muliggjør data- ”tagging”, -deling, -søking, -lagring og gjenfinning. Tjenesteregisteret UDDI som er beskrevet i seksjon 2.2, er et eksempel på en INI-kjernetjeneste.

2.5 Semantic Web Services

Semantic Web Services (SWS) bygger på en kombinasjon av fagområdene Semantic Web og Web Services. Sistnevnte er beskrevet i seksjon 2.2, mens Semantic Web bygger på en visjon om at datamaskiner skal kunne håndtere meningsinnhold, og ikke bare syntaks slik vi er vant til fra før. Semantikk er altså meningsinnhold, og for å beskrive meningsinnholdet i de begrepene vi ønsker å bruke, benytter man ontologier. Mer informasjon om Semantic Web finnes i [7].

Hovedbudskapet i SWS er å bruke semantiske teknikker for å beskrive de Web Services som man får tilgjengeliggjort i en tjenesteorientert arkitektur. Poenget med semantikken er å gjøre det mulig å gi presise tjenestebeskrivelser som tilrettelegger for automatisering.

En annen og litt mer vidtfavnende illustrasjon av hvordan SWS defineres som at man har tatt det beste fra flere verdener, er vist i Figur 2.3.



Figur 2.3 Semantic Web Services kombinerer flere fagfelt

Dagens bruk av Web Services forutsetter i stor grad forhåndskunnskap om det som kreves for å benytte seg av dem og hvor tjenestene fysisk sett er å finne. I en tjenesteorientert arkitektur har man modeller for dynamiske oppslagstjenester (Dynamic Service Discovery). For å gjøre oppslagstjenesten fullstendig automatisert og dynamisk er det nødvendig at tjenestene er beskrevet på en semantisk entydig måte. Vanlig tekst og naturlig språk strekker ikke til.

Det finnes ulike initiativer som konkurrerer om å bli en akseptert standard for SWS. Blant de som er foreslått overfor World Wide Web Consortium (W3C) er:

- Web Service Ontology Language (for) Services (OWL-S)
- Web Service Modelling Ontology (WSMO)
- Web Service Semantics - Web Service Description Language (WSDL-S)
- Semantic Annotation Web Services Description Language (SAWSDL)
- Semantic Web Services Ontology (SWSO)

Prosjektet har gjort en overordnet vurdering av SWS i form av et oversiktsnotat [8] som sammenligner ovennevnte initiativer. Vår vurdering er at det ennå gjenstår vesentlig arbeid før det blir klart hvordan dette teknologiområdet best kan utnyttes i Forsvaret og når verktøyene vil være modne nok. Utsiktene for denne typen løsninger er svært lovende, og arbeidet med internasjonal standardisering vil være viktig for den videre utviklingen på området.

2.6 Informasjonssikkerhet

Hensikten med den tjenesteorienterte arkitekturen er å øke muligheten for å tilgjengeliggjøre og dele informasjon. Dette fører også til økt sårbarhet ved at mer data vil være tilgjengelig for en som klarer å bryte seg inn i systemet. Tradisjonell bruk av IP-kryptering sikrer informasjonen mellom rutere tilknyttet et domene, men vil ikke sikre informasjonen i lokalnettet bak krypto-apparatet. Hvis vi ser på utfordringene relatert til Information Warfare og Computer Network Attacks (CNA), så vil slike angrep hovedsakelig fokusere på lokalnettene og informasjonssystemene bak krypto-apparatene fordi det er her informasjonen er dårligst beskyttet og dermed mest sårbar. Gode sikkerhetstjenester som ivaretar sikkerheten helt ut i endesystemene vil derfor bli svært viktig.

Karakteristisk for dagens situasjon er atskilte sikkerhetsdomener som beskytter informasjon med forskjellig sensitivitet ved fysisk, kryptografisk og administrativ isolasjon. Det er bare svært begrenset informasjonsflyt mellom disse sikkerhetsdomenene. For å muliggjøre en mer dynamisk informasjonsflyt som man ser for seg i et NbF, må informasjon som er nødvendig for å kunne utføre et oppdrag være tilgjengelig uavhengig av graderingsnivå. Det er brukerens aksessprivilegier som bør styre tilgangen til informasjonen, og ikke hvilket nettverk og system vedkommende er knyttet til. Det er derfor behov for å bevege seg bort fra sikkerhetsdomene-tankegangen og over mot beskyttelse av selve informasjonsobjektene ved bruk av sikkerhetsmerker, digitale signaturer og streng aksesskontroll basert på brukerens aksessprivilegier. Dette vil gjøre det mulig å gruppere informasjonen etter oppdrag og behov. Prosjektet demonstrerte bruk av slike løsninger for Web Services i SecSOA demonstratoren under CWID 06 (se 3.4), og det anbefales at Forsvaret fokuserer mer på å ta i bruk slik teknologi.

Det er viktig å ta sikkerhet med i betraktning tidlig når nye løsninger skal velges. Det finnes i dagens systemer lite sikkerhet på applikasjonsnivå eller informasjonsnivå, da det er vanskelig å introdusere dette på tvers av heterogene applikasjoner. Det vil sannsynligvis være enklere å etablere ende-til-ende løsninger ved å fokusere på sikring av XML-informasjon som en del av mellomvaren. Mulige løsninger for dette ble demonstrert i SecSOA demonstrasjonen under CWID 06. Her ble det vist at det er mulig å innføre generiske sikkerhetsløsninger i Web Services uavhengig av applikasjonene. NSM er også positive til slike løsninger og det anbefales at Forsvaret vurderer hvordan slike løsninger kan tas i bruk operativt.

Ende-til-ende sikkerhet ekskluderer ikke bruk av etablerte, tiltrodde sikkerhetstjenester på lavere lag. For eksempel kan IP-kryptering benyttes i tillegg for å ivareta konfidensialitetsbeskyttelse av informasjon med høyere graderinger. Link kryptering kan også benyttes for å beskytte mot trafikkanalyser. Vedrørende trafikkanalyser så forskes det på interessante alternative metoder for anonymisering av datatrafikk, som på sikt kanskje kan erstatte behovet for link-kryptering.

Som beskrevet i seksjon 3 finnes en rekke spesifikasjoner og standarder relatert til sikkerhet i XML og Web Services. Prosjektet har implementert og testet flere av disse spesifikasjonene i sin demonstrator. Spesifikasjonene er et godt skritt i riktig retning, men er ikke alene tilstrekkelig for å innføre de sikkerhetsmekanismene som man ser for seg på sikt, med bl.a. merking av

informasjonsobjektene og aksesskontroll basert på brukerprivilegier. Når det gjelder sikkerhetsmerker finnes det pr. i dag ingen offisielle spesifikasjoner eller standarder basert på XML. På FFI drives det forskning på dette området i samarbeid med bl.a. NC3A. Med fokus på internasjonale operasjoner er det viktig å velge løsninger basert på de samme standardene som våre samarbeidspartnere. Vi er nå ved en korsvei hvor nye løsninger basert på bl.a. anbefalinger fra NNEC FS skal realiseres og standarder og spesifikasjoner skal velges. Det er viktig at Norge er med der det skjer og kan bidra til å forme løsningene. Det anbefales derfor at det satses tungt på deltagelse i relevant internasjonalt standardiseringsarbeid.

