Konsept for styring av

elektronisk informasjon

i Forsvaret

Godkjent pr. 1. september 2005

Innhold

1. Innledning

Informasjonsteknologi påvirker i stadig større grad oss alle, både hjemme og på jobb. De fleste tar mobiltelefon, bruk av ett betalingskort i alle butikker, og at vi kan kommunisere og informere via Internett, som en selvfølge. Offentlig virksomhet, og dermed også Forsvaret, står foran store utfordringer med å tilpasse seg den nye informasjons- og kunnskapsalderen.

Konsept for nettverksbasert forsvar er et resultat av utviklingen i samfunnet nasjonalt og internasjonalt, teknologisk, kunnskapsmessig, sosialt og kulturelt. Konseptet er også påvirket av den type konflikter, og militære operasjoner som har funnet sted i de senere år, og de nye trusselbildene etter 11 september 2001.

Styring av elektronisk informasjon og kunnskap til å nyttiggjøre seg denne, er viktige innsatsområder i realiseringen av et nettverksbasert forsvar. Betydningen kan være ulik i sivil og militær sammenheng, fra virksomhet til virksomhet, og innenfor ulike deler av Forsvaret. I sivil, og ikke minst i kommersiell sammenheng, blir styring av informasjon og utvikling av kunnskap vektlagt for å sikre at virksomhetene skaper bærekraftige konkurransefortrinn. For Forsvarets operative virksomhet vil for eksempel etablering, vedlikehold og distribusjon av konsistente situasjonsbilder kreve en effektiv styring av elektronisk informasjon. For å utvikle Forsvaret til en lærende organisasjon, vil det være viktig og nødvendig med en systematisk kunnskapsforvaltning. For å oppnå informasjonsoverlegenhet, som er vektlagt i konsept for nettverksbasert forsvar, kreves altså effektiv styring av informasjon.

I den nettverksbaserte tenkningen legges det vekt på å utnytte muligheter for organisering og tilrettelegging av arbeidet på nye og mer effektive måter. Ønskede effekter er:

- ***økt deling av informasjon og kunnskap***
- ***bedre samarbeid***
- ***bedre og enklere koordinering og synkronisering***
- ***distribuert og virtuell organisering***

Summen av dette skal bli raskere og riktigere beslutninger. For å bidra til at dette blir en realitet, har Forsvarsdepartementet utarbeidet et konsept for styring av elektronisk informasjon som er ment å gi overordnede føringer for kompetansebygging og planlegging, samt invitere til diskusjon. Konseptet tar primært utgangspunkt i Forsvarets virksomhet, selv om vi ser at Forsvaret fremover vil stå overfor store utfordringer med nye eksterne aktører og samarbeidspartnere. Konseptet er videre avgrenset til styring av elektronisk informasjon.

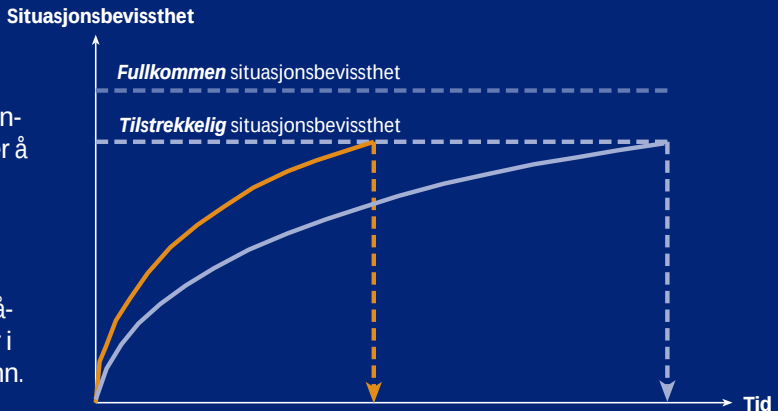
2. Betydningen av raskere og riktigere beslutninger

2.2 Raskere beslutninger

Napoleon uttalte en gang:

«Du kan be meg om hva som helst, unntatt tid.»

Beslutningstakere settes under stadig sterkere press etter hvert som informasjonsmengden øker, og kravene til kompetanse for å tolke og analysere informasjonsmengden dermed blir forsterket. Når mange aktører skal operere i en koordinert samhandling med behov for hyppige beslutninger, er det en utfordring for beslutningstakere å orientere seg i mengden av og kvaliteten på den informasjonen som er tilgjengelig. En annen utfordring er å identifisere manglende informasjon, for deretter å etterspørre slik spesifikk informasjon, samt å sikre samhandling uten misforståelser. Det vi har behov for er i praksis et beslutningsfortrinn.



