FFI RAPPORT

INI SOM NETTSENTRISK VIRKSOMHETSOMGIVELSE - BRUK AV "ENTERPRISE METADATA" OG "COMMUNITIES OF INTEREST" (COIs)

HAFNOR Hilde

FFI/RAPPORT-2006/00862

INI SOM NETTSENTRISK VIRKSOMHETSOMGIVELSE - BRUK AV "ENTERPRISE METADATA" OG "COMMUNITIES OF INTEREST" (COIs)

HAFNOR Hilde

FFI/RAPPORT-2006/00862

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
Postboks 25, 2027 Kjeller, Norge

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
NO-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2006/00862	UNCLASSIFIED	41
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFI-II/898/912	-	

4) TITLE

INI SOM NETTSENTRISK VIRKSOMHETSOMGIVELSE - BRUK AV "ENTERPRISE METADATA" OG "COMMUNITIES OF INTEREST" (COIs)

BECOMING NET-CENTRIC - USE OF ENTERPRISE METADATA AND COMMUNITIES OF INTEREST (COIs)

5) NAMES OF AUTHOR(S) IN FULL (surname first)

HAFNOR Hilde

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Net-Centric	a) Nettsentrisk
b) Communities Of Interest	b) Interessefellesskap
c) Metadata	c) Metadata
d) Information sharing	d) Informasjonsdeling
e) Netbased collaboration	e) Nettbasert samarbeid

THESAURUS REFERENCE:

8) ABSTRACT

Net-centricity is an approach that provides users the ability to access applications and services that make sense to them through a web-enabled space, while simultaneously moving toward a web-enabled user community in which each member can both provide and access data. Net-centricity makes it possible to move beyond traditional communities of interest (COIs), such as command and control or intelligence, to full cross-functional information exchange across the battlespace.

Today Net-centric processes are emerging, being discovered, and are actively developed by industry, universities and the military Services (US and NATO). As Net-Centric technology is becoming more reliable and trusted, military culture is adapting to more intensive use of its expanded capabilities.

This report explores the term Net-centricity and the use of COIs and Enterprise Metadata as pivotal mechanisms in the military effort of becoming net-centric.

9) DATE	AUTHORIZED BY	POSITION
	This page only	
2006-03-15	Vidar S Andersen	Director

ISBN 82-464-0998-0

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

INNHOLD

APPENDIKS

INI SOM NETTSENTRISK VIRKSOMHETSOMGIVELSE - BRUK AV "ENTERPRISE METADATA" OG "COMMUNITIES OF INTEREST" (COIs)

1 INNLEDNING

En sentral oppgave i prosjekt 898 NBF Beslutningsstøtte er å se på grunnleggende elementer i tjenesteinfrastrukturen i et fremtidig nettverksbasert forsvar (NBF). En del av denne oppgaven består i å foreslå en strategi for hvordan metadata (”data om data”) kan brukes for publisering og gjenfinning av informasjonsressurser i Forsvarets informasjonsinfrastruktur (INI).

Ifm Forsvarsdepartementets (FD) planarbeid innenfor programområdet INI utarbeidet prosjektet høsten 2005 en rapport ”Operative Beslutningsstøttetjenester – Fremtid NBF” (1) som beskriver en teknologisk fremtidsvisjon for 2014+, samt en løsning for 2008 som et skritt på veien. I 2014+-perspektivet ser man for seg tjenesteinfrastrukturdelen av INI realisert som en sikker og dynamisk tjenesteorientert arkitektur basert på åpne standarder. Anbefalingene i rapporten begrunnes i Forsvarets behov for transformasjon av dagens løsninger slik at informasjon (strukturert og ustrukturert) i fremtiden kan deles mellom langt flere enheter enn i dag. Rapporten inngikk som en del av prosjektets aktivitet rundt anbefalinger av COTS-teknologier og åpne standarder, som er den andre hovedaktiviteten innenfor prosjektets oppgave ifm grunnleggende elementer i tjenesteinfrastrukturen.

Samtidig har det vært et pågående arbeid i NATO NEC (3) som beskriver en fremtidig nettsentrisk datastrategi som har som hensikt å støtte nettsentriske operasjoner. NATO-arbeidet har tatt utgangspunkt i amerikanernes ”Net-Centric Data Strategy” (2) hvor de beskriver sin visjon for håndtering og styring av informasjonsressurser ”Enterprise Wide” i Global Information Grid (GIG). Det som driver dette arbeidet er målet om økt tilgang til, og deling av, informasjonsressurser hvor metadata og ”Communities Of Interest” (COIs) inngår som sentrale begreper og betraktes som forutsetninger for realisering. COIs introduseres som et generelt begrep for å beskrive samarbeidskonstruksjoner som et essensielt virkemiddel for måloppnåelse.

Såkalte ”Enterprise Metadata” og organisering rundt virtuelle informasjonsrom (COIs) utgjør kjernen i det som vi videre i rapporten omtaler som nettsentrisk tilnærming til ”Information management” eller på norsk: Nettsentrisk informasjonsstyring. En nettsentrisk metadatastrategi vil være et viktig verktøy i denne prosessen. Visjonen er at når en slik strategi på sikt er fullt operativ vil man ha en kraftfull *virtuell* informasjonsnettverksomgivelse som effektivt støtter nettbasert tilgang og deling av informasjonsressurser på tvers av organisatoriske grenser og nivåer.

Målsettingen med prosjektets strategiarbeid er å beskrive tilnærminger/løsningskonsepter som muliggjør tilgang til informasjonsressurser i Forsvarets nettverksbaserte beslutningsstøtte-tjenester - i henhold til sentrale NBF-ideer. Strategien vil skissere løsningskonsepter/-tilnærminger på overordnet nivå - altså ingen implementasjonsguide.

Det er planlagt to hovedleveranser ifm metadatastrategiarbeidet:

- Foreslå en nettsentrisk metadatastrategi med fokus på *operativ virksomhet* som FD kan ta videre (FFI-Rapport).
- Peke på utfordringer ved realisering av en slik strategi, gjeldende forutsetninger og utfordringer ved implementasjon (FFI-Rapport).

Arbeidet med prosjektets metadatastrategi startet opp høsten 2005 og frem til nå har arbeidet omfattet fordypning i sentrale begreper, hva som skal inngå i en metadatastrategi, samt hvorfor vi trenger en slik strategi. Mye av dette forarbeidet baserer seg på arbeidene i (2) og (3) samt den 2014+-visjonen prosjektet skisserte i (1).

Slik vi vurderer det så er arbeidene gjort i (2) og spesielt i NATO NEC (3) i tråd med hva vi mener er en farbar vei å gå ut fra hvordan vi vurderer teknologiutviklingen i et 10-års perspektiv (1). Vi har derfor ikke til hensikt å ”finne opp hjulet på nytt” og foreslå en helt annen type datastrategi enn det som er allerede er skissert i USA og NATO, men har heller som mål å ta utgangspunkt i det som foreligger og ytterligere konkretisere og tilpasse det til norske forhold.

I denne rapporten oppsummeres deler av forarbeidet gjort høsten 2005. Rapporten har først og fremst som hensikt å utdype noen sentrale begreper og prinsipper for nettsentrisk tenkning, søkt forklart på en slik måte at man ikke skal behøve å være en fullbefaren teknologiekspert for å kunne lese og forstå hovedessensen i det som presenteres i rapporten. Tanken er at dette kan danne et utgangspunkt for å oppnå prinsipiell enighet om begreper og felles forståelse utover det rent teknologiske. Videre søker rapporten å legge til grunn et mer helhetlig syn på *hvorfor* vi (i et NBF) trenger en slik strategi (dvs hva som motiverer for dette).

Til sist har rapporten som ambisjon å få frem et vesentlig budskap: Hvorvidt en eventuell implementasjon av denne type metadatastrategi blir vellykket eller ei, avhenger veldig mye av organisatorisk vilje og evne til å etablere en ny type brukeratferd (sentrert rundt COIs) som på sikt skal kunne evne å utnytte teknologien på en effektiv og god måte. Veien mot nettsentrisk organisering (både teknologisk og organisatorisk) er en evolusjonær prosess som tar lang tid og kan ikke systemutvikles eller organisasjonsdesignes på tradisjonell måte. Derfor er store deler av det som presenteres her forsøkt belyst ut fra hvordan brukere og organisasjon berøres av dette.

Rapporten skal ikke betraktes som en ”oppskrift” på hvordan man skal organisere seg, men skal heller oppfattes som en introduksjon til nettsentrisk tenkning og nye forståelsesmodeller, muliggjort av dagens IKT-utvikling. Rapporten er derfor på ingen måte uttømmende.

Rapporten er videre inndelt som følger: I kapittel 2 introduseres begrepet ”Net-Centricity” hvor det i korte trekk beskrives hva som ligger i begrepet, og hvorfor en slik type tenkning bør ses i sammenheng med NBF. I kapittel 3 skisseres kort visjonen for nettsentrisk datastrategi slik den er beskrevet i NATO NEC (3). Videre beskrives fenomenet ”Communities Of Interest” i mer detalj i kapittel 4. ”Enterprise Metadata” introduseres i kapittel 5, og noen sentrale elementer som vil inngå i en metadatastrategi presenteres i kapittel 6. Kapittel 7 omtaler kort noen sentrale utfordringer knyttet til realisering av en nettsentrisk metadatastrategi. Til sist blir det en oppsummering og konklusjon i kapittel 8.

2 ”NET-CENTRICITY”

Innledningsvis kan man litt enkelt si at ideen til å tenke i retning av nettsentrisk løsninger (både på teknologisk og organisatorisk plan) er særlig begrunnet i de generelle samfunnstrender som har vært tydelige en god stund allerede:

- Krav om økt tilgang til informasjon
- Krav om økt tilgjengelighet - for andre - av informasjon
- Informasjon etterspørres over organisatoriske grenser og landegrenser

Sett fra et teknologisk perspektiv er det populære engelske begrepet ”Net-Centricity” den generelle forestillingen om å transformere storskala intranett til å bli kapabilitetsbaserte, tjenesteorienterte arkitekturer (Service Oriented Architecture eller SOA), som muliggjør et nytt informasjonsstyringskonsept. Her omtalt som *nettsentrisk informasjonsstyring*. Et styrings-konsept som dreier seg mindre om sentralisert informasjonsstyring men mer om å muliggjøre fleksibilitet, hurtighet, dynamisk organisering av kapabiliteter og tjenester, i nær sanntid, for å oppnå ønsket effekt og resultat.

Sett fra brukerens og organisasjonens perspektiv er ”Net-Centricity” ideen om at eksisterende og fremtidige IKT-systemer innenfor en organisasjon skal konstrueres til å bli en ”helhetlig og sømløs” informasjons- og tjenestetilbyder innenfor en strategisk omgivelse, som tillater praktisk talt alle ansatte (og datarelaterte applikasjoner) hurtig oppdagelse av (”discover”), tilgang til og bruk av organisasjonens informasjonsressurser. ”Net-Centricity” sett fra dette perspektivet innebærer kort sagt å bryte ned ikke bare teknologiske ”stovepipes” men også organisatoriske ”stovepipes”. Dette for å tilrettelegge for dynamisk tilgang og deling av informasjon på tvers av teknologiske og organisatoriske grenser (både vertikalt og horisontalt), basert på moderne nettverksøkonomiske prinsipper for selvorganisering og elektronisk markedsstyring (jfr kapittel 4.6).

I militære sammenhenger ønsker man å skape en ekvivalens til dette for bedre å kunne legge til rette for transformasjonen mot et effektivt NBF.

2.1 Nettsentriske teknologier

I (1) beskrives en teknologivisjon for 2014+. Der blir det spesielt lagt vekt på bruk av en tjenesteorientert arkitektur (SOA) basert på åpne standarder (Web Services og XML) samt fleksibel sikkerhet på informasjonsnivå. Disse tre elementene vurderes som viktige grunnforutsetninger for å komme et skritt videre i å få realisert INI til å bli en reell nettsentrisk omgivelse. Først og fremst fordi:

- Ved å realisere INI som en tjenesteorientert arkitektur vil man kunne få til at militære informasjonsressurser tilgjengeliggjøres som tjenester man faktisk kan aksessere gjennom nettverket. F eks kan en UAV betraktes som en militær informasjonsressurs som kan tilgjengeliggjøres som en tjeneste i nettverket. På denne måten kan brukere koble seg opp til UAVen direkte gjennom nettet.

- Web Services (inklusive semantiske teknologier) er en implementeringsteknikk som forener fremhenting og organisering av informasjon fra ulike systemer ved hjelp av felles forståelse av XML-basert meldingsutveksling. Dette er teknologier som mer og mer glir over på brukernes premisser.
- Bruk av sikkerhetsmerker, digitale signaturer og streng aksesskontroll basert på brukerens aksessprivilegier vil gi en mer dynamisk sikkerhetsløsning hvor brukerens aksessprivilegier styrer tilgangen til informasjonsressursene og ikke hvilke nettverk eller system man er knyttet til. Dette er avgjørende for hvorvidt man klarer å realisere ønsket fleksibilitet i informasjonsressurstilgangen eller ei (f eks å inkludere uforutsette brukere). Sikkerheten må håndteres som en del av SOA design, og ikke gjennom egne sikkerhetsarkitekturer.

Disse basisteknologiene er muliggjørende i sin karakter. Bruk av ”Enterprise Metadata” betraktes som en forutsetning for å få realisert økt fleksibilitet i tilgangen til, og gjenfinning av informasjon på tvers.