På kort sikt er det lite trolig at man klarer å bevege seg bort fra den tradisjonelle inndelingen av gradert informasjon i sikkerhetsdomener. Det man kan forsøke å få til i dette perspektivet er en mer automatisert flyt av informasjon mellom sikkerhetsdomenene. For å sende informasjon fra lavt nivå til høyt nivå eller mellom sikkerhetsdomener på samme graderingsnivå (for eksempel mellom nasjonal Hemmelig og NATO Secret), finnes det bl.a. diode løsninger som muliggjør en automatisert filterfunksjon. Utfordringen ligger i å automatisere utvekslingen av informasjon fra høyt nivå til lavt nivå (for eksempel sende Begrenset informasjon fra et System High Hemmelig domene til et Begrenset domene). Løsninger prosjektet har testet ut i sine demonstratorer går ut på å binde sikkerhetsmerker som angir sensitiviteten til informasjonsobjektene ved bruk av digitale signaturer. Disse sikkerhetsmerkene kan deretter sjekkes av XML ”guards” når informasjonen er på vei inn og/eller ut av domenene. Det anbefales at Forsvaret jobber videre med disse løsningene med fokus på løsninger som lar seg godkjenne av sikkerhetsmyndighetene.

2.7 Gjennomgående tjenestekvalitet

For å sikre levering av viktig tidskritisk informasjon, er det viktig å etablere en informasjonsinfrastruktur med gode mekanismer for å håndtere tjenestekvalitet. Dette er nødvendig bl.a. for å kunne differensiere informasjonsutvekslingen i henhold til prioritet og kommunikasjons- og informasjonssystemenes kapasitet. Gjennomgående løsninger for tjenestekvalitet på ulike nivåer, både på informasjonsnivå, nettnivå og transmisjonsnivå, må sees i sammenheng og koordineres for maksimal utnyttelse av ressursene. En slik infrastruktur bør i størst mulig grad bygge på standarder og tilgjengelig hyllevare. Det blir derfor viktig å se nøye på hvilke eksisterende og kommende teknologiske løsninger som kan tenkes å være passende å basere seg på, samtidig som man prøver å ha et helhetlig bilde av infrastrukturen.

Mellomvaren gir applikasjoner en uniform måte å benytte underliggende teknologi på. Brukeren kan definere ønsket tjenestekvalitet uten å måtte kjenne til egenskapene til transmisjonsmediet. Det er mellomvarens oppgave å ta hensyn til tjenestekvalitet på så vidt forskjellige transmisjonsmedier som trådløse nettverk, kablede nettverk og militære taktiske linker ved å foreta en avbildning av brukerens ønskede tjenestekvalitet ned på underliggende lag. Prosjektet har vurdert noen alternative løsninger for hvordan tjenestekvalitet kan håndteres på mellomvarenivå og hvordan disse kan avbildes ned på nettverket. Dette arbeidet er dokumentert i [9] og [10].

Det finnes per i dag ingen ferdig, standardisert løsning for tjenestekvalitet for Web Services. I

NATO er det ennå ikke tatt stilling til konkrete løsninger for tjenestekvalitet på Web Service-nivå. I NNEC FS [2] og NCOIC[4] [11] er nødvendigheten av tjenestekvalitetsstøtte påpekt, men man har ikke kunnet gi anbefalinger ettersom det finnes lite hyllevare og enda færre standarder på dette området. En mulighet er å ta utgangspunkt i ideen bak den proprietære løsningen WS-QoS [9;10]; å bygge på eksisterende standarder så langt det er mulig og bygge manglende deler selv. I så fall anbefaler vi å benytte et modulært design for å kunne bytte ut egne komponenter med standarder når disse blir tilgjengelige.

Ulike brukere har ulike tjenestekvalitetsbehov definert av deres rolle som bruker av en Web Service. Ulike behov kan avbildes på et sett tjenestekvalitetsparametere, som igjen kan brukes under oppslag for å velge en bestemt tjeneste basert på tjenestekvalitetsklasser. Tjenestekvalitetsklassene vil gjenspeile hvilken tjenestekvalitet som kan tilbys basert på tilgjengelige ressurser (f.eks. det underliggende transmisjonsmediet). Ofte er det ikke nok ressurser til å kunne tilfredsstille alle brukere, og tilgangen må da gis til brukere med høyest prioritet.

Det er behov for et språk for å spesifisere ulike nivåer av tjenestekvalitet for Web Services. Språket må kunne spesifisere alle aspekter ved tjenestekvalitet og kunne brukes i forbindelse med oppslag. Industrikonsortiumet NCOIC [11] har ennå ikke tatt stilling til tjenestekvalitet, men med tanke på deres adopsjonsprofil for nye standarder er det rimelig å anta at de vil velge OASIS Web Services Quality Description Language (WS-QDL [9]) for spesifisering av tjenestekvalitet når den er ferdig utviklet (de har så langt stilt seg bak samtlige WS-standarder). For å sikre evnen til samspill med andre NATO-systemer er vår anbefaling på det nåværende tidspunkt å uttrykke tjenestekvalitetsparametere på en måte som i framtiden vil kunne oversettes til WS-QDL på en enkel måte. Inntil WS-QDL blir tilgjengelig så kan man ta noe annet i bruk (se [9;10] for flere detaljer). Flere utredninger må foretas før en konkret anbefaling kan gis.

Informasjon om den tjenestekvaliteten som ulike tjenester tilbyr må gjøres tilgjengelig for klienter i et tjenesteregister, slik at denne informasjonen kan brukes ved valg av tjenester. Det finnes ingen standarder for dette i skrivende stund, men proprietære løsninger benytter en front-end til UDDI i kombinasjon med et egenutviklet spesifikasjonsspråk. I mangel av standarder kan man utvikle en egen løsning, eller ta utgangspunkt i f.eks. WS-QoS [9].

For å oppnå gjennomgående tjenestekvalitet, er det viktig at løsningene for tjenestekvalitet på mellomvarenivå er interoperable med løsninger for tjenestekvalitet på nettverksnivå. På nettverksnivå finnes det mange eksisterende løsninger for differensiering av trafikk og tjenestekvalitetsstøtte for IP-nettverk og øvrige nettverk som brukes i sivil sammenheng. For militære systemer er taktiske radiolinker også et aspekt å ta hensyn til. NATO dekker hva som bør gjøres med kablede nettverk. Ingen spesielle føringer er lagt på løsninger for taktiske nett, ei heller for tjenestekvalitet på Web Service-nivå. TACOMS[5] [12] og INSC[6] [13] definerer noen

[4] Network Centric Operations Industry Consortium
[5] TACOMS Post 2000
[6] Interoperable Networks For Secure Communications

konkrete QoS-klasser; det er nærliggende å velge dem, eller i alle fall noe som er nært nok til at man kan avbilde egne klasser mot disse. For IP-nettverk er Diffserv trukket frem av både TACOMS, ETNA[7] [14] og INSC.