Figur 1. *Beslutningsfortrinn vil si å oppnå tilstrekkelig situasjonsbevissthet først.*

Da fullkommen situasjonsbevissthet til enhver tid er en umulighet i praksis, fattes beslutninger når tilstrekkelig situasjonsbevissthet er oppnådd. Som figuren viser, oppnås et fortrinn dersom vi får til dette raskere enn vår motstander (oransje kontra grå kurve). Dette fører videre til et handlingsetterslep hos vår motstander, ved at vi kommer på innsiden av hans beslutningssløyfe, dvs at vi beslutter og handler med bakgrunn i oppnådd situasjonsbevissthet raskere enn vår motstander rekker å respondere.

2.3 Riktigere beslutninger

Gjennom styring av elektronisk informasjon, kan vi oppnå høyere tempo i prosessene for forvaltning og formidling av denne. Dette gjør at vi potensielt kan få mer tid til refleksjon forut for beslutninger, og at vi derigjennom oppnår et beslutningsfortrinn ikke gjennom kvantitet (høyere antall beslutninger), men snarere gjennom kvalitet i våre beslutninger. Det er derfor av stor betydning å identifisere og beskrive hvilken elektronisk informasjon som er nødvendig for å oppnå et riktigst mulig beslutningsunderlag.

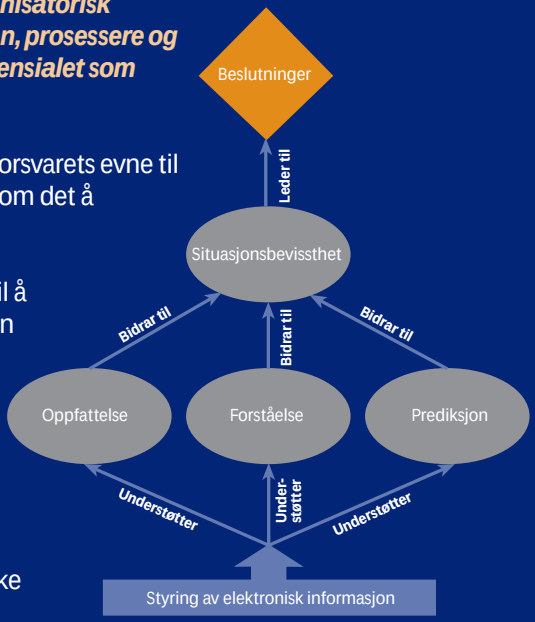
3. Hvorfor er styring av elektronisk informasjon viktig?

I konsept for nettverksbasert forsvar står det at:

«NBF dreier seg i hovedsak om menneskelig og organisatorisk atferd. Det fokuserer på å oppnå tilgang til, samle inn, prosessere og styre informasjon for å dra fordel av det økende potensialet som ligger i informasjonsnettverk.»

Konseptet bygger med andre ord på individenes og Forsvarets evne til å utvikle og utnytte elektronisk informasjon, for gjennom det å muliggjøre raskere og riktigere beslutninger.

Situasjonsbevissthet omfatter evnen og muligheten til å kunne oppfatte situasjonen - med andre ord tilstanden og dynamikken i de faktorer som påvirker den. Persepsjon innebærer evnen til å sanse og sette sammen inntrykkene til et rasjonelt og objektivt bilde av situasjonen. Forståelse omfatter identifikasjon og tolkning, samt gjenkjenning av tilsvarende situasjoner basert på praktisk eller teoretisk erfaring. Med prediksjon menes den dynamiske forståelsen av situasjonen som danner grunnlag for vurdering av ulike handlingsalternativer. Effektiv styring av elektronisk informasjon må støtte opp under disse komplekse og samvirkende prosessene.



Figur 2. *Styring av elektronisk informasjon understøtter situasjonbevissthet.*

4. Hva innebærer styring av elektronisk informasjon?

4.2 Definisjoner

I dette konseptet har vi valgt å bruke NATOs definisjoner, som sier at informasjonsstyring (eng: Information Management, forkortet IM) er:

«The process by which the organization efficiently plans, collects, organizes, uses, controls, disseminates and disposes of its information, and through which it ensures that the value of that information is identified and exploited to the fullest extent.»

I dette legger vi at informasjon skal håndteres mest mulig elektronisk gjennom hele dens livssyklus, og at vi derigjennom sikrer et best mulig beslutningsunderlag.

4.3 Forholdet mellom informasjon og kunnskap

Figur 3 forklarer en sentral sammenhengen:

Verditrappen tar utgangspunkt i at data blir tilgjengeliggjort slik at det er mulig å hente ut relevant informasjon. Informasjon settes sammen til ulike budskap, som blandet med erfaringer, verdier og innsikt, er det som legger grunnlaget for kunnskapsforvaltning. Styring av elektronisk informasjon bidrar til at man beveger seg oppover verditrappen, og at Forsvaret dermed blir i stand til å hente ut de nettverksbaserte effektene vi tidligere har omtalt.