2.2 INI som nettsentrisk omgivelse

”Nettsentrisk” blir i kommersielle sammenhenger beskrevet som ”En løsning som er tilgjengelig via Internett”. Dette er en ganske brukbar beskrivelse dersom man sammenlikner INI med et slags internett, og det kan man som *bruker* godt gjøre. For en bruker vil INI først og fremst være en nettverksomgivelse som på en enkel og fleksibel måte skal tilby informasjonsressurser ”sømløst” (som tjenester) gjennom nettverket. I dag har Forsvarets INI en lav grad av å være en nettsentrisk omgivelse fordi man har relativt få ressurser som er tilgjengeliggjort gjennom nettverket. Likefullt opererer man 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.

Denne visjonen beskriver faktisk INI som en nettsentrisk omgivelse. Dvs en omgivelse hvor nettbasert tilgang og deling av informasjon gjennom hele nettverket er blitt en mulighet, samt det muliggjørende aspektet som inkluderer mennesker, prosesser og organisasjon.

Gitt de grunnteknologiene nevnt i kapittel 2.1 (transformere INI til å bli en kapabilitetsbasert, tjenesteorientert arkitektur) sammen med bruk av ”Enterprise Metadata” og etableringen av COIs, vil en ha mulighet til å komme nærmere denne visjonen.

Bruk av ”Enterprise Metadata” og COIs berører mennesker og organisasjon. COIs er, som tidligere nevnt, en konstruksjon for deling av informasjonsressurser gjennom nettverket (nettbasert samarbeid), og ”Enterprise Metadata” er en mekanisme for at brukere skal kunne oppdage og finne disse ressursene på tvers gjennom hele virksomheten. En datastrategi, basert på metadata og COIs, vil da være verktøyet man bruker for å kunne være i stand til å fokusere på deling av informasjonsressurser på en *strukturert* måte.

En (meta)datastrategi befatter seg altså ikke med operative behov i vanlig forstand – men heller med *hvordan* man skal få tilrettelagt organisasjonsprosesser, informasjonsressurser og teknologiske løsninger for å få realisert økt tilgang og deling der man trenger det - og når man trenger det (uansett behov, geografisk/organisatorisk ståsted og tid). Dette skal til sammen bidra til å skape en militær "nettverksomgivelse" som inkluderer mennesker, teknologi og prosesser. Målet er at når en slik strategi er fullt operativ vil man ha en *virtuell* nettverksomgivelse som effektivt støtter tilgang og deling av informasjonsressurser på tvers av organisatoriske grenser og nivåer, samt en mer effektiv måte å håndtere organisasjonens informasjonsressurser på.

2.3 Samarbeid og deling av informasjon i NBF

Visjonen om INI som muliggjørende og "helhetlig og sømløs" informasjons- og tjenestetilbyder, samt fokuset på ønsket om økt samarbeid (på tvers) i militære operasjoner, aktualiserer behovet for denne type nettsentrisk tenkning i NBF.

I sum kan man si at målet med NBF er å oppnå informasjonsoverlegenhet for å kunne gjøre gode og effektive beslutninger. Følgende kortversjon kan oppsummere essensen i de mest sentrale NBF-visjonene:

- Bedre *situasjonsbevissthet* gjennom utbredt *deling av informasjon* i nettverk på tvers
- Bedre *samvirke* av styrker på grunnlag av felles situasjonsbevissthet
- Økt evne til "Selvsynkronisering/selvorganisering"

En sentral forutsetning for å komme et skritt nærmere disse visjonene er å øke *samarbeid* på tvers av militærorganisatoriske grenser, fagdisipliner, forsvarsgrener og nivåer. Samarbeid forutsetter tilgang til og deling av informasjon. Skal man kunne evne å oppnå økt samvirke (interaksjon/samarbeid) innenfor og mellom styrkeelementer trenger man både *vilje* og *evne* til deling av informasjon.

Med *vilje* menes at man har arbeidspraksiser (kultur) hvor det er naturlig å dele informasjon i stedet for å holde informasjon for seg selv. Med *evne* menes her to ting: Først og fremst at man faktisk har reelle teknologiske muligheter for økt deling av informasjon (dvs interoperabilitet og tilgjengelighet), men også at organisatoriske strukturelle elementer som f eks at militært regelverk faktisk tillater økt deling av informasjon. Det er et faktum at dagens regelbaserte sikkerhetspolicy ikke tillater mye deling av informasjon, mens en noe mer risikobasert sikkerhetspolicy vil kunne øke den muligheten (1). Dagens interoperabilitetsproblemer og "stove pipe" systemer (arven) er i så måte også mye en konsekvens og refleksjon av tidligere tiders manglende militær vilje og evne til deling av informasjon.

Når man nå ønsker å endre denne viljen og evnen i militær virksomhet, opplever man kanskje ikke bare motstand i organisasjonens regelverk, policies og mennesker (som man faktisk forventer), men også at teknologien ofte står "i veien" og bidrar til å hindre en utvikling i den retning man ønsker[1]. Teknologien sementerer status quo isteden for å være den ønskede

[1] F eks at det oppstår en "lock-in" situasjon (innelåsningseffekt). D v s når det som i økonomien omtales som "switching cost" (kostnader knyttet til det å bytte teknologi) blir for høye. Lock-in situasjoner kan oppstå både på teknologisk og økonomisk nivå, samt på brukernivå.

fasilitator og katalysator for endring. Spørsmålet blir da: Hvordan kan man gjennom teknologiske løsninger støtte opp under og fremme ønsket om en militær atferd preget av både evne og vilje til økt samarbeid og deling av informasjon? Mao: Hvordan gjøre INI mer muliggjørende for militær virksomhet? Hvordan realisere en gjennomgripende teknologisk støtte (INI) for samarbeid og deling av informasjon på tvers av våpengrener, forsvarsgrener og tradisjonelle kommandonivåer?

Ut fra et teknologisk ståsted ser man nå en mulighet for å komme et skritt videre på denne veien:

- Transformere INI til å bli en kapabilitetsbasert, tjenesteorientert arkitektur.
- Etablere COIs (som gir støtte til nettbasert samarbeid mellom mennesker på tvers).
- Bruk av ”Enterprise Metadata” for at brukere skal kunne oppdage og finne relevante ressursene på tvers gjennom hele INI.
- En mer dynamisk sikkerhetsløsning for å oppnå ønsket fleksibilitet i informasjonsressurs-tilgangen. Overgangen til en mer risikobasert sikkerhetspolicy vil stå sentralt her.

3 NETTSENTRISK (”ENTERPRISE”) DATAVISJON

I dagens militærteknologiske IKT-virkelighet sliter man med en del problemer. Det gjelder velkjente ting som f eks den fortsatt store mangelen på interoperabilitet, mangfoldet i dataformater og operativ fragmentering og segmentering av informasjon (etter type, klassifikasjon, kommando, ”mission”, osv). Ved søk etter informasjon finner man enten ingen ting eller alt for mye. Og finner man noe er det ofte slik at man ikke forstår den informasjonen man fant. Ofte er informasjon skjult i proprietære formater i ikke-tilgjengelige systemer, eller informasjonen ligger i åpne formater men er ikke tilgjengelig pga sikkerhetsregler (nivåer), brannmurer, ikke tilkoblete systemer, ikke sammenkoblete kommunikasjonssystemer, osv.

Man sliter også med det man kan kalle for IKT-politiske problemstillinger knyttet til eierskap og bruk av ulike miljøbundne systemer. Dette er miljøer, som gjennom ”sine” systemer, eier alle informasjonsressursene knyttet til systemet. I slike systemer er det ofte lagt ned mye arbeid og prestisje (ofte over flere år) som nå kommer i konflikt med hva organisasjonen for øvrig trenger.

Selv om man i dag har mye ny og moderne informasjonsteknologi tilgjengelig (f eks: disker med fellesområder for dokumentlagring, felles web-sites i mange fasonger, intranett- og internettilgang, moderniserte K2-systemer (f eks NORCCIS), mailsystemer, moderne søkeverktøy, osv) har ikke problemene blitt særlig mindre. De har heller eskalert i omfang.

3.1 Fra prosessorientering til dataorientering

For å imøtekomme noen av disse problemene trenger vi en strategi for å håndtere dette bedre i fremtiden. En datastrategi som representerer et skifte fra “prosessorientering” til “data-orientering”. 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: Skille informasjonsressursene fra systemene.

Hensikten bak en slik tankegang i en militær kontekst er å muliggjøre effektive beslutninger i militære operasjoner gjennom å gjøre dataressurser (informasjon og tjenester) s*ynlig*, *tilgjengelig* og *anvendelig* når og hvor aktører (mennesker og applikasjoner) i nettverket skulle trenge det, inkludert ”uventede” aktører. Samt å bedre interoperabilitet mellom ulike system i Forsvarets organisasjon på tvers av militære faggrener og nivåer, med andre nasjonale enheter, f eks politi, toll og fiskerimyndigheter (”Joint National Interoperability”) og med andre nasjoner og alliansepartnere (”Coalition Interoperability”).

Følgende punkter oppsummerer kort datavisjonen for en militær nettsentrisk omgivelse slik den blir skissert i NATO NEC (3):

- Målet er å populere hele nettverket med alle typer av data/informasjonsressurser (etterretningsmessige og ikke-etterretningsmessige data, rådata og prosesserte data). Dette tvinger frem et paradigmeskifte fra: ”Process, exploit and disseminate” (standardisering og punkt-til-punkt grensesnitt) til ”post before processing” (hvor prosessering blir gjort i brukerapplikasjonsomgivelsen). Autoriserte brukere og applikasjoner skal ha umiddelbar tilgang til data som er postet i nettverket uten ”Process, exploit and disseminate”-forsinkelser.
- Kjernen i en dataorientert strategi er dataene. *Data* i denne konteksten betyr praktisk talt alt av hva man har av *nettbaserte* informasjonsressurser av typen tjenester/systemer/-applikasjoner, systemfiler, databaser, dokumenter, bilder, lydfiler, web-sites, osv. Med tjenester menes også militære ressurser som er tilgjengeliggjort som tjenester og som kan aksesseres gjennom nettverket. Informasjonsressurser, dataressurser og data er begreper som i denne konteksten (og i denne rapporten) betyr det samme.
- Alle dataressurser skal gjøres synlig, tilgjengelig og anvendelig når og hvor aktører (brukere og applikasjoner) i nettverket skulle trenge det (post & pull).
- Brukere (og applikasjoner)[2] må ”tagge” (merke) sine dataressurser med informasjon om dataressursen (metadata) for å muliggjøre oppdaging og gjenfinning av data (”Discovery”), og 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 samt målemetoder.
- Det skal være fleksibel og hurtig tilgang og deling av informasjon på tvers av systemer/tjenester, brukerdomener, dataformater og grensesnitt.

Hovedmålet med en slik visjon er å øke datamengden som blir synlig gjennom hele organisasjonen - ”Enterprise Wide”. Dvs mer ”Enterprise” data, mer COI-data og mye mindre ”private” data[3], samt sikre at data er tilgjengelig og brukbar 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 denne datavisjon baserer seg på tre kjernefaktorer:

---

[2] ”Brukere” i denne konteksten er både mennesker og applikasjoner.
[3] ”Enterprise” data, COI-data og ”private” data utypes videre i kapittel 5.3.

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).
2. *Metadata*, som tilbyr en måte å beskrive dataressurser på samt bruken av metadata- og ”Discovery”-registre samlet i såkalte ”Shared Spaces” (felles informasjonsrom) i nettverket. Metadata introduseres som en forutsetning for å få til målet om ”Discovery” gjennom søk i nettverket. ”Shared Spaces” introduseres som en konstruksjon som muliggjør en distribuert men effektiv og håndterbar organisering av metadata. ”Shared Spaces” er i denne sammenheng tilknyttet COIs.
3. *INI-kjernetjenester (”Core Services”)* som muliggjør data- ”tagging”, -deling, -søking, -lagring og gjenfinning.

Disse tre punktene sammen med båndbredde, sikkerhet og fusjonskapasiteter utgjør nøkkelfaktorene i datavisjonen. Videre i rapporten utdypes hovedsaklig de to første punktene sett ut fra spørsmålene: Hvilke føringer vil realiseringen av en slik tankegang gi på virksomhetsnivå? Hvordan berøres brukere og organisasjon av dette? Hva kreves?

Punkt tre er en forutsetning for de to første. Sammen med sikkerhet er dette punktet tidligere omhandlet i (1).

4 ”COMMUNITIES OF INTEREST” (COIs)

Generelt er COIs et begrep som beskriver enhver samling av mennesker med en erklært felles interesse som har behov for å utveksle informasjon – et såkalt *interessefellesskap*. De er ofte tverrfaglige og er geografisk og organisatorisk uavhengige. COIs er virtuelle samhandlingsarenaer (nettbaserte interessefelleskap) og betraktes derfor av mange for å være et slags ”internettfenomen”. De er ofte løst sammensatt og favner bredt ved at de dekker et stort antall potensielle grupper av ulike typer og størrelser.

4.1 ”Definisjon”

Begrepet COI dukker nå 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[4].

[4] Det betyr ikke at alle prosjekter og arbeidsgrupper nødvendigvis defineres som COIs.

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 (deling av informasjon mellom nasjoner), kommando- og kontroll (K2) eller ifm ikke-operative virksomhetsprosesser av ulike typer (f eks stab/støtte funksjoner).