2.8 Web Services over Disadvantaged Grids

Web Services er i dag den vanligste teknologien for realisere SOA. Web Services er basert på bruk av XML og muliggjør interoperabilitet mellom forskjellige systemer, men gir samtidig høyere overhead og dermed økte krav til datarate på linken. Mens industrien kompenserer for dette med å utvikle nye kommunikasjonsteknologier med stadig høyere datarater, er situasjonen annerledes i taktiske nett i Forsvaret der trådløse taktiske kommunikasjonsteknologier ofte har svært begrenset datarate og variabel linkkvalitet, sammenliknet med kommersielle alternativer. NbF Grid vil bestå av ulike transmisjonssystemer som sannsynligvis vil være integrert som ett nettverk ved bruk av IP-teknologi. Enkelte av disse transmisjonssystemene kan ha relativt høy datarate og vil velges hvis forholdene ligger til rette for det. Men det vil også være situasjoner hvor det eneste som fungerer er radiosystemer med lav datarate og ofte høy forsinkelse og pakketap (f.eks. VHF og HF). Vi omtaler disse som ”Disadvantaged Grids” i mangel av et dekkende norsk begrep. I NbF sammenheng er det viktig å ha tilgang til enkelte av tjenestene i informasjonsinfrastrukturen selv om det bare er mulig å kommunisere over et Disadvantaged Grid. Prosjektet har derfor bevisst satset på å vurdere teknikker for å redusere overhead i XML og Web Services, og dermed gjøre det mulig å bruke SOA-tjenester over Disadvantaged Grids. Følgende alternativer er vurdert:

- Komprimering av XML data
- Bruk av taktisk meldingstjeneste som bærer
- Distribusjonsmekanismer
- Proxy noder

Det har blitt utført både teoretiske studier, praktiske eksperimenter og målinger. Resultatene som har kommet fram av dette arbeidet er beskrevet i rapport [15], og kan oppsummeres på følgende måte.

Når det gjelder teknikker for å redusere overhead i XML og Web Services for å muliggjøre bruk av SOA-tjenester over Disadvantaged Grids, viste målinger at det er mye å hente ved å komprimere XML data. XML har mye overhead og er dermed ”komprimeringsvennlig”. Flere algoritmer gav en reduksjon i datastørrelsen på mer enn 95 %. Formålet med denne undersøkelsen var ikke å velge én metode som er best, ettersom valget vil være avhengig av kravene som stilles i hvert enkelt scenario. Både prosesseringstid og komprimeringsrate er faktorer som må vurderes ved valg av algoritme. Det anbefales å ta i bruk XML komprimeringsteknikkene som beskrevet i rapporten [15] og samtidig monitorere arbeidet med utvikling av en standardisert løsning, som bør følges når den blir tilgjengelig.

[7] European Theater Network Architecture

I NATO og i det sivile markedet er det mye fokus på Web Services. Prosjektet har derfor utført eksperimenter med Web Services over en rekke simulerte kanaler, for å vurdere om det er hensiktsmessig å benytte denne mellomvareteknologien i taktiske nett. Vi har benyttet Meldingstjenesten i Forsvaret (MIF) som databærer. I Web Services benyttes protokollen SOAP for å utveksle informasjon mellom de ulike komponentene. En fordel med SOAP er at den ikke er begrenset til en spesiell transportprotokoll. I de fleste Web Services applikasjoner benyttes HTTP for transport av SOAP meldingene, men det åpnes også for bruk av andre transportprotokoller som SMTP (Simple Mail Transfer Protocol) eller FTP (File Transfer Protocol). Tanken er at hvis meldingsoverføringsprotokollen SMTP kan benyttes, så kan også andre meldingssystemer benyttes, som for eksempel MIF. FD har som en del av INI programområde satt i gang et prosjekt for å etablere en gjennomgående meldingstjeneste i Forsvaret (P8002). Det vil si at de ønsker å etablere en infrastruktur basert på MIF mellom strategisk og taktisk nivå for alle forsvarsgrener. Vi mener at det i en migrasjonsperiode kan være fordelaktig å utnytte denne infrastrukturen, hvis mulig, til å utveksle Web Services informasjon mellom enheter på alle nivåer.

Undersøkelsen viser at det er teknisk mulig å benytte MIF som bærer av SOAP meldinger, og på denne måten realisere bruk av Web Services i taktiske nett, forutsatt at man benytter komprimering og en effektiv kommunikasjonsprofil. Dersom man benytter XOmail som bærer, så har de to taktiske profilene komprimering innebygget, noe som vil være velegnet for kommunikasjon over så vel taktiske som strategiske nettverk. Forutsetningen for at dette skal virke, er at hyppigheten på meldingene som sendes ut ikke er så stor at den overskrider nettets kapasitet selv ved bruk av komprimering. Man kan i slike tilfeller tenke seg å benytte ulike teknikker for å optimalisere selve meldingsutvekslingen. Vi har presentert to teknikker i rapporten [15]:

1. Optimalisering av representasjon og informasjonsutveksling
2. Bruk av proxies

Begge disse teknikkene vil føre til enda bedre utnyttelse av den kapasiteten man har til rådighet i kommunikasjonssystemene. Det finnes i dag ingen kjente implementasjoner av de nevnte teknikkene som fungerer med Web Services, XML og SOAP. Videre arbeid innen dette område er derfor nødvendig.

3 Eksperimentering

Prosjektet har hatt eksperimentering som en viktig del av arbeidsformen. Fire eksperimenter er gjennomført i samarbeid med eksterne parter i Forsvaret.

Kortnavn	Eksperiment	Gjennomført
BG04	Blue Game 2004	April 2004
NII04	Integrasjon av ressursregister med NORCCIS-II	November 2004
BG05	Battle Griffin 2005	Mars 2005
CWID06	CWID 2006 – SecSOA	Juni 2006

Til eksperimentene har prosjektet benyttet en bildeoppbyggingsdemonstrator, heretter kalt Demonstratoren. Den har i ulike versjoner og modenhetsgrader vært et teknisk fundament for systemdelen av eksperiment-aktivitetene i prosjektet.

Demonstratoren er fundert på en simulert bildeoppbyggingsprosess som gjennomføres i et distribuert (desentralisert) system av programvaremoduler og datamaskiner. Grunnstammen i Demonstratoren er

- generering av objekter og simulerte militære styrker
- simulering av sensorinformasjon
- distribuert datainnsamling og –fusjon, med et situasjonsbilde som resultat

I løpet av prosjektet har flere bestanddeler i Demonstratoren blitt bygget til. Utvidelsene er konkrete resultater av eksperimentrettet teknologiutprøving. Eksempler her er

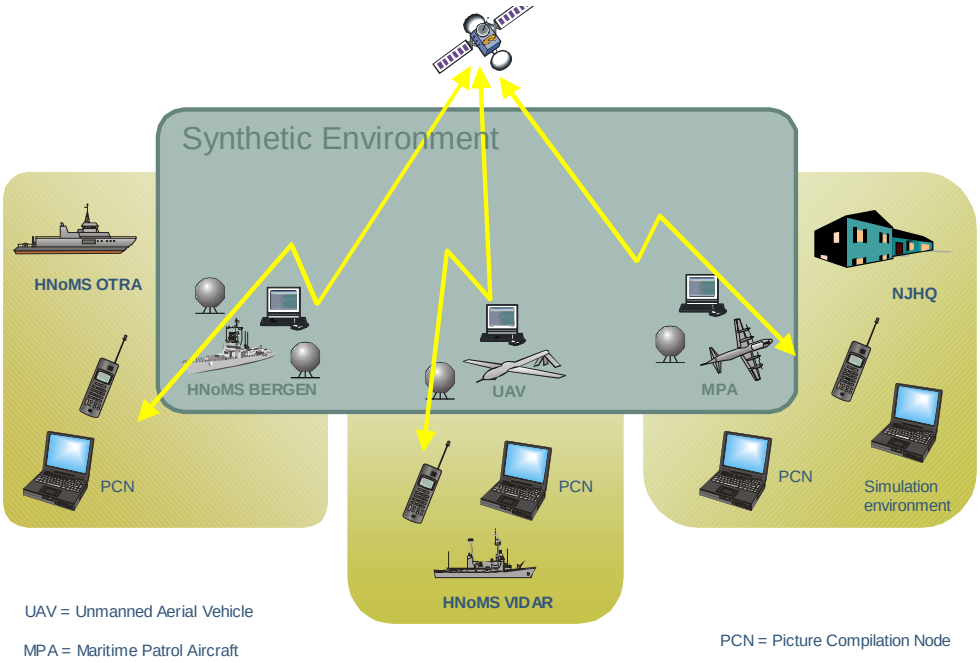
- peer-to-peer utveksling av situasjonsbildeinformasjon ved bruk av JXTA (BG04)
- innnføring av et eksperimentelt tjenesteregister (NII04)
- portalløsning for visualisering og brukerinteraksjon (BG05)
- Web Services, Publish/Subscribe, objektorientert MIP og ende-til-ende sikkerhetsløsninger (CWID06)

I det etterfølgende gis en kort oversikt over hvert av eksperimentene. Mer informasjon vil være å finne i tidligere utgitte publikasjoner fra prosjektet (se konkrete referanser under hvert eksperiment).