Figur 3. *Verditrapp for informasjon.*

4.4 Håndtering av kunnskap

Deling av kunnskap forenkles ved at den kodifiseres og gjøres tilgjengelig som elektronisk informasjon. For å forklare, og se på hvilken type kunnskap som er enkel og vanskelig å gjenbruke og dele elektronisk, etableres følgende kunnskapskategorier:

- *Eksplisitt kunnskap formidles gjennom kodifisert informasjon. Dette er blant annet den typen kunnskap som formidles gjennom lærebøker og e-læring. Eksplisitt kunnskap kan lett gjenbrukes og deles elektronisk.*

- *Erfaringsbasert kunnskap utvikles gjennom praktiske erfaringer. Forsvaret må ha et bevisst forhold til at også den erfaringsbaserte kunnskapen skal gjenbrukes og deles. Dette kan gjøres ved at den blir dokumentert elektronisk f eks i lessons learned databaser, og ikke bare delt muntlig eller gjennom handling.*

- *Taus kunnskap opparbeides gjennom lang tids erfaringer og kan utvikles til å bli en intuisjon hos medarbeiderne slik at de kan ta beslutninger «uten å tenke». Denne kunnskapskategorien er den som er vanskelig å tilgjengeliggjøre elektronisk. Deling kan imidlertid gjøres gjennom mentorordninger, on the job-training eller gjennom simulatortrening.*

For Forsvaret er den erfaringsbaserte og tause kunnskapen viktig, fordi beslutninger ofte må fattes svært raskt, og konsekvensene kan bli alvorlige hvis det tas feil beslutninger. Det er derfor viktig at organisasjonen har et bevisst forhold til disse kunnskapsområdene. Ressurser bør kanaliseres inn mot hvordan man kan få kodifisert, lagret, gjenbrukt og delt erfaringsbasert og taus kunnskap.

Når man i konsept for nettverksbasert forsvar snakker om å dra fordel av det økende potensialet som ligger i informasjonsnettverk, er styring av elektronisk informasjon og kodifisering av kunnskap sentralt for å gjøre dette mulig.

5. Hvordan oppnås styring av elektronisk informasjon?

5.2 Ledelse og styring

I henhold til forsvarets fellesoperative doktrine (FFOD), er kommando- og kontrollsystemet et integrert system som består av doktrine, prosedyrer, organisasjon, personell, utstyr, anlegg og kommunikasjoner, som sikrer at alle nivåer har tilstrekkelig data for å planlegge, lede og kontrollere sine aktiviteter. En sentral del av dette er informasjon, og da ikke primært mengden av informasjon, men at den er tilgjengelig til rett tid, i rett mengde og i riktig form.

For å ivareta dette, er det nødvendig med en helhetlig og målrettet styring av elektronisk informasjon som tidligere beskrevet i kapittel 1. Dette stiller krav til ledelse og styring med forankring i Forsvarets ledelse.

5.3 Organisering

Arbeidet med styring av elektronisk informasjon bør ledes av et sentralt strategisk element som sikrer prioriteringer av investeringer og tiltak. Dette ledelseselementet må sikre en koordinering og konsistens i hele virksomheten. Videre må det sørges for at modeller og metoder blir utviklet og implementert, og at det blir innført verktøy for å måle resultatene og at gevinster blir realisert.

FFOD omtaler informasjon som en sentral innsatsfaktorer i basisfunksjonene K2 (i K2S-et) og i etterretning. På mange måter beskrives etterretning helt tilsvarende som informasjonsstyring, dog med en klar avgrensning av hvilke typer data og informasjon det fokuseres på (data og informasjon om andre land, fiendtlige eller mulige fiendtlige styrker eller elementer, eller aktuelle og mulige operasjonsområder). Tidligere hadde organisasjonen et bedre situasjonsbilde over egne styrker basert på kjente situasjoner, kjent trussel og kjente handlingsmønstre med basis i