4.2 COI-medlemsskap

COI-medlemsskap inkluderer mange forskjellige konsumenter og produsenter av informasjon som trenger å dele den samme semantiske kunnskapen. Det være seg vanlige brukere, domene eksperter, systemutviklere, mfl. COI-deltagere kan også representere organisasjoner utenfor den militære organisasjonen (f eks innenfor værvarsling). I en nettsentrisk omgivelse er alle både konsumenter og produsenter av informasjonsressurser.

Det er meningsløst å danne COIs som ingen eller bare noen få er medlem av. Ideen er at alle brukere i organisasjonen skal være medlem av en eller flere COIs, basert på arbeidsoppgaver og behov. Det er ingen begrensning på antall medlemmer i en COI, eller antall COIs man kan være medlem av. En COI skal ha frihet til selv å kunne definere hensiktsmessige mekanismer for håndtering av COI-medlemsskap.

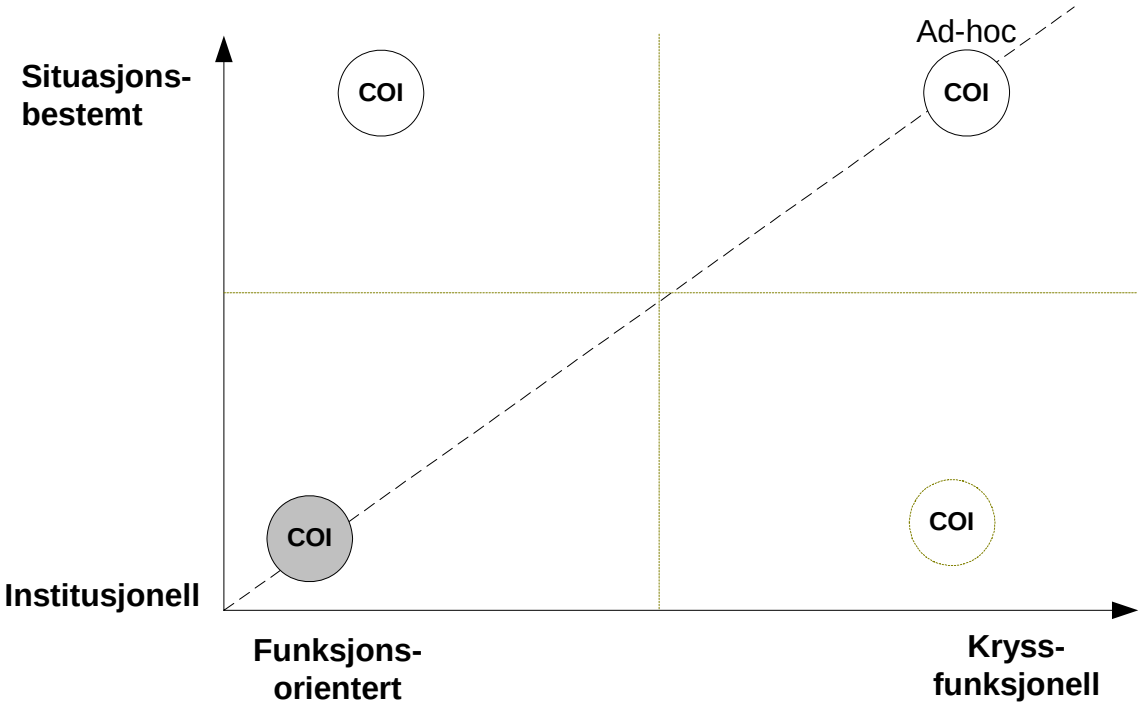
Et COI-medlemsskap kan være frivillig eller obligatorisk avhengig av hvilke roller deltagerne har. En deltagers engasjement kan også endres gjennom livssyklusen til en COI. F eks ved dannelsen av en COI vil typisk initiell medlemsmasse inkludere ledere fra ulike deler av Forsvaret, men etter hvert som innsatsen i fellesskapet utvikler seg fra planleggingsstadiet til å ha et mer faglig fokus vil medlemsmassen kanskje heller kreve en større fagmessig eller funksjonell representasjon. Og hvis du f eks mener at din COI vil påvirke sentrale anskaffelses-prosesser, da bør respektive anskaffelsesorganisasjoner bli oppmuntret til å knytte seg opp og delta i fellesskapet.

COIs skal selv ha frihet og fleksibilitet til å engasjere en rekke deltagere i forskjellige tidsintervaller gjennom hele livssyklusen for å sikre at brukerbehovene til enhver tid er tilfredsstillende ivaretatt.

4.3 Typer av COIs

COIs kan fremvise en rekke karakteristikker avhengig av interessefellesskapets mål eller oppgaver og oppdrag. I figur 4.1 nedenfor illustreres de mest alminnelig COI-typene, som gjennom begrepene situasjonsbestemt, institusjonell, funksjonsorientert, kryssfunksjonell (3) brukes for å karakterisere COIs.

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 planleggings-scenarier. Eller en COI som opprettes i forbindelse med et spesifikt oppdrag. For at en



Figur 4.1 En COI kan være institusjonell (fast) eller dannes mer spontant (ad hoc)

situasjonsbestemt COI skal kunne dannes og være ”operativ” relativt raskt (f eks ifm 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 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.

Nettsentrisk tilnærming tillater oss å gå utover ”tradisjonelle” COIs, som f eks kommando og kontroll eller etterretning, til full kryssfunksjonell informasjonsdeling på tvers

En annen måte å karakterisere COIs på er gjennom *varigheten* av dataressursene eller aktiviteten som foregår. Noen COIs innehar bare noen få samarbeidssesjoner for å fullføre det de skal, mens andre COIs kan bestå i årevis fordi det vil være et kontinuerlig behov for disse. Det er opp til fellesskapet eller ”tasking authority” å bestemme hvor lenge en COI skal vare.

I figur 4.2 og 4.3 nedenfor illustreres hva som kan være eksempler på COIs i nasjonal og internasjonal sammenheng.

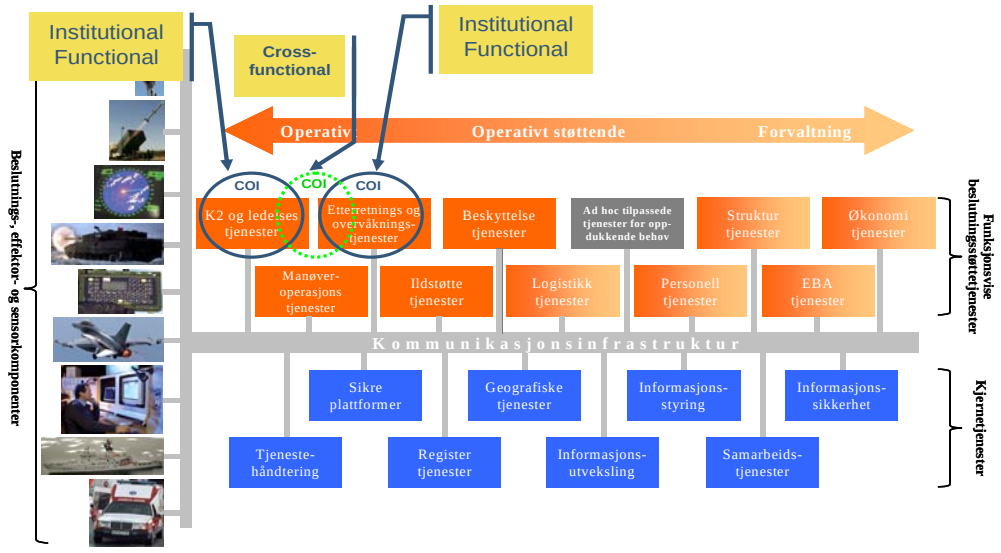


Figure 4.2 Eksempel 1: Forsvarsdepartementets (FD) referansemodell (1)

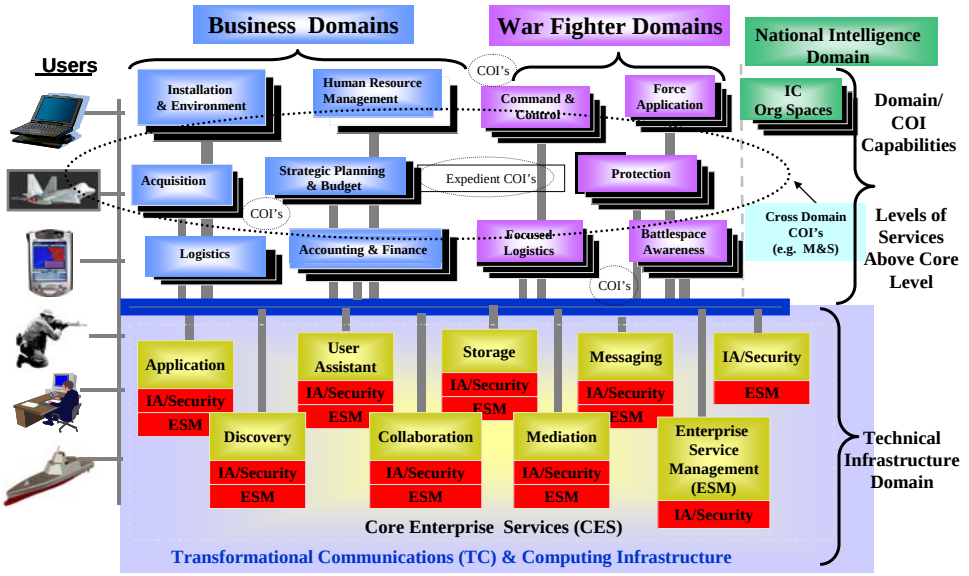


Figure 4.3 Eksempel 2: NATOs Enterprise Servise Strategy (NOSWG)(9)

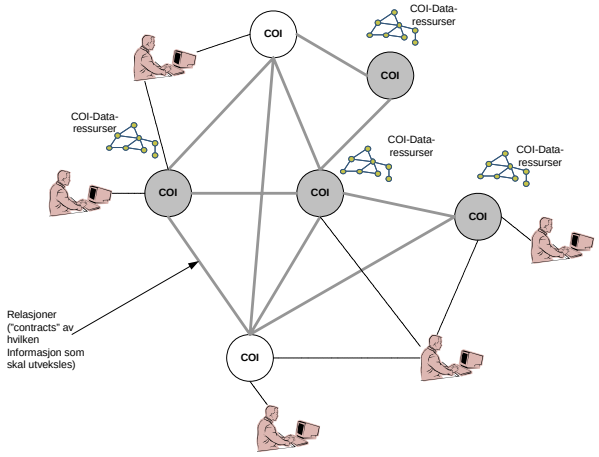
COI er en konstruksjon for deling av dataressurser	
Institusjonelle COIs: Ansvar for utvikling av vokabularer, datamodeller, registrering av metadata-skjemaer, identifisere/utvikle andre datarelaterte ressurser, mm.	**Funksjonelle COIs:** Involverer aktører innenfor et funksjonsområde
Situasjonsbestemte COIs: Utnytter eksisterende ressurser i nettverket (vokabularer, applika-sjoner, mm).	**Kryssfunksjonelle COIs:** Involverer aktører fra ulike funksjons-områder
Varighet: Noen COIs kan eksistere over lang tid, andre kun over noen samarbeidssesjoner.	

4.4 'Dannelse av COIs

COIs dannes på flere forskjellige måter og kan være sammensatt av deltakere som representerer en bestemt funksjon eller bestå av representanter på tvers av funksjoner.

De første COIs man starter med å etablere er gjerne de institusjonelle og ofte funksjons-orienterte. De er som regel top-down drevet og er de som blir bærebjelkene for den initielle organisering og oppbygging av informasjonsressursene i organisasjonen. Disse er som regel få i antall. De initielle COIs vil typisk struktureres iht organisasjonens eksisterende topologi – enten det dreier seg om avgrensede funksjonsområder eller allerede etablerte samarbeidsoppgaver på tvers av funksjonsområder (kryssfunksjonelle). Etter som tiden går vil disse COIene kunne tilgjengeliggjøre sine informasjonsressurser gjennom nettverket. Det å stimulere til denne type metadatabasert samarbeid vil kunne lede til at man lettere oppdager potensielle samarbeids-partnere og videre lede til dannelsen av mer situasjonsbestemte COIs (funksjonelle eller kryss-funksjonelle) basert på ressursene i de allerede eksisterende COIs. Ettersom tiden igjen går (organisasjonens COI-modenhetsgrad øker) vil man raskere og raskere kunne være i stand til å etablere behovsdrevne COIs f eks til bruk i f m tidskritiske ad hoc oppdrag eller til samarbeid av mer uformell karakter. Noen av disse kan dannes top-down, andre kan dannes bottom-up (det siste kan være typisk for dannelser av såkalte uformelle COIs men ikke nødvendigvis).

Situasjonsbestemte COIs vil etter hvert kunne bli ganske mange i antall, hvor noen etter hvert kanskje går over til å bli mer institusjonelle fordi det viser seg at de er av mer varig verdi, eller de avsluttes og nye oppstår. Etter hvert som all militær virksomhet blir COI-basert (virtuelt nettverk av COIs) vil organisasjonen ha bedre evne og fleksibilitet i teknologistøtte for samarbeid og dermed lettere kunne imøtekomme organisasjonens foranderlighet m h t uforut-sette krav og endringer i behov (det er i hvertfall visjonen). Det er nettopp dette som i datavisjonen i (2) og (3) blir omtalt som en virtuell informasjonsnettverksomgivelse.



Figur 4.4 Eksempel på nettverk av COIs

Figur 4.4 ovenfor viser et eksempel på nettverk av COIs hvor noen COIs (typisk institusjonelle – skravert i grått) har bygd opp COI-spesifikke dataressurser og datamodeller mens andre (hvite) utnytter eksisterende ressurser i nettverket (typisk situasjonsbestemte). Eksempelet viser også at brukere kan være tilknyttet en eller flere COIs. Relasjonene mellom COIene er etablerte forbindelser (”kontrakter”) mellom COIs mht hvilken type informasjon som skal utveksles.