3.1 Blue Game 2004

Formålet med prosjektets deltakelse på BG04 var todelt. I et operativt perspektiv ville eksperimentet utforske verdien av ad hoc organisering av informasjonsutvekslingen. Med ad hoc organisering menes at man muliggjør informasjonsmessig sammenkobling av enheter på kort varsel, uten omfattende forhåndsplanlegging. Man kan tenke seg en oppslagstjeneste som holder rede på informasjon om aktørene og som gjør det mulig å koble opp til en egnet enhet ut fra behovet der og da. Hypotesen var at dette ville øke evnen til å etablere et felles situasjonsbilde under forhold der bidragsyterne kommer og går i en dynamisk styrkekonfigurasjon.

På det tekniske området var det et mål i seg selv å gjennomføre en kjøring av Demonstratoren i et realistisk operativt miljø. Figur 3.1 viser at det fra lokasjonene KNM Otra, KNM Vidar og FOHK ble kjørt en distribuert simuleringsomegn. De samme stedene simuleres det samarbeidende noder (henholdsvis KNM Bergen, en UAV og en MPA) som gjennomfører distribuert bildebygging. På alle tre lokasjonene var det mulig å se et felles situasjonsbilde. Datakommunikasjonen foregikk over Iridium satelitt.



Figur 3.1 Faktiske og syntetiske deltakere i eksperimentet BG04

Bakgrunnen for eksperiment-gjennomføringen var delvis en direkte utfordring som ble gitt til FFI av J7 ved FOHK, som ønsket at det ble synliggjort konkrete aktiviteter innenfor NbF-området. Eksperimentet var et samarbeid mellom tre FFI-prosjekter. I tillegg til NbF Beslutningsstøtte deltok

- **Simutrex**, som foresto utvikling og kjøring av den distribuerte simuleringsomegnen
- **NbF Grid**, som stod for datakommunikasjon og det nettverkstekniske, og som i tillegg fikk gjennomført målinger på kommunikasjonsprotokollen JXTA

Tilbakemeldingene på eksperimentet var positive. Den operative responsen bekreftet at prosjektet arbeidet i riktig retning og at denne type eksperimentering ble vurdert som en hensiktsmessig arbeidsform i NbF-utviklingen. Teknisk sett fungerte Demonstratoren i operativ setting, selv om eksperimentet også indikerte at peer-to-peer kommunikasjon (i eksperimentet representert ved JXTA) er til dels svært ineffektivt når kommunikasjonsforholdene er begrensede (det vi senere har betegnet ”Disadvantaged Grids”).

Mer informasjon finnes i hovedrapport [16], samt i [17], [18], [19].

3.2 Integrasjon av ressursregister med NORCCIS-II

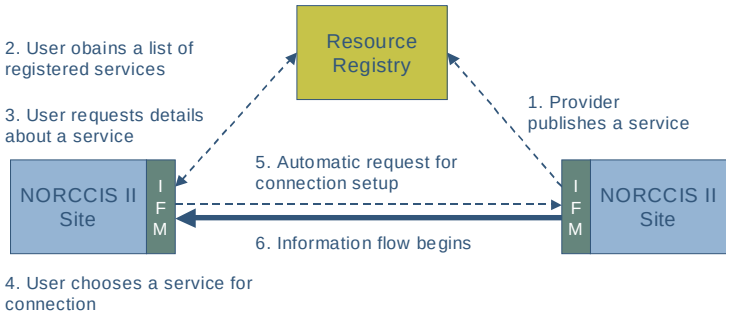
Denne aktiviteten innbefattet teknisk eksperimentering i samarbeid med FLO/IKT. Hensikten var å prøve ut muligheten av at det norske kommando- og kontrollsystemet NORCCIS-II ble satt i stand til å utnytte en eksperimentell oppslagstjeneste. Fra prosjektets side innebar det utvikling av et ressursregister, som var ment å inneholde metadata om tilgjengelige ressurser generelt, og informasjonssystemtjenester spesielt.

Registeret ble utviklet som en sentralisert løsing, da primærfokuset var på innhold og teknisk sett enkel tilgang til registeret. Utfordringen som ligger i å desentralisere en oppslagstjeneste, ble ikke sett på i dette arbeidet. Prosjektet vant her de første erfaringene med bruk av semantiske teknologier, idet Resource Description Framework (RDF) ble brukt for å modellere metadata i registeret.

Parallelt med FFIs arbeid med ressursregisteret gjennomførte FLO/IKT utviklingen av modulen Information Flow Manager (IFM). Selve eksperiment-gjennomføringen skjedde som en laboratorieøvelse den 25. november 2004, da partene i samarbeid demonstrerte følgende prinsipielle steg i bruken av en oppslagstjeneste:

- registrering av en IFM-administrert tjeneste i ressursregisteret (1)
- klientoppslag for å gjenfinne en registrert tjeneste (2-3-4)
- klient-tilkobling til tjenesten som ble funnet (5-6)

Nummer-henvisningene refererer til stegene slik de er fremstilt i Figur 3.2.



Figur 3.2 Grunnleggende sekvens i bruken av en registertjeneste

Eksperimentet tyder på at det med relativt små endringer i eksisterende applikasjoner er mulig å utnytte en oppslagstjeneste.

Se eksperimentrapport [20] for mer informasjon.