Disse relasjonene vil kunne beskrives og bli redegjort for. Man kan f eks tenke seg et nettverksperspektiv i arkitekturdesign hvor organisasjonen fremstilles som et (komplekst) sett av *relasjoner* som tillater å bli ledet, redegjort for, visualisert, forespørret og lett navigerbar.

Denne type tenkning legger til rette for alle-til-alle kommunikasjon, men vil i praksis ikke være det.

4.5 Krav til COIs

COIs krever arbeid. COIs utvikles og vedlikeholdes ikke av seg selv. Det er heller ikke forbeholdt noen spesielle organisatoriske miljøer, eksperter eller utpekte dedikerte enkeltpersoner å gjøre det. I et nettsentrisk perspektiv er dette alles ansvar. Som medlem av en COI skal man:

- Selv sørge for å gjøre sine informasjonsressurser synlige, tilgjengelige og forståelige.
- Bidra aktivt i å definere COI-spesifikk vokabular og taksonomier (ontologier) for å få til semantisk og syntaktisk forståelse av informasjonsressursene.
- Registrere semantisk og strukturert metadata

I praksis betyr det at hver enkelt COI (dvs medlemmene) vil ha som oppgave å samle inn, organisere og vedlikeholde data slik at deres datamål oppnås. Dataressursene som COIen innehar skal annonseres (gjennom tagging med metadata og posting til ”shared spaces”) slik at andre COIs kan oppdage disse. For hver COI bør en utvikle COI-spesifikke ontologier som representerer COIens forståelse av informasjonen som skal deles. Ontologier kan bestå av datakategorier, skjema, vokabular, nøkkelord, og taksonomier.

Hver COI vil også ha mulighet til å definere sine spesifikke metadata som er basert på ontologien og som vil fungere som en utvidelse av metadataene som er felles for hele virksomheten[5]. Andre ressurser som f eks mail og kalendersystemer, økonomisystemer, kontorstøttesystemer osv, som er felles for alle betraktes ikke som COI-spesifikke dataressurser. Disse typer ressurser vil være tilgjengelig for alle og ikke bygd opp tilknyttet en spesifikk COI. COIs har kun ansvar for å bygge opp ressurser som er spesifikke for COIen eller er blitt produsert der. For at denne type aktivitet skal slå igjennom og bli en naturlig del av medlemmers gjøremål er det avgjørende at det etableres insentivstrukturer (belønningssystemer) i virksomheten for å fremme denne type atferd. Brukere og systemutviklere skal oppmuntres og anspores til deltagelse. For spesielt interesserte lesere kan man i (6) studere amerikanernes foreløpige draft til implementasjonsguide for COIs (datert november 2005). Der kan man i større detalj lese om hvilke aktiviteter som bør settes i gang for å operasjonalisere COIs, hvem som er nøkkelmedlemmer, osv. I Appendiks A er det gjengitt en oversikt over hvilke roller man ser for seg innenfor en COI. Tabellen er hentet fra (6).

4.6 Nettverk av COIs

Som nevnt tidligere i kapittelet tilbyr COIs virtuelle samhandlingsarenaer for individer med

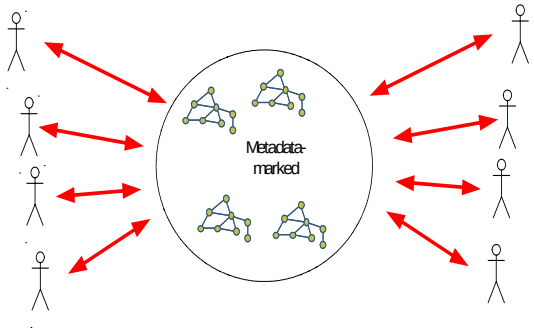
[5] Gjelder først og fremst institusjonelle COIs.

felles interesser hvor man altså deler ideer/informasjon av formell eller uformell, strukturert eller ustrukturert art. Samlet sett vil COIs være en kritisk informasjonsnettverkstopologi som går utover og på tvers av organisatoriske og geografiske grenser. Informasjonen tillates å skaleres globalt og kan lett distribuere og knyttes opp hvor som helst. Høy myndighetsgrad (”selvråderett”) og samarbeid innen hver enkelt COI kan lede til mer selvorganisering og muliggjøre mer automatisert tilpassninger til organisasjonens behov. Med selvråderett ligger det et ansvar og forpliktelse om å ha vilje til å dele informasjon.

Det kreves en ”riktig” implementasjon, ikke bare på teknologisiden men også på organisatorisk nivå, for å få til et godt fungerende nettverk av COIs som skal bidra til oppfylle organisasjonens nettsentriske målsettinger. Fokus på relasjoner mellom COIs blir viktig. Mye av dette krever en endring av atferd og tankesett, både for de som kan teknologien og for alle de som skal nyttiggjøre seg den. Det er vanskelig. Noen ganger kan bruk av analogier være til hjelp til å danne seg bilder i forståelsen:

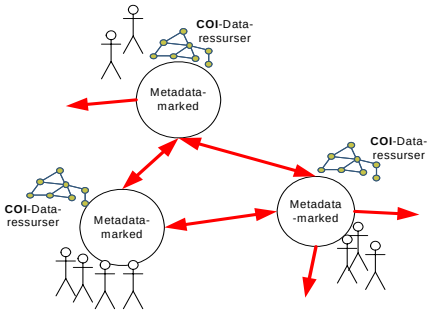
Mange organisasjoner styrer sine dataressurser (som f eks metadata) i store felles datalagre og bruker analogien datamarked, metadatamarkedplasser eller markedsrom. I en slik virtuell verden vil virksomhetsprosessene flyttes til markedsplassen – en markedsplass definert og skapt av informasjonsteknologien. I denne modellen har autonome og anonyme individer interaksjon med hverandre gjennom markedet. Individer og organisasjoner betraktes ikke som å ha interaksjon med hverandre men å ha interaksjon mot det ”mytiske” markedet (figur 4.5). I en slik organisasjon vil synligheten av metadataene være det viktigste.

Organisasjonen som ”Markedsplass”



Figur 4.5 Interaksjonen mot markedsplassen kommer i fokus

Organisasjonen som ”Nettsentrisk”



Figur 4.6 Samarbeid og deling av data mellom mennesker kommer i fokus

Organisasjonen som markedsplass er tuftet på standard økonomisk tenkning. Ideen om bruk av COIs derimot, er fundert på nettverksøkonomiske prinsipper. I nettverksøkonomien står relasjoner sentralt[6]. I et nettsentrisk perspektiv er metadatamarkedet et nettverk av COIs som etablerer relasjoner i en slags nettverksøkonomi, hvor de økonomiske fordelene øker med størrelsen (d v s hvor den økonomiske verdien øker med vekst i antall brukere). Denne modellen, i motsetning til standardmodellen, betrakter individer som *partnere* som etablererer *relasjoner* med hverandre. Evnen til å etablere forbindelser med hverandre anses som en essensiell del av verdiskapningen. I en slik organisasjon vil metadataene som støtter COIs være det viktigste (figur 4.6).

[6] Typisk kunde-selger relasjon.

Et viktig kriterium for ”riktig” implementasjon er å ha en grunnleggende forståelse for hvordan nettverk fungerer. Sosiale nettverk skiller seg ikke så mye fra andre typer nettverk enten det er snakk om webbaserte-, naturlige-, teknologiske-, sosio-tekniske- eller økonomiske nettverk. Hvordan nettverk oppstår, hvordan de ser ut og hvordan de utvikler seg er grunnleggende for å kunne bevege en organisasjon mot en nettsentrisk tilnærming til informasjonsstyring. Denne rapporten tar ikke mål av seg å utdype dette temaet videre, men en introduksjon til denne type nettverksforståelse finnes i (8).

5 METADATA

Begrepet metadata har blitt brukt mye de siste 15 årene, og har blitt spesielt vanlig gjennom den økende populariteten av World Wide Web. Men de underforliggende konseptene har vært i bruk så lenge ansamlinger av informasjon har blitt organisert og strukturert.

Metadata beskrives på flere måter. Noen beskrivelser er ”videre” enn andre, alt etter hva de skal beskrive og i hvilken kontekst de skal brukes. Ofte forklares metadatata som ”data om data” eller “*Data that describes and defines other data*” (9). Denne generelle beskrivelsen inkluderer et nærmest grenseløst spekter av muligheter - alt fra en menneskelaget tekstlig beskrivelse av en ressurs til maskingenerert data som kun er brukbar for software applikasjoner. I vår nettsentriske sammenheng er en ofte brukt beskrivelse betraktet som et nyttig utgangspunkt: *“Metadata is data which assists in the identification, description, evaluation and selection of an information object”*. “Object” vil i denne sammenheng forstås som data/informasjonsressurs.

Metadata sammenlignes ofte med tradisjonell katalogisering slik det utføres i bibliotekene, der man setter data som tittel, forfatter, utgivelsesår m.m i tilknytning til en bok eller et tidskrift for å kunne identifisere disse. De opplysninger som ligger på katalogiseringskortet og som gjør oss i stand til å finne boken på hyllen er eksempel på metadata. En av hovedhensiktene med å registrere metadata i biblioteker (katalogposter, bibliografiske beskrivelser, o l) er nettopp å være et hjelpemiddel for *gjenfinning*.

Innenfor IT-bransjen har metadata vært brukt i mange år og er etter hvert blitt et begrep som popper opp over alt og brukes om det meste. I Pollock & Hodgson (10) settes dette på spissen hvor de hevder at *”All IT-systems are metadata systems”*. Metadata finnes i databaser, mobiltelefoner, J2EE-applikasjoner og XML dokumenter for å nevne noen. Metadata har hovedsakelig blitt brukt av teknologieksperter for å designe og lage systemer. Problemet har vært at man ikke har hatt standardiserte beskrivelser man har kunnet følge. F eks i XML-verdenen så kan individer som modellerer det samme domenet designe XML-skjemaer med vidt forskjellige metadatainnhold.

5.1 Hva er nytt?

Metadata er altså ikke noe nytt. Hva består så det nye av? Litt enkelt kan svaret sies å være *anvendelsen* (bruksområdet): Introduksjonen av store og helt nye brukergrupper av metadata sammen med det etter hvert påtrengende behovet for å skape en levedyktig digital omgivelse

(infrastruktur) som er i stand til å håndtere de mange prosessene implementert i software og tilby aksess til de mange ressursene i nettverket. Samt at ved den raskt pågående utviklingen av de forskjellige web-teknologiene har potensialet ved å bruke metadata blitt aksentuert gjennom visjonen om den semantiske web'en. Kort sagt: "Internettsamfunnet". Internettsamfunnet involverer mange flere typer av *brukere* og *virksomheter* på en helt ny måte.

Så, fra å være en ekspertaktivitet forbeholdt typisk systemutviklere og bibliotekarer har metadata blitt en aktivitet også for ikke-eksperter; dvs en aktivitet som både angår og involverer de fleste brukere i dag. Bruk av metadata står derfor sentralt i den nettsentriske visjonen: I en nettsentrisk militær kontekst vil alle brukere både *produsere* og *forbruke* (konsumere) metadata for *nettbasert informasjon.* Generelt brukes metadata til:

- Søking
- Oppdaging ("discovery")
- Lokalisering
- Relevansvurdering og annen evaluering
- Utvelgelse
- Semantisk interoperabilitet
- Ressursadministrasjon

Når det snakkes om metadata for *nettbasert informasjon* har de noen spesielle egenskaper:

- Det er behov for metadata for å forbedre *presisjonen* ved søking på nettet.
- Metadata er et begrep som brukes langt utenfor bibliotekarenes og IT-ekspertenes rekker.
- Det er behov for metoder som er så enkle at det ikke kreves ekspertise på linje med f eks vanlig katalogisering i biblioteket eller programmeringskunnskaper.

5.2 Hovedtyper av metadata

Metadata kan brukes til å beskrive dataressursenes strukturelle og relasjonelle egenskaper, formater, sikkerhetsnivå eller semantikk.

I Pollock & Hodgson (10) refereres det til et 6-lags hierarki av metadatatyper. Dette er en differensiering og inndeling myntet på ekspertene (dvs systemutviklere) og utypes ikke her. I denne rapporten nøyer vi oss mellom å skille mellom 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 en COI. 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 kunne gjøre søk og gjøre ”enterprise discovery” av informasjonsressurser på tvers av ekspertdomener og virksomheter. Dette er metadata som i denne rapporten blir kalt for ”Enterprise metadata”.

5.3 ”Enterprise metadata”

For å illustrere nærmere hva man mener med ”Enterprise metadata” ut fra en nettsentrisk innfallsvinkel kan man tenke seg å inndele informasjonsressursene (dataene) i tre kategorier: 1) Private data, 2) COI-spesifikke data og 3) Virksomhetsdata (”Enterprise data”).

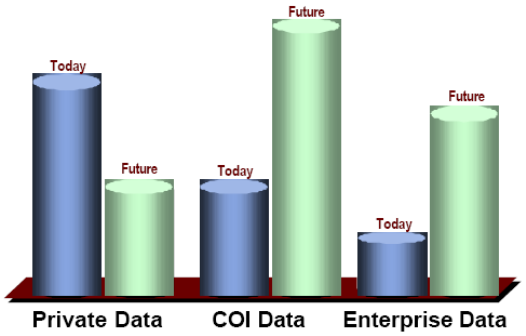
Private data er typisk informasjonsressurser holdt innenfor spesifikke systemer og sikkerhets-domener. Dataressursene er ikke tilgjengelige og ikke synlige for andre enn kun de som har spesiell autorisasjon. COI-spesifikke data er informasjonsressurser som er knyttet til en spesifikk COI og er tilgjengelig og synlig for alle COI-medlemmene i nettverket. Virksomhetsdata er informasjonsressurser som skal være tilgjengelig og synlig gjennom nettverket på tvers gjennom hele virksomheten. For å forklare bedre hva som menes med dette tar vi utgangspunkt i private data.

Dagens virkelighet er at de fleste militære informasjonsressurser er av type private data. De er ikke tilgjengelige for brukere utenfor sine domener. De er pr i dag ikke søkbare gjennom nettverket fordi det ikke er knyttet en søkbar beskrivelse (”nettsentrisk metadata”) til ressursen. Dersom man ikke vet om eksistensen til disse ressursene fra før av har man i dag ingen mulighet til å oppdage ressursene. Noen av disse informasjonsressursene er av spesielle årsaker (ofte sikkerhetsmessige) nødt til å være private, men langt fra alle. Mange av disse ressursene kan tenkes å være relevante for mange andre brukere i virksomheten. Mange av disse dataene er i dag helt unødvendig av privat type, dette av flere grunner (noen nevnt i kap.3). En av de mest åpenbare grunnene er de teknologiske og/eller informasjonsmessige interoperabilitets-problemene som man fremdeles sliter med. Ved å gjøre det teknologisk mulig å søke på disse ressursene gjennom hele nettverket, basert på metadata[7], ville en kunne ikke bare kunne gjøre ressursene mer tilgjengelig i en COI eller på tvers gjennom hele organisasjonen, men også gjøre det mulig å *oppdage* (”discover”) ressursens eksistens uten å måtte vite om den på forhånd. ”Discovery” eller på norsk ”oppdaging eller oppdagelse” er i denne sammenheng *evnen* til å lokalisere informasjonsressurser i nettverket gjennom konsistente og fleksible søkemetoder. Denne evnen blir i NATO sammenheng betraktet som en *kapabilitet* – en ”Enterprise Discovery Capability”.

Det å kunne oppdage og dele ressurser på denne måten mener man vil kunne gi store gevinster i form av økt samarbeid og mer effektiv deling av ressurser. Ved å etablere slike teknologiske

[7] I NATOs Discovery Metadata Specification (NDMS) (4) defineres såkalte ”discovery metadata elements”. Dette er kjernemetadata som vil være felles for alle COIs. NDMS er inndelt i 3 lag, hvorav ett er et såkalt kjernelag. Det er dette laget som fungerer som felleslag for alle COIs (se kapittel 5.4).

løsninger vil en danne et godt fundament for å komme et steg nærmere visjonen om en nettverksomgivelse (INI) som langt mer effektivt enn i dag støtter nettbasert tilgang og deling av informasjonsressurser på tvers av organisatoriske grenser og nivåer. Figur 5.1 viser hvordan amerikanerne tenker seg skiftet fra dagens militære situasjon hvor man har det meste av virksomhetens informasjonsressurser som private data til en fremtid hvor man har mer COI-spesifikke data eller virksomhetsdata som resultat av økt deling av informasjonsressurser i en nettsentrisk omgivelse.



Figur 5.1 *Visjon: Mer virksomhetsdata (”Enterprise Data”), mer COI-spesifikke data og mindre private data (2)*

5.4 Metadataformater

Man bruker ulike sett av metadata helt avhengig av hvilken type brukere man har, hvilke prosesser som skal utføres og hvilken type informasjonsressurs man skal representere. Dette kalles for ulike metadataformater. Det finnes en rekke forskjellige metadataformater som er utviklet for det spesielle formålet å "katalogisere" informasjon. De varierer sterkt når det gjelder kompleksitet og generalitet, og ikke minst når det gjelder den notasjonen som brukes. I BIBSYS registreres f eks metadata vha MARC-formatet (Machine Readable Catalogue Format). MARC formatet er utviklet med tanke på å tilfredsstille de behov et bibliotek har for beskrivelse av informasjonsobjekter. MARC-formatet er derfor tilpasset de arbeidsoppgaver som bibliotekarer, katalogisatorer og andre i biblioteket utfører. Bibliotekenes katalogisering er ofte veldig detaljert og ikke så lett å forstå for andre enn bibliotekarene. MARC-formatet har eksempelvis mange hundre ulike felter for beskrivelse.

I internettsammenheng er dagens bruk av metadata begrenset. Nettdokumenter karakteriseres ofte nettopp av mangel på metadata, f eks at det er vanskelig å finne presise opplysninger om tittel og hvem som er forfatter av dokumentet, osv. Dagens bruk av metadata er i stor grad rettet mot å utnytte søkemotorer som AltaVista, Google og HotBot som alle tar hensyn til de to metadatafeltene *description* og *keywords* under sin indeksering.

Det finnes imidlertid formater som er laget for ”katalogisering” av nettbaserte tjenester og informasjon. Som nevnt har nettbaserte ressurser noen spesielle egenskaper sammenlignet med tradisjonelle papirdokumenter. Sammen med kravet om at ”katalogiseringsarbeid” skal kunne utføres av andre enn bibliotekarer har dette påvirket utviklingen av *enkle* formater. Ett av disse er Dublin Core.

Dublin Core Metadata Element Set (DC) er et format utviklet med tanke på publisering av informasjonsressurser via Intranett. DC er en enkel standard for ressursbeskrivelse med gjenfinning som mål. DC består av et kjernesett (core) av 15 metadataelementer. Fordelen med DC er at det er lett å lage, forståelig for alle, lett å tilpasse, fleksibelt og systemuavhengig. DC er i dag nærmest blitt en internasjonal standard for bruk av metadata. DC gir utgiver muligheter til å beskrive en publikasjon mer detaljert enn ved bruk av kun de enkle metadatafeltene nevnt ovenfor. DC er ment å dekke langt mer enn tradisjonelle dokumenter i tekstlig form. Det har derfor fått en utforming som i sin enkelhet tar sikte på å omfatte tekst, lyd, bilder osv. I appendiks B gjengis de 15 elementene i DC-formatet. Elementene har beskrivende navn som tar sikte på å formidle en felles forståelse for hva elementet skal inneholde. I tillegg til disse elementene finnes det også mekanismer for å presisere hva slags informasjon som er registrert vha tilleggsattributter.

Det er ingen grunn til å tro at noe format vil få oppslutning av "alle" (heller ikke Dublin Core), til det er behovene og tradisjonene for forskjellige. Det medfører at vi får behov for å utveksle metadata mellom forskjellige systemer. Det krever konverteringsprogram.

De fleste organisasjoner som tar i bruk metadata for gjenfinning og oppdaging av nettbaserte ressurser definerer sine egne spesifikke formater tilpasset organisasjonens virksomhet, men mange baserer etter hvert sine metadataformater på DC. Figur 5.2 nedenfor viser som et eksempel på et metadataformat NATOs Discovery Metadata Specification (NDMS). Spesifikasjonen er basert på ISO 15836 the Dublin Core Metadata Element Set (17). NDMS har utover DC elementene tilleggselementer som skal støtte NATOs krav for å oppnå ”Enterprise Discovery Capability”. NDMS inngår som en sentral del av NATO NEC (3) fremtidig nettsentrisk datastrategi.

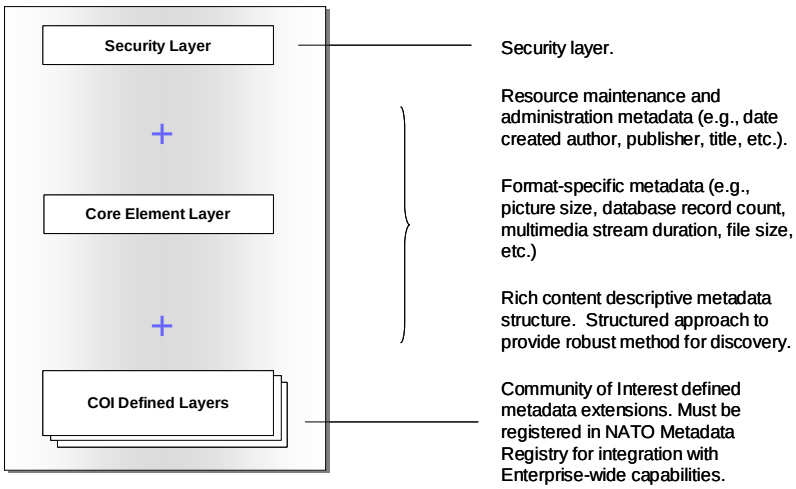
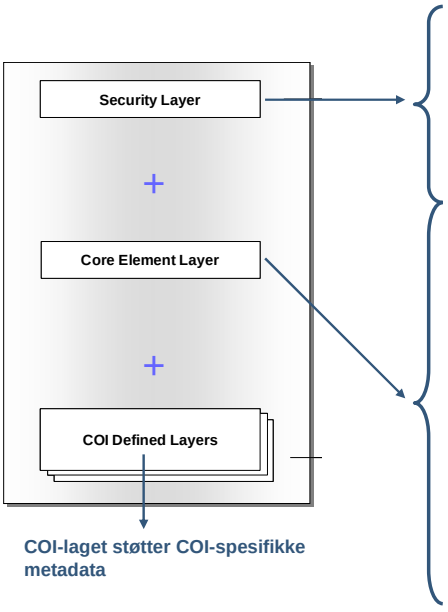


Figure 5.2 Eksempel: NATO Discovery Metadata Specification (NDMS) - Composition and Layer Elements (basert på Dublin Core) (4)

NDMS er inndelt i tre lag; et sikkerhetslag, et kjernelag og et COI-spesifikt lag. De to første lagene er spesifisert i spesifikasjonen gitt i (4) mens COI-laget skal spesifiseres av de respektive COIs. Hvert av de tre lagene har et definert ”eierskap” hvor ”eierne” har ansvar for innholdet (f eks er innholdet i sikkerhetslaget ”eid” av NATO INFOSEC). Kjernelaget vil være felles for alle COIs (jfr forrige delkapittel).

COI-laget støtter domenespesifikke- eller COI-spesifikke krav til ”discovery” og er en forlengelse eller utvidelse av de to første lagene. For å gjøre dette laget synlig i NATO-nettverket må dette laget registreres i NATOs Metadata Registry[8]. Dette må gjøres av alle COIs som ønsker å bli integrert i og bidra til NATOs ”enterprise discovery capability”. I figur 5.3 nedenfor viser i litt mer detalj elementene som inngår i de to første lagene.



Layer Description	Elements	Obligation
Security layer elements enable the description of security classification and other security-related fields. These fields provide for the specification of security-related attributes of the associated data assets and may be used to support access control. Additional security elements may be represented using the metadata elements defined by organizations and Communities of Interest, and stored in COI Defined Layers.	policy	Mandatory
	classification	Mandatory
	category	Conditional
Core Elements Consist of: - resource elements to describe aspects of a data asset that support maintenance, administration, and the derivation of the data asset. - format elements to provide the description of physical attributes of the asset and include elements such as the file size, bit-rate, and mime type. - content elements to provide the description of concepts and additional contextual aspects of the data asset being tagged and include such elements as subject, description, and coverage. These elements are intended to capture asset-level information that describes the content and/or context. An additional purpose of the content elements is to aid in precision discovery and to offer a level of description that is better than simple indexing.	title	Mandatory
	identifier	Mandatory if Applicable
	creator	Mandatory
	publisher	Recommended
	contributor	Optional
	date	Mandatory
	rights	Optional
	language	Optional
	type	Optional
	source	Optional
	relation	Optional
	format	Optional
	subject	Mandatory
	description	Mandatory
	coverage	Recommended

Figur 5.3 NDMS Layer Elements (4)

Et annet eksempel på et metadataformat er DoDs Discovery Metadata Specification (DDMS), hvor ”Core Layer” tilsvarer de to første lagene i NDMS og ”Extensible Layer” tilsvarer COI-laget. Hensikten med denne spesifikasjonen er tuftet på de samme nettsentriske datavisjonene som for NDMS.

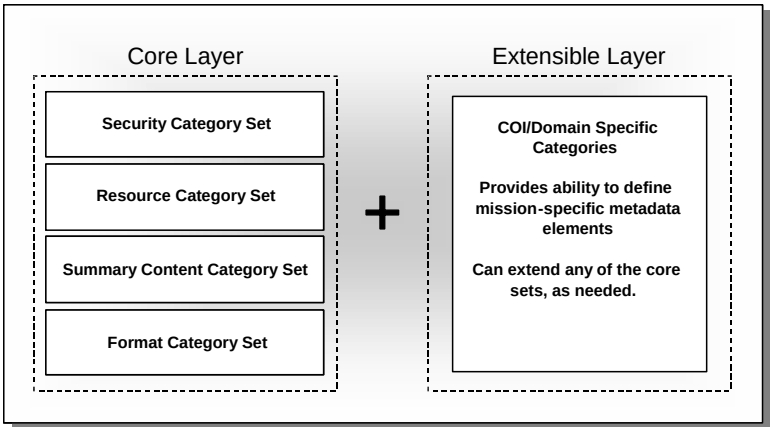


Figure 5.4 DDMS Layer Elements (5)

De fleste av NDMS- og DDMS-elementene er valgfrie med et minimum av obligatoriske felt.