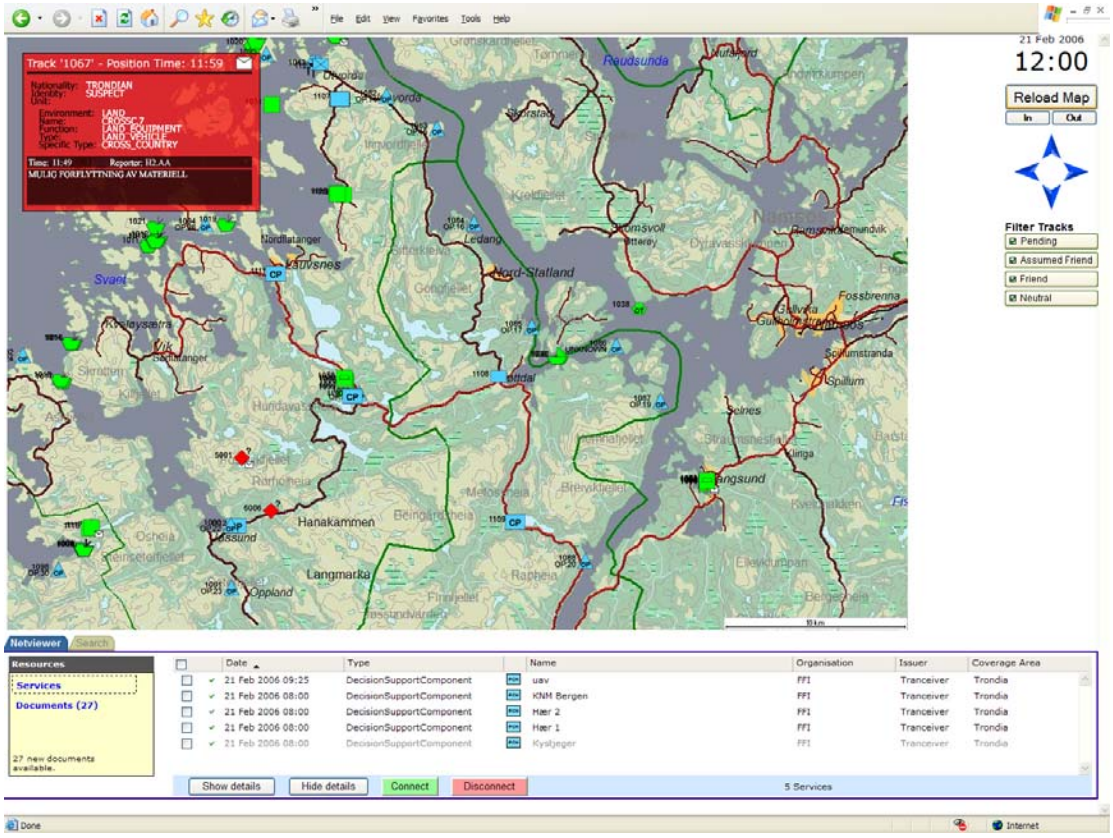
3.3 Battle Griffin 2005

Vinteren 2005 fikk prosjektet anledning til å bruke operativt personell aktivt i eksperiment-sammenheng. Under øvelse Battle Griffin på Sprova i Nord-Trøndelag fikk vi disponere en halv dag fra hver av i alt 18 etterretningsoffiserer som var til stede. Formålet var fortsatt å utforske NbF-ideene om å muliggjøre dynamisk styrkekonfigurasjon. Men i motsetning til BG04, som i hovedsak gjennomførte en demonstrasjon av distribuert bildeoppbygging, ville BG05 se nærmere på organisasjonens rolle og menneskene i den i kontekst av et dynamisk NbF.

Begrepet situasjonsbevissthet (eller mer presist det engelske Situation Awareness, i det følgende forkortet SA) står sentralt i BG05. Det ble gjennomført eksperimentelle målinger av SA, både på individnivå og i grupper. Eksperimentet, som ble gjennomført tre ganger (en kjøring hver dag, med nye forsøkspersoner hver gang), foregikk som følger:

- Tre grupper a to personer samarbeidet om å bygge et felles situasjonsbilde. Det var i utgangspunktet ingen rangordning innen eksperimentet – gruppene samarbeidet flatt (peer-to-peer) på taktisk nivå.
- Demonstratoren var satt opp slik at hver gruppe så ”sitt” geografiske område. De hadde muligheter til, via funksjonen NetViewer, å søke etter og finne de andres situasjonsbilder, og koble seg opp der. I tillegg fantes det simulerte informasjonskilder i overflod.
- Hendelsesforløpet simulerte et 4-timers forløp som ble spilt av i løpet av en time.

Figur 3.3 viser arbeidsflaten som forsøkspersonene hadde foran seg.



Figur 3.3 Hovedvinduet i portalløsningen som ble brukt under BG05

Forsøkspersonene hadde som oppgave å samarbeide om å bygge et felles bilde. Det ble gjort observasjoner underveis, og de ble bedt om å besvare omfattende spørreskjemaer både underveis og etterpå. På basis av dette ble individuell og gruppevis SA "målt" i forhold til i hvilken grad kandidatene og gruppen hadde forstått de operasjonelle sammenhengene. Dette ble sett opp mot bl.a. deres oppfattelse av teknologistøtten (altså om Demonstrator-funksjonaliteten de ble tilbudt ble oppfattet som et nyttig verktøy for denne type oppgave).

BG05 kunne ikke forventes å gi klare svar om fremtidig arbeid og organisering innenfor NbF. Eksperimentet må betraktes som et lite men viktig bidrag til det å vinne erfaring med å vurdere denne type spørsmål. Det bekrefter antakelsen om at menneskelige og organisasjonsmessige aspekter må inkluderes sammen med teknologi i arbeidet frem mot NbF.

Hovedkonklusjonene fra BG05 er:

- Nye tekniske løsninger kan øke evnen til å etablere et felles situasjonsbilde når styrkene konfigureres dynamisk.
- Prosessene i bildeoppbyggingen bør tilpasses slik at man får størst mulig operativ nytteverdi ut av de nye teknologiske mulighetene

Eksperimentet ble gjennomført i samarbeid med FFI-prosjekt 879 "NbF i operasjoner", som prøvde ut et eksperimentelt konsept for "Forhandlingsbasert ressursallokering". Situasjoner som krevde ressursallokering var lagt inn i det hendelsesforløpet som forsøkspersonene ble utsatt for, og forhandlingene som oppstod ble observert.

Mer informasjon finnes i hovedrapport [21], samt i [22], [23], [24], [25].

3.4 CWID 2006 – SecSOA

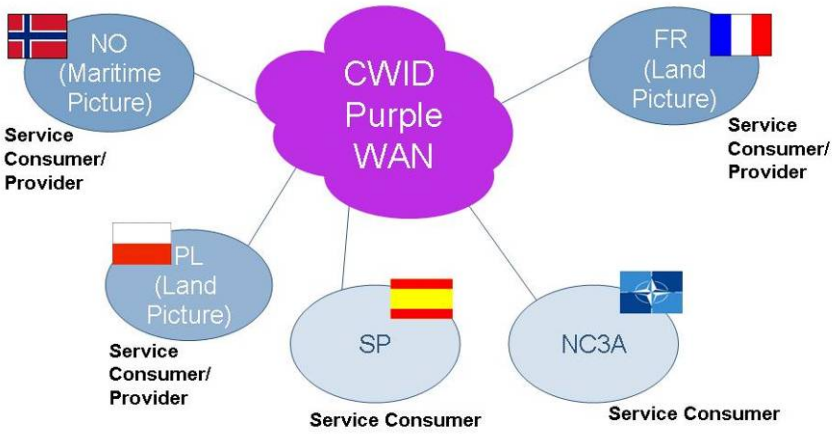
SecSOA – eller "Secure SOA supporting NEC" som den mer fullstendige tittelen er – hadde som mål å vise den gode samlede effekten av å kombinere ny teknologi på fire ulike områder:

- Etablering av et dynamisk tjenesteregister
- Publish/subscribe-type informasjonsutveksling basert på Web Services
- Ende-til-ende sikkerhet
- Objektorientert utnyttelse av MIP-datamodellen C2IEDM

Prosjektets eksperiment under NATO CWID 2006 var en del av et internasjonalt samarbeid i regi av NATO-forskningsgruppen IST-061. Samtidig hadde vi et nasjonalt samarbeid med FLO/IKT om en eksperimentell integrasjon mellom Demonstratoren og NORCCIS-II, primært for å kunne overføre data fra Demonstratoren til NORCCIS-II for profesjonell fremvisning.