[8] ”Metadata Registry” blir nærmere omtalt i kapittel 6.

Men jo flere felt som fylles ut, jo mer øker sjansene for at ressursene blir synlige gjennom søk slik at de ”oppdages”.

6 SENTRALE ELEMENTER SOM INNGÅR I EN METADATASTRATEGI

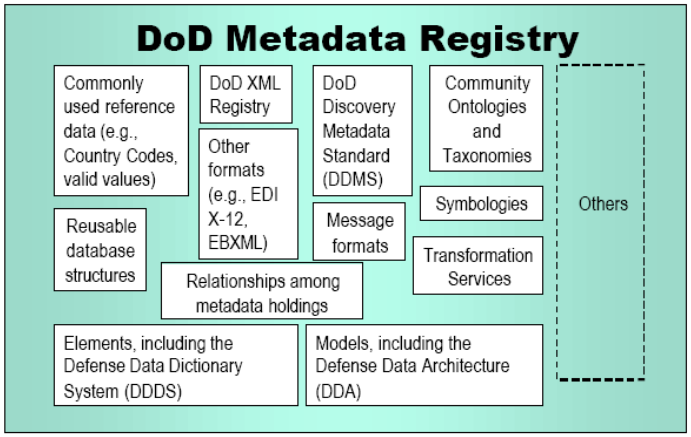
En nettsentrisk metadatastrategi har som hensikt å angi omrisset av visjonene for håndtering av dataressurser i en nettsentrisk omgivelse. Strategien skal være en helhetlig tenkning om hvordan dele informasjon gjennom hele organisasjonen. Sagt med andre ord: En nettsentrisk metadatastrategi skal fungere som et ”verktøy” til hjelp for å fokusere på *deling* av dataressurser i hele virksomheten.

I dette kapittelet beskrives i hovedtrekk noen av de mest sentrale elementene som vil inngå i en slik strategi basert på de tidligere nevnte arbeidene gjort i DoD og NATO. Disse elementene vil også måtte adresseres i en norsk militær nettsentrisk metadatastrategi.

Metadataregistre, ”Discovery Registry” og såkalte ”Shared Spaces” er sentrale mekanismer for å realisere lagring og prosessering av metadata og dataressurser.

6.1 Metadataregister

Et metadataregister (”Metadata Registry”) vil være et sted hvor de strukturelle og relasjonelle metadataene lagres og er en nøkkelkomponent for å oppnå virksomhetens interoperabilitetsmål. Alle dokumentformater, grensesnitt spesifikasjoner og utvekslingsmodeller brukt av systemer/-applikasjoner/tjenester lagres i dette registeret. F eks vil alle COIs ha et ansvar for å støtte inter-operabilitet gjennom å aktivt delta i å bygge opp slike metadataregistre. Dette vil i hovedsak være et ansvar for systemutviklere tilknyttet de ulike COIs. Figur 6.1 viser et eksempel (fra DoD) på hva som kan inngå i et metadataregister.



Figur 6.1 Eksempel på innhold i et metadataregister (2)

Et metadataregister vil typisk være en software applikasjon som bruker en database for å lagre og søke etter data. Typiske brukere av dette registeret vil være systemutviklere og applikasjoner. Data som f eks XML-skjemaer, taksonomier og ontologier kan lett oppdages og gjøres til-gjengelig for alle så snart de er publisert i registeret. Disse metadatataregistrene vil utgjøre en føderasjon av metadataregistre (”registry of registries”) i organisasjonen. En føderasjon tillater

flere metadataregistre å bli integrert og synkronisert inn i et virtuelt sentralt register som på den måten gir et enkelt punkt for gjenfinning og fremhenting av strukturelle metadata i organisasjonen.

6.2 ”Discovery Registry”

”Discovery Registry” eller ”oppdagelsesregister” er et slags oppslagsregister for sluttbrukeren og må ikke forveksles med Metadataregisteret som beskrevet i 6.1. Et ”Discovery Registry” inneholder *instanser* av *metadata*, dvs selve informasjonen som beskriver informasjonsressursen (f eks sikkerhetsinformasjon, navn, beskrivelse av ressursen, innhold, osv). COIs vil ha ansvar for å opprette og vedlikeholde disse registrene. Et ”Discovery Registry” vil typisk være en software applikasjon som bruker en database for å lagre og søke etter metadata som beskriver informasjonsressursene. Typiske brukere av et slikt register er sluttbrukere som vil bruke søkeportaler og applikasjoner for å lokalisere akkurat den informasjonsressursen som er relevant for dem, uten å måtte bruke tid på å søke mange forskjellige kilder. Sluttbrukerne vil også ha et ansvar her for å bidra til beskrivelsen av de informasjonsressursene som de selv vil gjøre tilgjengelig for andre (annonsere) i nettverket. Disse beskrivelsene lagres i et slikt register.

Det vil i tillegg være et ”Enterprise Discovery Registry” som linkes til COI-registrene for å skape en føderasjon av ”registry of registries”. Enterprise-registeret vil også inneholde metadata av informasjonressurser postet av sluttbrukere eller applikasjoner uten en spesifikk COI- eller domene tilknytning.

Registrene vil være søkbare gjennom web-baserte grensesnitt. Web-grensesnittet vil ha et konsistent utseende og vil støtte posting av metadata til registeret og informasjonsressursen til ”shared spaces”. Alle ”Discovery Registries” vil følge samme ”Enterprise discovery interface standard” som tillater søk innenfor et register eller på tvers av registre (dvs innenfor en COI eller på tvers av COIs).

6.3 ”Shared Space”

Et ”shared space” (delt informasjonsrom) er en mekanisme som tilbyr brukere lagring og tilgang til informasjonsressurser innenfor et avgrenset område (typisk en COI). ”Shared space” fungerer som oppbevaringssteder (lagringsplasser) hvor brukere (og applikasjoner) kan poste sine informasjonsressurser.

Alt det som lagres på et ”shared space” skal i prinsippet gjøres tilgjengelig for andre i nettverket. Eksempel: I sin aller enkleste form kan et ”shared space” være et fellesområde på FISBasis for lagring av filer. Et ”Enterprise-shared space” er områder som er tilgjengelig for alle brukere innenfor eller på tvers av sikkerhetsdomener i nettet (f eks nettverk av COIs). Fysisk består disse informasjonsrommene av servere og kjernetjenester i nettverket.

Målet er at brukere (og applikasjoner) går fra hovedsaklig å håndtere private data til å gjøre sine informasjonsressurser tilgjengelig gjennom ”shared spaces” enten det er innenfor en COI eller tilgjengelig for alle (”enterprise wide”).

For å summere, innenfor denne konteksten (metadatatastrategi) så vil ”shared spaces” inneholde et metadataregister, et ”Discovery Registry”, de informasjonsressursene (dataene) som er fysisk lagret innenfor området samt et sett med kjernetjenester som gjør det mulig å prosessere og hente data (se figur 6.2).

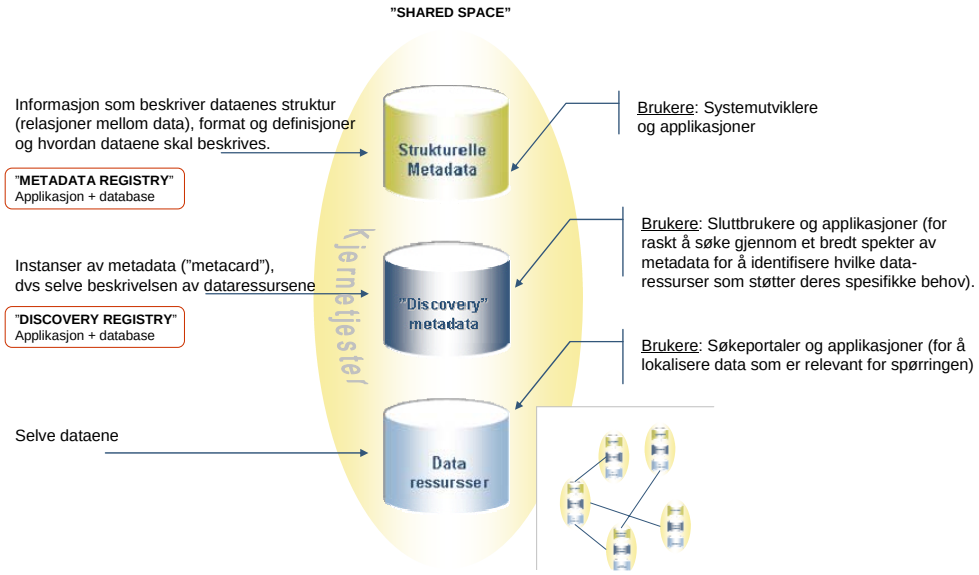


Figure 6.2 ”Shared space” & nettverk av ”shared spaces”

I den nettsentriske tenkningen opererer man ikke med ett sentralisert ”shared space”, men med et nettverk av ”shared spaces” som skal spille sammen (se firkant nederst til høyre i figur 6.3). Helt analogt med tanken om nettverk av COIs beskrevet i kapittel 4.5. I figur 6.3 vises som et eksempel NATOs beskrivelse av et ”Shared Data Environment” (”Metadata Catalog” i figuren tilsvarer det vi i denne rapporten har valgt å kalle ”Discovery Registry”).

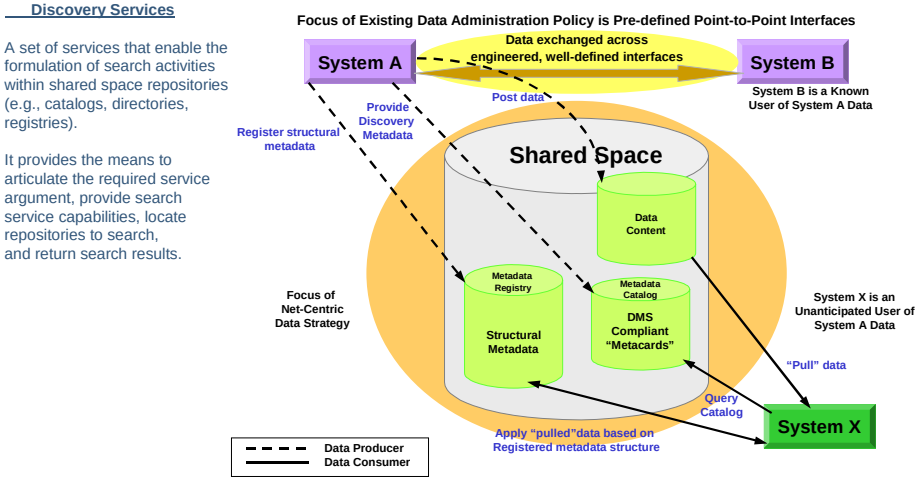


Figure 6.3 Eksempel: NATOs ”Shared Data Environment” (3)

Ved å kunne søke på dataressurser gjennom hele nettverket basert på metadata og ”shared spaces”, vil det gjøre det mulig for brukere å *oppdage* (”discover”) ressursens eksistens uten å måtte vite om den på forhånd. Som nevnt i kapittel 5.3 er ”discovery” altså *evnen* til å lokalisere informasjonsressurser i nettverket gjennom konsistente og fleksible søkemetoder. Det er denne

evnen NATO betrakter som en *kapabilitet* – en ”Enterprise Discovery Capability” (se figur 6.4).

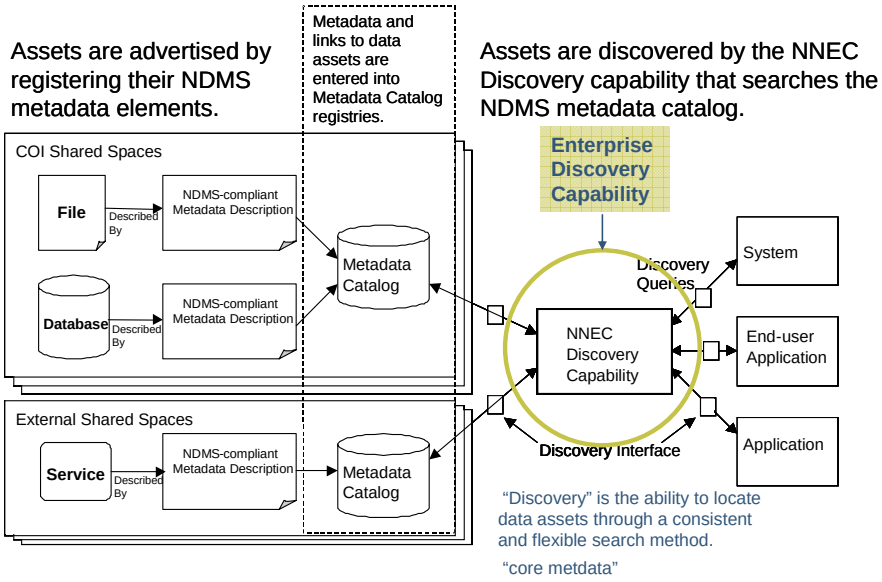


Figure 6.4 *NDMS Usage Conceptual Diagram (3)*

7 NOEN UTFORDRINGER

Det vil være mange utfordringer knyttet til realisering av en nettsentrisk metadatastrategi. Mange av disse vil være store utfordringer knyttet til både teknologi og organisasjon.

Dette kapittelet skraper kun på overflaten og har ikke som ambisjon å gå i dybden eller være uttømmende på dette området.

7.1 Informasjonsstyring

Dagens etablerte informasjonsstyring er dominert av ”state-of-the-practice” innenfor utvikling av virksomhets arkitekturer, som kort kan oppsummeres i tre følgende aktiviteter (7):

- Baseline – ”as-is” arkitektur
- Utvikle ”to-be” strukturer og prosesser (virksomhetsperspektiv) optimalisert i forhold til avkastningsgrad (Return Of Investment, ROI)
- Rette inn IKT-investeringer i henhold til oppdragsbehov (mission).

Selv om det er mange fordeler ved en slik strukturert tilnærming er det store spørsmålet likefullt hvorvidt dette er tilstrekkelig innenfor en nettsentrisk omgivelse?

Kritikken går på at i en nettsentrisk omgivelse (f eks INI) vil informasjonsomgivelsen og den underliggende infrastruktur være i konstant forandring. Det har ofte de seneste årene vist seg at både endringshastigheten av underliggende infrastruktur og den økende hyppigheten av nye krav til informasjonsomgivelsen går langt fortere enn evnen til å lage et ”to-be” virksomhetsperspektiv av informasjonsomgivelsen. ROI er i sin natur uforutsigbar.

I tillegg vil operative styrker måtte kunne evne å hurtig omorganisere og respondere til flere typer oppdrag – også de oppdrag som nærmest er umulig å forutsi på forhånd. Det eneste man kan si med sikkerhet om fremtiden er at fremtiden er uforutsigelig og at endringer vil være konstante og uunngåelige. Den erkjennelsen tyder på at det ikke er tilstrekkelig å prøve å lage informasjonsstyringskonsepter som innretter IKT-investeringer iht oppdragsbehov (”mission”). Dersom man gjør det vil man risikere i beste fall å suboptimalisere og i verste fall etablere nye stove-pipes – såkalte ”mission stove-pipes”.

7.2 Semantisk forståelse

Semantisk forståelse og interoperabilitet vil også være en av de neste store utfordringene som vil møte IKT-miljøene. Ettersom Web-services og SOA får større utbredelse og gjør det mulig å knytte IKT-systemer direkte mellom samhandlende partnere – skjønner systemene fortsatt ikke innholdet i meldingene de utveksler. F eks så opererer EU med tre lag for interoperabilitet som har en klar innbyrdes sammenheng (15):

1. Teknisk interoperabilitet som omfatter beskrivelse av protokoller og standarder som er nødvendig for teknisk å knytte ulike systemer sammen (datautveksling).
2. Semantisk interoperabilitet som omfatter definisjon, beskrivelse og standarder for metadata og verktøy for informasjonsmodellering
3. Organisatorisk interoperabilitet som omfatter standardisering/harmonisering av forretningsprosesser mellom enheter.

Det er ingen tvil om at de to siste nivåene (2 og 3) vil være de som blir mest krevende. SOA adresserer kun den tekniske interoperabiliteten (dvs nivå 1).

Fra et teknologisk ståsted vil verdien av samhandlingen i et nettsentrisk perspektiv først og fremst ligge i det å oppnå interoperabilitet på det semantiske nivået, dvs å sikre presis mening og felles oppfattelse av betydningen av informasjonen som utveksles (jfr definisjonen av COI om felles vokabular, s14). Det er først da man kan begynne å snakke om reelle muligheter for organisatorisk interoperabilitet og for å oppnå mer dynamiske COI-dannelser på kryss og tvers.

Semantiske teknologier (som f eks ontologier) vil selvsagt stå sentralt i dette arbeidet (1). Likefullt vil en av de store utfordringene fremover være å unngå feilsatsninger i forhold til fremtidige utviklingstrekk og standardiseringstiltak.

7.3 Sikkerhet

Sikkerhet er et stort og viktig tema som denne rapporten ikke belyser i noen særlig grad, men likefullt forutsetter er der. Sikkerhetsaspektene kan nok sies å være en av de aller største utfordringene man kommer til å møte. Sikkerhet gir ikke bare teknologiske utfordringer (mye av teknologien er faktisk her allerede) men er også i høyeste grad en organisatorisk og kulturell utfordring. Det er helst det siste som vil være den aller største utfordringen. Får man ikke endret dagens sikkerhetsregler vil det sette en effektiv bremse på en nettsentrisk utvikling.

Eksempelvis tillater ikke dagens militære regelverk deling av informasjon i noen særlig grad.

Det er en ”need-to-know” praksis som gjelder og ikke en ”need-to-share” praksis som står i fokus. Som nevnt i kapittel 2.5 er det et faktum at dagens regelbaserte sikkerhetspolicy ikke tillater mye deling av informasjon. En mer risikobasert sikkerhetspolicy vil kunne øke den muligheten, men da må man faktisk være villig til å endre dagens regelverk. Behovet er så definitivt til stede. Regelbasert sikkerhetstenkning er et barn av tidligere tiders militære virkelighet. Dagens situasjon krever andre måter å tenke sikkerhet på. Dette vil ta tid og kreve masse arbeid fordi sikkerhet berører stort sett all militær virksomhet på ulike måter.

I (1) beskrives noen av de sikkerhetsutfordringer man står overfor på teknisk side. Der beskrives også noen nye sikkerhetsteknologier for å kunne realisere en fremtidig nettsentrisk tilnærming. Men det fordrer at vi klarer å endre våre mentale modeller om hva sikkerhet i militære sammenhenger er. Gitt følgende eksempel:

En måte å tenke digital informasjonssikkerhet på i dag er knyttet til systemet, nettverket eller maskinen informasjonen er en del av. Har man kun ett lite informasjonsobjekt klassifisert til konfidensielt eller hemmelig blir automatisk hele systemet, nettverket eller PCen klassifisert konfidensielt eller hemmelig. Da sier det seg selv at systemet ikke kan utveksle informasjon med andre systemer som har lavere klassifikasjon, selv om systemet også innehar masse ugradert informasjon som ville kunne vært interessant for mange andre å få tilgang til. Det gjør det hele veldig lite fleksibelt, og tilgjengeligheten for andre brukere og systemer nærmest lik null. Hvis en derimot kan tenke seg at man legger sikkerheten på selve informasjonen – og *ikke* på systemet eller nettverket – da vil en oppnå større fleksibilitet og tilgjengelighet. Dette er i tråd med en dataorientert tilnærming hvor man skiller dataene fra systemene og prosessene hvor den inngår. Metadataene vil her være sentrale fordi disse vil angi sikkerhets- og tilgangsnivåer. Sammen med teknologier som f eks sikkerhetsmerker, digitale signaturer og streng aksesskontroll basert på brukerens aksessprivilegier vil dette kunne regulere sikker tilgang til dataressurser. Da er det brukerens aksessprivilegier som styrer tilgangen til informasjons-ressursene og ikke hvilke nettverk eller system ressursen er knyttet til. Dette vil gi en mer dynamisk og fleksibel tilgang til informasjonsressurser (også det å inkludere uforutsette brukere).

Dette var et enkelt eksempel, men det illustrerer noe viktig. Nemlig at det går an å tenke annerledes og det faktisk går an å få det til, men at dagens sikkerhetsregler (som også er inngravert i dagens militære informasjonssystemer) og etablert praksis (kultur) står i veien for å gjøre dette i nær fremtid.

Et annet viktig aspekt ved dette eksempelet er brukernes tillit. En av utfordringene teknologene står overfor dersom de skal etablere nye og mer fleksible sikkerhetsløsninger er å skape tillit til disse og det sikkerhetsarbeidet som gjøres. Poenget her er at det ikke bare er tillit til teknologien i seg selv som er avgjørende. Det er også helt avgjørende at *prosessene rundt* sikkerhetsarbeidet må gjøres på en tillitsvekkende måte. Tillit fører til økt brukervennlighet og det gjelder å utvikle og ta i bruk teknologien på en tillitskapende måte.

7.4 ”Co-evolution”

Mange hevder at NBF først og fremst handler om menneskelig og organisatorisk atferd og ikke

så mye om teknologi. Det viktigste er individers og organisasjoners *evne til tilpasning* gjennom *økt utnyttelse* av informasjon. Vi er langt på vei enig i det, men - og det er et stort men her – vi mener at NBF handler *like mye* om teknologi som det handler om mennesker og organisasjon. For hvis man tar teknologi ut av NBF-likningen og setter den på sidelinjen som en *passiv* aktør - hvordan skal man da reelt og gjennomgripende *øke* individers og organisasjoners *evne* til tilpasning gjennom *økt utnyttelse* av informasjon?

Det betyr likevel ikke at man ikke er enig i at det i noen grad har vært overfokusert på teknologiens rolle i det praktiske NBF-arbeidet – både i nasjonale og i internasjonale sammenhenger. Noe som bl a har ført til at man langt på vei har ignorert, og dermed ikke økt, den militære organisasjonens *anvendelseskompetanse* og *tilpasningsevne* av den nye teknologien (dvs evnen til å utnytte teknologiens potensiale i større grad)[9]. Spesielt i Norge synes det som om man har fokusert lite på *transformasjonsprosessen.* Overgangen til en nettsentrisk organisasjonstenkning vil også være en slags transformasjonsprosess som inkluderer en rekke store teknologiske- og ikke minst store sosiale utfordringer. Denne prosessen vil nødvendigvis ta tid.

De fleste er etter hvert inneforstått med at man ikke bare kan sette inn ny teknologi[10] i gammel setting og tro at man får utnyttet teknologien fullt ut (11)(12)(13). Denne innsikten har ofte blitt tatt til inntekt for isolerte syn gjeldende både for og i mot teknologiens rolle i NBF. Den type polarisering er *ikke fruktbar*. Det vil være like uheldig å utvikle organisasjonen isolert fra de teknologiske mulighetene som det vil være å utvikle teknologiske løsninger isolert fra organisasjonen. Spesielt gjelder dette situasjoner der et stort antall mennesker er involvert og hvor behovet for endring er uttalt og erklært. En slik tilnærming gir dysfunksjonelle resultater. Det man ønsker seg er en koordinert utvikling som kan gi synergiske resultater - det som i K2-litteraturen omtales som ”co-evolution” (14). Ved å ta inn teknologi som *likeverdig* variabel i NBF-likningen (som en *aktiv* aktør fordi den påvirker sine omgivelser) sammen med organisasjon, prosesser og individ vil man på sikt kunne få frem en koordinert utvikling mot effektive arbeidspraksiser og trekke ut effekter som ikke var mulig å forutse *uten* den nye teknologien. Det innebærer at mennesker og organisasjon endrer sin oppførsel ifm bruk (anvendelse) av teknologien og dermed øke sin evne til utnyttelse av informasjon.

En eventuell implementasjon av en nettsentrisk metadatastrategi vil være et eksempel på akkurat det: Organisasjonen må fremme en såkalt ”nettsentrisk atferd” på individnivå for å trekke ut de ønskede *kollektive* effektene. Kollektive effekter fordrer kritisk masse. Kritisk masse betyr her at det oppnås en tilstrekkelig stor mengde av brukere (produsenter) organisert i COIs som faktisk annonserer sine ressurser i nettverket og en tilstrekkelig stor mengde av konsumenter som opplever en merverdi av å få tilgang til disse ressursene. Da først kan man reelt måle summen av opplevd nytteverdi i organisasjonen (jfr bruk av epost). En slik utvikling av arbeidspraksiser skjer selvsagt ikke over natten. Dette vil være en evolusjonær og forhåpentligvis en koordinert utvikling. Selv om arbeid og kunnskap om metadata tradisjonelt har vært en aktivitet forbeholdt

[9] Eksempel: I internasjonale sammenhenger hvor nordmenn deltar i konkrete operasjoner viser det seg at det ofte er organisasjonsstrukturer, nasjonale agendaer og nasjonale sikkerhetspolicies (altså ikke-teknologiske elementer) som står i veien for å ta i bruk allerede tilgjengelig teknologi (et eksempel på dette er gitt i 16).

[10] Spesielt berører det Informasjons- og kommunikasjonsteknologi (IKT) som er ”innvevd” i sentrale arbeidsprosesser.

teknologer og IT-miljøer, og som dermed har beskyttet vanlige brukere fra den type kompleksitet, så vil metadata i en nettsentrisk sammenheng involvere aktører langt utover det tradisjonelle. Å få de ønskede effekter av en slik tilnærming stiller krav til organisasjonen og menneskene på en ny måte.

Det er viktig at ikke bare teknologene tar eierskap i denne prosessen. Vanlige brukere og ikke minst de operative ledere i organisasjonen må også ta eierskap i prosessen. Det betyr at brukerne og lederne må se på teknologien som en aktiv aktør i prosessen og ikke bare ta for gitt at ”teknologien ordner seg selv – at den kommer”. For – tar man for gitt at teknologien kommer og dermed ignorerer den – hvilke teknologiske løsninger risikerer man å få da?

Gjennom etablering av gode og gjennomtenkte insentivstrukturer og utstrakt kursing eller opplæring i nettsentriske praksiser vil organisasjonen kunne fremme en såkalt ”nettsentrisk atferd” på individnivå for å trekke ut de ønskede effektene. Men det forutsetter at en slik prosess er forankret på høyeste nivå i den militære organisasjonen. Det å vedta en slik strategi bør være en top-down styrt avgjørelse hvor sentrale militære ledere ”ute i felten” og hjemme er aktive inn mot dannelsen og kontinuiteten av denne prosessen. Dette er et viktig skritt for å anspore og oppmuntre andre til deltagelse. Det bør være en mer bottom-up prosess hvordan man innholdsmessig realiserer en slik strategi.

Utvikling av en mer nettsentrisk metadatastrategi for det norske forsvar vil kunne bidra til at Forsvaret tar et stort steg nærmere noen av de mest sentrale NBF-visjonene. Derfor vil arbeidet med en metadatastrategi for Forsvaret og realiseringen av den handle like mye om mennesker og organisasjon som det handler om teknologi (eller var det omvendt...?).