Forskningsgruppen IST-061 hadde som erklært mål å vise resultatene av sitt arbeid på NATO CWID 2006. Første del av arbeidet var et sett med spesifikasjoner [26], som var ferdige i mars 2006. Mye var basert på bruk av åpne standarder innenfor Web Services verdenen, men

omfattende tillegg måtte utvikles bl.a. på områdene tjenesteregister og sikkerhet. Etter ferdigstillelsen av spesifikasjonsdokumentet i mars krevdes det intens innsats for å kunne gjennomføre på CWID i juni.



Figur 3.4 Deltakende nasjoner i SecSOA på CWID06

Som medvirkende nasjoner på CWID06 deltok Frankrike og Polen fra IST-061 i tillegg til Norge. I tillegg, som vist på Figur 3.4, deltok Spania og NC3A i SecSOA testingen, noe som gir en god indikasjon på verdien av de spesifikasjonene som er laget. De kom med sent i prosessen, men maktet raskt å lage noe som fungerte. Tyskland og Nederland var også med i IST-061, men fikk ikke deltatt med egne løsninger på CWID. De har likevel gitt verdifulle bidrag til evalueringsprosessen i etterkant.

For prosjektet har deltakelsen i IST-061 og på CWID 2006 først og fremst vært en uvurdelig lære- og erfaringsprosess. Utbyttet av først å være med på å definere et sett med spesifikasjoner, for deretter å delta i å avdekke de mange svakheter som uvilkårlig vil bli avslørt når noe faktisk skal implementeres i henhold til de samme spesifikasjonene, er meget verdifullt. Det har gitt alt fra førstehånds teknologi-innsikt på det individuelle plan til velutviklede samarbeidsrelasjoner både innad og utad.

Arbeidet har videre vært banebrytende innenfor sikkerhetsområdet, i den forstand at prosjektet gjennom dette har vært med på å initiere løsninger som på sikt kan muliggjøre fremtidsvisjonene om sikker og fleksibel informasjonsutveksling. Løsninger her er en nødvendig forutsetning for full utnyttelse av potensialet som ligger i NbF.

Mer informasjon er å finne i hovedrapport [27], eksperimentnotat [28], samt [29;30] og oppdatert spesifikasjon [31].

4 Internasjonale aktiviteter

4.1 NATO-forskningsgruppen IST-061

Som nevnt foran var prosjektets eksperiment under NATO CWID 2006 en del av et internasjonalt samarbeid i regi av NATO-forskningsgruppen IST-061. Deltakende nasjoner i forskningsgruppen i tillegg til Norge var Frankrike, Polen, Nederland og Tyskland. NC3A var i perioder også med i gruppen. På norsk side var Thales Norge representert i gruppen sammen med FFI. Thales Norge og FFI hadde et godt samarbeid i forskningsgruppen.

I den innledende fasen av forskningsgruppen var det diskusjon om innretning og målsetting for gruppen. På forslag fra FFI ble det etter hvert enighet om at gruppen skulle ha eksperimentfokus og dessuten gjennomføre en demonstrasjon under CWID 2006. Forskningsgruppens navn etter denne innledende runden ble ”Secure Service Oriented Architectures (SOA) supporting Network Enabled Capabilities”. Mandatet for gruppen finnes i [32].

Et viktig resultat fra gruppen er demonstratorspesifikasjonen som har blitt laget [26]. En oppdatert versjon gjøres også offentlig tilgjengelig. Sluttrapport fra gruppen er under utarbeidelse [33].

4.2 Andre NATO-grupper

Prosjektet var også representert i andre grupper og fora innenfor NATO. Disse gjennomgås i det følgende.

– *MMHS (”Military Message Handling System”)* arbeidsgruppe under NC3B SC/5. Prosjektet har ledet aktiviteten for taktisk MMHS og bl.a. vært editor for STANAG 4406 Annex E som beskriver de taktiske meldingsprotokollene. Prosjektet har også vært editor for den militære standarden ACP 142-PMUL (versjon 2) som er en pålitelig transportprotokoll for multicast av meldinger på taktisk nivå. Prosjektet har også fått gjennomslag for standardisering av protokollen ”Direct Message Profile” som et nytt alternativ i STANAG 4406 Annex E. Denne protokollen er tilpasset tidskritiske meldinger over taktiske kommunikasjonssystemer med ekstremt liten datarate og er implementert i vårt nasjonale meldingssystem.

– *”XML Namespace Managers Forum”* under NC3B SC/5. Dette syndikatet ble i hovedsak opprettet for å arbeide med etableringen av et NATO XML Registry. Formålet til dette registeret er å samle, lagre og fremme spredningen og gjenbruk av XML komponenter. Mens arbeidet med etableringen av et NATO register pågår har en inngått en avtale om bruk av ”US DoD Metadata Registry and Clearinghouse” som en interim løsning. I tillegg til arbeidet med registeret har gruppen jobbet med retningslinjer for bruk av XML innenfor NATO. Prosjektet har deltatt i denne prosessen, i hovedsak ved kommentering av diverse dokumenter. Fra 2007 vil denne gruppen bli en permanent del av NC3B SC/5, under navnet ”XML Services Working Group”.

– *Land Group 1*. Prosjektet har støttet FFI-prosjektet 878 (Soldatutrustning videreføring/ NORMANS) i dets arbeid i Land Group 1. Vi har bidratt til å utarbeide arkitekturen i deres C4I STANAG for soldatkommunikasjon. Her har vi bl.a. anbefalt bruk av de taktiske MMHS protokolløsningene (definert i STANAG 4406 Annex E) som ser ut til å bli akseptert.

Prosjektet har også vært med på innledende møter i forkant av formell opprettelse av nye NATO forskningsgrupper (såkalte ”Research Task Board Exploratory team”). Disse er:
– IST-068 “XML in Cross-Domain Security Solutions
– IST-075 “Semantic Interoperability”

Disse gruppene vil bli fulgt opp av nye prosjekter ved FFI Avdeling Ledelsessystemer.

5 Internasjonale publikasjoner

Arbeidet i prosjektet har blitt publisert ved ulike konferanser. De artikler som har blitt presentert oppsummeres nedenfor i kronologisk rekkefølge:

#	**Artikkel**	**Konferanse**	**Reise-rapport**
1.	Situation awareness, the abstraction hierarchy and the design of user interfaces of command and control decision support systems [34]	HPSAA II - *Human Performance, Situation Awareness and Automation Technology*, DAYTONA BEACH, USA, 22 - 25 mars 2004	[35]
2.	Peer-to-Peer Technology – An Enabler for Command and Control Information Systems in a Network Based Defence? [36]	*9th Command and Control Research and Technology Symposium 2004* (9th CCRTS), San Diego, June 15-17 2004 *9th International Command and Control Research and Technology Symposium 2004* (9th ICCRTS), Copenhagen, 14-16 September 2004	[37] [38]
3.	Ad hoc Organization of Distributed Picture Compilation and Support for Situation Awareness in Network Based Defence – An Exploratory Experiment [39]	*10th International Command and Control Research and Technology Symposium*, McLean VA, June 13-16 2005	[40]
4.	Discovering Semantic Web Services in Dynamic Environments [41]	*IEEE European Conference on Web Services* (ECOWS 2005), November 2005	[42]
5.	A Conceptual Service Discovery Architecture for Semantic Web Services in Dynamic Environments [43]	*International Workshop on Semantics Enabled Networks and Services*, IEEE International Conference on Data Engineering, April 2006	
6.	Security in Service Oriented	*Information Assurance for Defence*,	

#	Artikkel	Konferanse	Reise-rapport
	Architectures - A Network Enabled Capability (NEC) Perspective [44]	*Securing Military Communications and Networks*, February 2006 arrangert av Defence IQ	
7.	An architecture for experimenting with secure and dynamic Web Services [45]	*11th Command and Control Research and Technology Symposium (2006 CCRTS),* San Diego, June 2006	[46]
8.	Experiences from implementing dynamic and secure Web Services [47]	*11th International Command and Control Research and Technology Symposium (11th ICCRTS),* Cambridge, September 2006	[48]

6 Andre bidrag

Prosjektet har i tillegg til de prosjektnære oppgaver bidratt inn i ulike overordnede prosesser og dokumentutarbeidelser i Forsvaret. For det første har prosjektet, sammen med andre prosjekter innenfor NbF programmet ved avdeling Ledelsessystemer, støttet FD i dets planarbeid i plangruppen for programområdet INI. Spesielt har dette arbeidet vært støtte til utarbeidelse av overordnet INI materiellplan.