8 OPPSUMMERING OG KONKLUSJON

Et av de mest sentrale målene innenfor militær tenkning i dag, både nasjonalt og internasjonalt, er å *øke* evnen til *samarbeid* på tvers av militærorganisatoriske grenser, fagdisipliner, forsvarsgrener og nivåer. Samarbeid forutsetter økt tilgang til, og deling av, informasjon. Nettbasert samarbeid anses for å ha et meget stort potensial mht fleksibilitet og effektivitet forutsatt støttet av en ”riktig” underliggende infrastruktur. Forsvarets nåværende INI støtter ikke denne type samarbeid i noen særlig grad.

En nettsentrisk metadatastrategi vil være et organisatorisk ”ledelsesverktøy” til hjelp for å fokusere på deling av dataressurser i organisasjonen. Implementasjonen av en slik strategi vil bidra til å bevege Forsvarets INI i en retning av å bli en nettsentrisk omgivelse som inkluderer nettsentriske virksomhetsprosesser og brukeratferd. Dette vil dramatisk kunne øke evnen til samarbeid i Forsvaret.

Nettsentrisk tenkning er opprinnelig fundert på ideen om å støtte nettbasert samarbeid og deling av informasjon på tvers av geografiske, kulturelle og organisatoriske grenser som følge av utviklingen av internett/web teknologier. Begrepet ”Net-centricity” slik det synes brukt i NATO og USA, brukes nærmest synonymt med begrepet Service Oriented Architecture (SOA) – men for store organisasjoner som Forsvaret er ikke dette bare er et teknologisk spørsmål men inneholder også et bredt spekter av sosiale utfordringer. SOA i seg selv løser f eks ikke viktige

aspekter som sikkerhet, men gir gode muligheter for å tenke nye og mer fleksible sikkerhetsløsninger både på teknisk og organisatorisk nivå.

Innføring av begrepet COI virker intuitivt enkelt og lett å forstå. Like fullt er det ikke helt trivielt når man går i dybden. Overgang til en COI-basert virksomhet krever at man tenker gjennomgående annerledes enn før (både teknologisk og organisatorisk) og har gode kunnskaper om hvordan nettverk dannes og oppfører seg. COIs kan både betraktes som et organiserings-prinsipp som fremmer økt samarbeid og deling av informasjon mellom mennesker, og som et informasjonsstyringsprinsipp for å håndtere enormt store mengder av data i en mer kompleks IKT-verden. Høy myndighetsgrad (”selvråderett”) og samarbeid innen hver enkelt COI kan også lede til mer selvorganisering. Ved å styre organisasjonen i en nettsentrisk retning tillater det oss (på sikt) å gå utover ”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.

Nettsentriske informasjonsstyringsprinsipper gir også nye utfordringer. Det kreves at også mange systemutviklere og andre teknologiske eksperter evner å gå utover de tradisjonelle lærdommer innenfor systemutvikling og arkitekturdesign. På sikkerhetssiden vil det også være store utfordringer hvor man både må ha evne og vilje til å tenke nytt om militær sikkerhet både når det gjelder teknologi og organisasjon. Det kreves mye arbeid for å utvikle en tillitsvekkende nettsentrisk sikkerhetstilnærming, samt gode og forpliktende ledelsesprosesser for å operasjonalisere COIs og INI-kjernetjenester. Det er viktig å kunne levere kjernetjenester som gjør målene i en nettsentrisk datastrategi oppnåelig.

INI er tett omsluttet av sosiale relasjoner, dypt forankret i menneskers arbeidspraksis (kultur). Det er derfor av helt avgjørende betydning at man systematisk og målbevisst arbeider med organisasjon og prosess. Spesielt på informasjonssiden er menneskene, prosessene og organisasjonen det største hinderet. F eks er menneskene de som har informasjonen, men å få informasjonen opp fra ”skuffen” og inn i de delte informasjonsrommene er en utfordring. Det å få mennesker til å bli komfortable med å gå fra en ”need-to-know” praksis til en ”need-to-share” praksis er en kulturell utfordring. Man bør inkorporere belønningssystemer (insentiver), og nettsentriske dataprosesser og praksiser gjennom trening og utdanning. Veien mot nettsentrisk organisering (både teknologisk og organisatorisk) er en evolusjonær prosess som tar tid og kan ikke systemutvikles eller organisasjonsdesignes på tradisjonell måte. Det hjelper lite å bruke masse tid og penger på nye teknologiske løsninger dersom man ikke tar organisasjonen og individer på alvor og investerer like mye i dem som man gjør på teknologisiden.

”Net-centricity” er en enkel og lettfattelig ide men er veldig vanskelig å realisere. En av årsakene til det er at den militære organisasjonen er organisert ”stykke for stykke”. Det er så mange bevegelige parter at forsøker man å jobbe med dette stykkevis og delt risikere man at man aldri lykkes. En transformasjon av denne type er en evolusjonær prosess og må i utgangspunktet bygges på eksisterende infrastruktur (teknologisk og organisatorisk). Ideelt vil man etablere 1, 2, 5 og 10-års planer for å monitorere og guide denne transformasjonen. Deler av organisasjonen vil sannsynligvis bevege seg fortere enn andre, men masterplanen for hele organisasjonen må stå fast.

Litteratur

(1) Gagnes T, Eggen A, Hedenstad O E, Rasmussen R, Sletten G (2005): Operative Beslutningsstøttetjenester – Fremtid NBF, FFI/RAPPORT-2005/03584.

(2) US DoD (2003): Net-Centric Data Strategy (May 9, 2003).

(3) NATO NEC (2005): NNEC Data Strategy, NATO/EAPC, Version 1.1, EAPC(AC/322-SC/5)N(2005)0018.

(4) NATO Data Administration Group (NDAG) (2005): Guidance on the use of metadata element descriptions for use in the NATO Discovery Metadata Specification (NDMS), Version 1.0. EAPC(AC/322-SC/5)WP(2005)0007.

(5) US DoD (2005): Department of Defense Discovery Metadata Specification (DDMS), Version 1.3, Office of the Assistant Secretary of Defense (July 29, 2005).

(6) US DoD (2005): Guidance to COIs for Implementing Net-Centric Information Sharing, DoD 8320.2-G, November 7, 2005. Draft.

(7) Bass T (2005): Information Management Challenges on the Path to Net-Centric Operations, In: *Proceedings of the IEEE Milcom 2005*, Atlantic City, NJ, October 17-20 2005.

(8) Hafnor H (2004): Aktør-nettverk teori som teoretisk rammeverk og praktisk verktøy for å analyse informasjonsinfrastrukturer i et NbF, FFI/RAPPORT-2004/00223.

(9) Wells E (2005): Net-Centric Operations & Warfare (NCOW), Reference Model (Version 1.1) & NC3TA Impacts, NOSWG June 2005.

(10) Pollock J T, Hodgson R (2004): Adaptive Information: Improving Business Through Semantic Interoperability, Grid Computing, and Enterprise Integration. John Wiley & Sons, Inc., Hoboken, New Jersey.

(11) Hafnor H (2002): Slagmarksdigitalisering, nettverkstenkning og informasjons-infrastrukturer: En innledende betrakting, FFI/RAPPORT-2002/02036.

(12) Bjørnstad A L (2004): NCW in Theory and Practice: A human factors perspective on why it might work and why we might not get there. FFI/RAPPORT-2004/02106.

(13) Alberts D S, Hayes R E (2005): Code of Best Practice: Campaigns of experimentation, Pathways to Innovation and Transformation, CCRP Publication Series. 2005.

(14) Atkinson S R, Moffat J (2005): The Agile Organization: From Informal Networks to Complex Effects and Agility, CCRP Publication Series. 2005.

(15) European Interoperability Framework (EIF)(2004): European Interoperability Framework for Pan-European eGoverment Services, Final Version 1.0, Office for Official Publications og theEuropean Communities, 2004.

(16) Hafnor H (2005): (U) Stabiliseringsoppdrag: Urban Disarmament – referansescenario, FFI/RAPPORT-2005/04002, Begrenset.

(17) ISO (2003): Information and Documentation – The Dublin Core Metadata Element Set, ISO 15836:2003(E), ISO TC 46/SC 4 N515.

APPENDIKS

A EKSEMPEL PÅ COI-ROLLER

Tabellen nedenfor er hentet fra draftet til ”Guidance to COIs for Implementing Net-Centric Information Sharing” (6).

Summary Definitions of COI roles

ROLE	DEFINITION
COI members	The personnel that participate in COI activities. COI members may come from any area of the Departement. The composition of COIs include data producers, data consumers, capability developers, operators, IT leadership, and portfolio managers.
COI lead	Meant to identify an individual from a specific Component who has been tasked to ”manage” the COI. Usually the Component that is leading the COI activity has committet to driving the COI to a solution and will ensure that agreements are implemented within Components plans, programs, and budgets.
COI Governing Authority	Typically meant to imply the IT portfolio manager (Mission Area lead or designated subportfolio manager) that will review and adjudicate COI conflicts and will push for Component implementation and support of those agreements.
COI stakeholders	Organizations or personnel who have an interest in the outcome of the COI effort. May not be active participants in the COI (i.e., a COI member) but will likely use and/or benefit from the capability.
Capability Developers	Personnel or organizations responsible for actually implementing the data sharing agreements (e.g. access services).
Data producers	Organizations, systems, programs, and personnel that create and maintain data assets.

B DUBLIN CORE

Dublin Core Metadata Element Set (DC) er et format utviklet med tanke på publisering av informasjonsressuser via Intranett. Dette formatet har fått navn etter Dublin Ohio, hvor Online Computer Libary Center (OCLC) og National Centre for Supercomputer Applications (NCSA) arrangerte en workshop i 1995, med det formål å komme fram til et generelt metadataformat. Siden da har det vært drevet et intenst arbeid for å komme fram til en så god og stabil standard som mulig.

DC er en enkel standard for ressursbeskrivelse med gjenfinning som mål. DC består av et kjernesett (core) av 15 metadataelementer. Fordelen med DC er at det er lett å lage, det er forståelig for alle, lett å tilpasse, fleksibelt og systemuavhengig. DC er i dag nærmest blitt en internasjonal standard for bruk av metadata. DC gir utgiver muligheter til å beskrive en publikasjon mer detaljert enn ved bruk av kun de enkle metadatafeltene description og keywords nevnt tidligere i kapittel 5.4.

DC er ment å dekke langt mer enn tradisjonelle dokumenter i tekstlig form. Det har derfor fått en utforming som i sin enkelhet tar sikte på å omfatte tekst, lyd, bilder osv. Listen over elementer med definisjoner ble publisert i desember 1996. Det ventes ingen vesentlige endringer i listen, selv om enkelte elementer har vært gjenstand for eksperimentell bruk.

Nedenfor gjengis i sin enkleste form de 15 elementene i DC-formatet. Elementene har et beskrivende navn som tar sikte på å formidle en felles forståelse for hva elementet skal inneholde:

#	Felt	Beskrivelse
1	**Title**	Det navnet som er gitt ressursen av opphavsmann eller utgiver.
2	**Creator**	Person(er) og eller institusjon(er) som er hovedansvarlig(e) for ressursens [intellektuelle] innhold.
3	**Subject**	Det emnet eller de emnene ressursen handler om eller beskriver.
4	**Description**	En tekstlig beskrivelse av ressursens innhold.
5	**Publisher**	Den instans som er ansvarlig for å gjøre ressursen tilgjengelig
6	**Contributors**	Person(er) eller institusjon(er) som har gitt betydelig [intellektuelt] bidrag til ressursen, men som er sekundær til den/de som er angitt i felt 2.
7	**Date**	Datoen ressursen ble gjort tilgjengelig i dette formatet.
8	**Type**	Ressursens form eller sjanger.
9	**Format**	Ressursens dataformat.
10	**Identifier**	Tekststreng eller nummer som entydig identifiserer ressursen.
11	**Source**	Identifikator (tekststreng eller nummer) som entydig identifiserer det verket

#	Felt	Beskrivelse
		som denne ressursen stammer fra.
12	**Language**	Det (eller de) språk som er brukt i ressursen.
13	**Relation**	Relasjonen denne ressursen har til andre ressurser.
14	**Coverage**	Angivelser av geografiske eller tidsmessige avgrensninger ved ressursen.
15	**Rights**	Referanse til opphavsrettsformulering, eller til en tjeneste som kan formidle informasjon om betingelsene for å få tilgang til ressursen.

I tillegg til disse elementene finnes det også mekanismer for å presisere hva slags informasjon som er registrert vha tilleggsattributter.

C FORKORTELSER OG AKRONYMER

DC	Dublin Core (standardisert metadataformat)
DDMS	DoD Discovery Metadata Specification
DoD	Departement of Defence (US)
COI	Community of Interest
COTS	Commercial of the Shelves
GIG	Global Information Grid (US)
IKT	Informasjons- og kommunikasjonsteknologi
INI	Forsvarets informasjonsinfrastruktur
ISAF	International Security Assistance Force
K2	Kommando og kontroll
MARC	MAchine Readable Catalogue
NATO NEC	NATO Network Enabled Capability
NBF	Nettverksbasert Forsvar
NDMS	NATO Discovery Metadata Specification
NORCCIS	Norwegian Command Control and Information System
NOSWG	NATO Open Systems Working Group
ROI	Reurn of Investments (avkastningsgrad)
SOA	Service Oriented Architecture
XML	eXtensible Markup Language