Videre har prosjektet, igjen sammen med andre prosjekter innenfor NbF programmet, bidratt inn i arbeidsgruppen INI-utredningen i Forsvarsstudie 07 (FS 07). Her har det spesielt blitt utarbeidet to dokumenter på oppdrag fra INI-utredningen. Dette er for det første et dokument [49] som oppsummerer de viktigste teknologiske trender innen informasjons- og kommunikasjonsteknologi (IKT), samt et dokument [50] som oppsummerer de viktigste anvendelsestrender innen IKT.

Prosjektet har også laget et forslag til en modifisert referansemodell for INI. Dette arbeidet startet som en del av ’P8009 Modernisering av kjernetjenester’ hvor man identifiserte noen områder hvor modellen kunne forbedres. Dette forslaget vil være et innspill til FDs revisjon av modellen som forventes startet ut på våren 2007. Det må også nevnes at prosjektet har gitt høringsinnspill til FOHK i forbindelse med NATO NEC Feasibility Study (vinter 2005).

Prosjektet har vært involvert i utarbeidelse av fremskaffelsesløsninger (FL) for flere prosjekter. Disse er:

- ’P9268 Variantbegrensing av Operative Beslutningsstøttetjenester’
- ’P8002 Gjennomgående militær meldingstjeneste’
- ’P9269 Beslutningsstøtte for stridsteknisk nivå’
- ’P8008 Interimsløsning Battlefield Management System’
- ’P8009 Modernisering av kjernetjenester’
- ’P8011 FISBasis H/NS for lavere taktisk nivå’
- ’P2912 COSS og NCAGS’

Referanser

[1] GAGNES Tommy, EGGEN Anders, HEDENSTAD Ole-Erik, RASMUSSEN Rolf, and SLETTEN Geir, "OPERATIVE BESLUTNINGSSTØTTETJENESTER - FREMTID NBF,"FFI/RAPPORT-2005/03584, Nov.2005.

[2] NC3A, "NATO Network Enabled Capability Feasibility Study,"Volume 1, Version 2.0, 2005.

[3] GAGNES Tommy, "A Survey of Service-Oriented Architecures, Event-Driven Architectures and the Current State of Web Services Technology,"FFI/NOTAT-2004/04264, 2004.

[4] GAGNES Tommy, BJØRNSTAD Rune, and LANGMYR Anders, "AN ARCHITECTURE FOR SERVICE DISCOVERY IN A NETWORK BASED DEFENCE,"FFI/NOTAT-2006/00115, 2006.

[5] HAFNOR Hilde, "INI SOM NETTSENTRISK VIRKSOMHETSOMGIVELSE - BRUK AV "ENTERPRISE METADATA" OG "COMMUNITIES OF INTEREST" (COIs),"FFI/RAPPORT-2006/00862, Mar.2006.

[6] NATO NEC, "NNEC Data Strategy, NATO/EAPC, Version 1.1,"EAPC(AC/322-SC/5)N 0018, 2005.

[7] GAGNES Tommy, "A SURVEY OF THE CURRENT STATE OF THE SEMANTIC WEB,"FFI/NOTAT-2004/03985, 2004.

[8] RUSTAD Marianne and GAGNES Tommy, "A survey of Semantic Web Services,"FFI/NOTAT-2006/03958, Dec.2006.

[9] JOHNSEN Frank Trethan and HAFSØE Trude, "Betraktninger rundt tjenestekvalitet for web services i NbF,"FFI/NOTAT-2006/02580, 2006.

[10] JOHNSEN Frank Trethan, HAFSØE Trude, and LUND Ketil, "Quality of Service considerations for Network Based Defense,"FFI/RAPPORT-2006/03859, 2006.

[11] "Network Centric Operations Industry Consortium (NCOIC)," www.ncoic.org, 2006.

[12] "TACOMS Post 2000," www.tacomspost2000.org.

[13] "INSC (Interoperable Networks For Secure Communications)," http://insc.nodeca.mil.no/ifs/files/startframe.html.

[14] "ETNA (European Theater Network Architecture)," www.eda.europa.eu.

[15] HADZIC Dinko, HAFSØE Trude, JOHNSEN Frank Trethan, LUND Ketil, and ROSE Kjell, "Web Services i nettverk med begrenset datarate,"FFI/RAPPORT-2006/03886, Dec.2006.

[16] RASMUSSEN Rolf, GAGNES Tommy, GUSTAVSEN Richard Moe, HAFNOR Hilde, HANSEN Bjørn Jervell, HAAKSETH Raymond, MEVASSVIK Ole Martin, OLAFSEN Runar, and ROSE Kjell, "EXPLORATORY EXPERIMENT "AD HOC ORGANIZATION OF PICTURE COMPILATION" CONDUCTED DURING BLUE GAME 2004: EVALUATION REPORT,"FFI/RAPPORT-2004/01940, June2004.

[17] HAFNOR Hilde and OLAFSEN Runar, "EKSPERIMENTERING MED AD HOC ORGANISERING AV BILDEOPPBYGGING I NBF: EVALUERING AV OPERATIV NYTTEVERDI - BLUE GAME 2004,"FFI/NOTAT-2004/01885, 2004.

[18] URDAHL Morten and LEERE Anton B, "TEKNISKE INSTALLASJONER FOR EKSPERIMENT "AD HOC ORGANISERING AV BILDEOPPBYGGING" UNDER BLUE GAME 2004,"FFI/NOTAT-2004/03184, 2004.

[19] OLAFSEN Runar, "(U) STØTTE AV SITUASJONSBEVISSTHET I PRAKSIS - FELTSTUDIE BLUE GAME 2004,"FFI/NOTAT-2004/02542 - Begrenset, 2004.

[20] GAGNES Tommy and LANGMYR Anders, "USER-DEFINED ACCESS TO SITUATION INFORMATION SERVICES - AN EXPERIMENT,"FFI/RAPPORT-2004/04171, Nov.2004.

[21] HAFNOR Hilde, HANSEN Bjørn Jervell, LANGMYR Anders, NORMARK Runar, RASMUSSEN Rolf, and ROSE Kjell, "EXPERIMENT REPORT: "AD HOC ORGANISATION OF PICTURE COMPILATION AND SITUATION AWARENESS IN NBD" - BATTLE GRIFFIN 2005,"FFI/RAPPORT-2005/01492, May2005.

[22] NORMARK Runar and HAFNOR Hilde, "EKSPERIMENTERING MED DISTRIBUERT SITUASJONSBILDEBYGGING VED ØVELSE BATTLE GRIFFIN 2005 - Metode og resultater,"FFI/RAPPORT-2005/01614, 2005.

[23] RASMUSSEN Rolf et al., "DEMONSTRATOR FOR BILDEOPPBYGGING - ANVENDT FOR EKSPERIMENTERING UNDER ØVELSE BATTLE GRIFFIN 2005,"FFI/NOTAT-2005/01474, 2005.

[24] HAFNOR Hilde, HANSEN Bjørn Jervell, and ROSE Kjell, "898 NBF BESLUTNINGSSTØTTE: BESKRIVELSE AV SCENARIO BRUKT UNDER BATTLE GRIFFIN 2005 EKSPERIMENTET,"FFI/NOTAT-2005/01524, 2005.

[25] FJELD Sven-Ivar, "NETVIEWER - Teknisk innsikt i en Web Services orientert GUI klient,"FFI/NOTAT-2005/01616, 2005.

[26] NATO RTO IST-061, "The NATO RTO/IST-061 Secure SOA Demonstrator Specification for CWID 2006, version 1.0,"Mar.2006.

[27] RASMUSSEN Rolf, EGGEN Anders, HADZIC Dinko, HEDENSTAD Ole-Erik, HAAKSETH Raymond, and LUND Ketil, "EXPERIMENT REPORT: "SECURE SOA SUPPORTING NEC" - NATO CWID 2006,"FFI/RAPPORT-2006/02538, Dec.2006.

[28] RASMUSSEN Rolf, EGGEN Anders, HADZIC Dinko, HAAKSETH Raymond, LUND Ketil, and ROSE Kjell, "EXPERIMENT DOCUMENTATION: "SECURE SOA SUPPORTING NEC" - NATO CWID 2006,"FFI/NOTAT-2006/02539, Dec.2006.

[29] ROSE Kjell, LUND Ketil, and SLETTEN Geir, "SUGGESTED IMPROVEMENTS TO THE MIP WEB SERVICES/OBJECT-ORIENTED XML INFORMATION EXCHANGE DATA MODEL,"FFI/NOTAT-2006/03599, Nov.2006.

[30] ROSE Kjell, "BINÆRKODING AV XML-DOKUMENTER - En innledende undersøkelse,"FFI/NOTAT-2006/02474, Aug.2006.

[31] EGGEN Anders, ANDREASSEN Morten, GEORGEL Dominique, HEDENSTAD Ole-Erik, HAAKSETH Raymond, JAMET Herve, LANGMYR Anders, MALOWIDZKI Marek, RASMUSSEN Rolf, SASSUS Pierre, and SLETTEN Geir, "The NATO RTO/IST-061 Secure SOA Demonstrator Specification for CWID 2006 (Version 2),"FFI/RAPPORT-2006/03921, 2006.

[32] NATO RTO IST-061, "TERMS OF REFERENCE - Secure Service Oriented Architectures (SOA) supporting Network Enabled Capabilities,"2005.

[33] NATO RTO IST-061, "Secure Service Oriented Architectures (SOA) supporting NEC,"2006.

[34] OLAFSEN Runar, "Situation awareness, the abstraction hierarchy and the design of user interfaces of command and control decision support systems," Proceedings of the Second Human Performance, Situation Awareness and Automation Conference (HPSAA II), Daytona Beach, 2004.

[35] OLAFSEN Runar, "HPSAA II, DAYTONA BEACH, USA, 22. - 25. MARS,"FFI/REISERAPPORT-2004/02230, June2004.

[36] GAGNES Tommy, BRÅTHEN Karsten, HANSEN Bjørn Jervell, MEVASSVIK Ole Martin, and ROSE Kjell, "Peer-to-Peer Technology – An Enabler for Command and Control Information Systems in a Network Based Defence?," Proceedings of the 9th Command and Control Research and Technology Symposium, San Diego, 2004.

[37] GAGNES Tommy and AAS Johan, "INNTRYKK FRA COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM 2004,"FFI/REISERAPPORT-2004/02552, July2004.

[38] REITAN Bård K and GAGNES Tommy, "9TH ICCRTS - THE NINTH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM,"FFI/REISERAPPORT-2004/03691, 2004.

[39] HAFNOR Hilde and NORMARK Runar, "Ad hoc Organization of Distributed Picture Compilation and Support for Situation Awareness in Network Based Defence – An Exploratory Experiment," Proceedings of the 10th International Command and Control Research and Technology Symposium, McLean VA, 2005.

[40] HAFNOR Hilde, BJØRNSTAD Anne Lise, REITAN Bård K, HALAAS Lasse, and ARNEBERG Gunnar, "2005 ICCRTS - 10th INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM,"FFI/REISERAPPORT-2005/02756, July2005.

[41] GAGNES Tommy, PLAGEMANN T, and MUNTHE-KAAS E, "Discovering Semantic Web Services in Dynamic Environments," Third IEEE European Conference on Web Services (ECOWS 2005): http://wscc.info/p51561/files/paper61.pdf, 2005.

[42] GAGNES Tommy, "EUROPEAN CONFERENCE ON WEB SERVICES 2005 OG CEPA6/CIG6 TECHNICAL WORKSHOP ON SEMANTIC INTEROPERABILITY,"FFI/REISERAPPORT-2005/03987, 2005.

[43] GAGNES Tommy, PLAGEMANN T, and MUNTHE-KAAS E, "A Conceptual Service Discovery Architecture for Semantic Web Services in Dynamic Environments," IEEE Computer Society, Proceedings of the 22nd International Conference on Data Engineering Workshops (ICDEW'06), 2006.

[44] EGGEN Anders, "Security in Service Oriented Architectures (SOA) - A Network Enabled Capability (NEC) Perspective," Information Assurance for Defence: https://kb.iqpc.co.uk/events/2694/topic/1, 2006.

[45] RASMUSSEN Rolf E, EGGEN Anders, and HAAKSETH Raymond, "An architecture for experimenting with secure and dynamic Web Services," Proceedings of the 11th Command and Control Research and Technology Symposium, San Diego, USA, 2006.

[46] RASMUSSEN Rolf, "2006 CCRTS - COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM ,"FFI/REISERAPPORT-2006/02713, Sept.2006.

[47] HAAKSETH Raymond, HADZIC Dinko, LUND Ketil, EGGEN Anders, and RASMUSSEN Rolf E, "Experiences from implementing dynamic and secure Web Services," Proceedings of the 11th International Command and Control Research and Technology Symposium, Cambridge UK, 2006.

[48] HAAKSETH Raymond and HADZIC Dinko, "11TH ICCRTS - INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM,"FFI/REISERAPPORT-2006/03961, Dec.2006.

[49] HEDENSTAD Ole-Erik, GAGNES Tommy, BENTSTUEN Ole Ingar, HAFNOR Hilde, EGGEN Anders, GJERTSEN Tor, and ØVREÅS Torunn, "SAMMENDRAG AV DE VIKTIGSTE TEKNOLOGISKE TRENDER INNEN IKT,"FFI 06.10.2006, Oct.2006.

[50] HEDENSTAD Ole-Erik, GAGNES Tommy, BENTSTUEN Ole Ingar, HAFNOR Hilde, EGGEN Anders, GJERTSEN Tor, and ØVREÅS Torunn, "SAMMENDRAG AV DE VIKTIGSTE ANVENDELSESTRENDER INNEN IKT,"FFI 06.10.2006, Oct.2006.