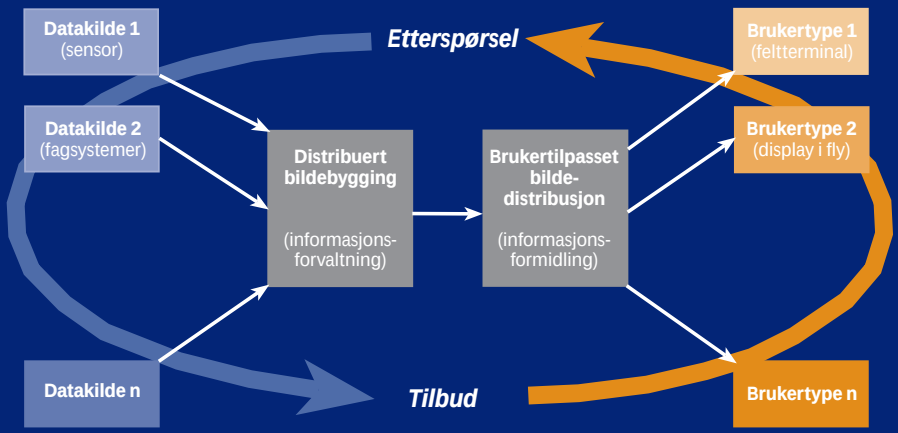
faste planer og prosedyrer. Organisasjonen for håndtering av informasjon om oss selv er derfor lavt dimensjonert. Dagens operasjonsmønstre har endret seg radikalt, og fremtidens operasjoner vil ha mindre forutsigbarhet med hensyn på lokalisering, organisasjon og involverte parter. Således må en i større grad basere seg på dynamiske planer som til enhver tid tilpasses den aktuelle situasjonen. Ut fra dette, ser vi at informasjonsstyring må fokuseres mer helhetlig i fremtiden, dvs omfatte alle typer relevante data og informasjoner, inklusive også det som angår egne styrker.

En organisasjon er menneskene den består av, og ikke minst den kulturen eller de kulturene som finnes i den. Erfaringer viser at en effektiv informasjons- og kunnskapsdeling har svært mye med kultur og holdninger å gjøre. Det må derfor utvikles kompetanse om hvordan man kan gjenbruke og dele informasjon elektronisk, og ikke minst hvordan organisasjonen kan utvikle en gjenbruks- og delingsadferd. Medarbeiderne må oppleve å kunne utnytte og bidra til Forsvarets samlede læring, ved at den informasjon og kunnskap som skapes blir gjenbrukt og delt.

5.4 Prosesser

I konsept for nettverksbasert forsvar presiseres det at informasjonsstyring ikke primært dreier seg om informasjonssystemer og -teknologi, men om den informasjon systemene gir adgang til, og hvordan den behandles og fordeles. Prosessene i Forsvaret må derfor i større grad tilrettelegges for elektronisk flyt og deling av informasjon. Arbeidsflyt i prosesser på tvers av geografi og avdelinger kan bidra til betydelig effektivisering, motivasjon og kvalitativ forbedring. Effekten oppnås bare gjennom fokusert styring av elektronisk informasjon, noe som igjen krever egne arbeidsprosesser for nettopp dette. Det handler om å drive med prosesskartlegging, prosess-analyse og omstilling i et livssyklusperspektiv, for å sikre at informasjon er tilpasset og bidrar til måloppnåelse. Det må også finnes prosesser som gjør det enkelt for medarbeiderne å se verdien av å bidra med og dele sin kunnskap. Det er slik man oppnår kontinuerlig læring både for den enkelte medarbeider og for Forsvaret totalt sett.

Figur 5 viser at det er to sentrale prosesser; distribuert bildebygging (forvaltning av informasjon i et livssyklusperspektiv) og brukertilpasset bildedistribusjon (formidling av informasjon i riktig format og i riktig kanal).



Figur 5. *Prinsipper for effektiv utvikling av informasjon.*

Det er viktig å forstå den gjensidige avhengigheten mellom prosessene. Informasjonen øker i verdi når den gjenbrukes og deles. Forutsetningen for å få til dette, er at den forvaltes profesjonelt gjennom hele dens levetid.

Figuren viser at det i prinsippet ikke er en direkte kobling mellom datakildene og informasjonskanalene. Dataprodusenter vet ikke alltid hvilke informasjonskonsumenter som kan ha behov for

deres data. Det er derfor viktig at data kontekstualiseres til informasjon (beskrives med metadata) og gjerne også analyseres (verdiøkes til etterretning). Dette gjør det mulig å kunne tilby beslutningsunderlag på riktig format og i riktig kanal i forhold til ulike brukeres operative behov. Som figuren viser, er det viktig å få til en gjensidig vekselvirkning mellom tilbud og etterspørsel av informasjon.

For tidskritisk informasjon, må det også etableres direkte linjer mellom datakildene og informasjonskonsumentene (f eks IFF løsninger), selv om dette vil kreve en egen kapasitet for kontekstualisering av data hos konsumentene. Det er dog viktig at denne typen data også inngår i en helhetlig forvaltning av informasjon, ved at hele eller et egnet utvalg av disse dataene leveres til felles kontekstualisering og analyse.

5.5 Teknologi

Det er i hovedsak utviklingen innen informasjonsteknologi, og de muligheter som ligger i løsningene denne teknologien har medført, som utgjør grunnlaget for nettverkstenkningen. All den tid vi har bestemt oss for å satse på at nettverkstenkningen skal styre den videre utviklingen av Forsvaret, må vi også lage en struktur og sammenheng i vår anvendelse av informasjonsteknologi som støtter dette. Sentrale momenter er:

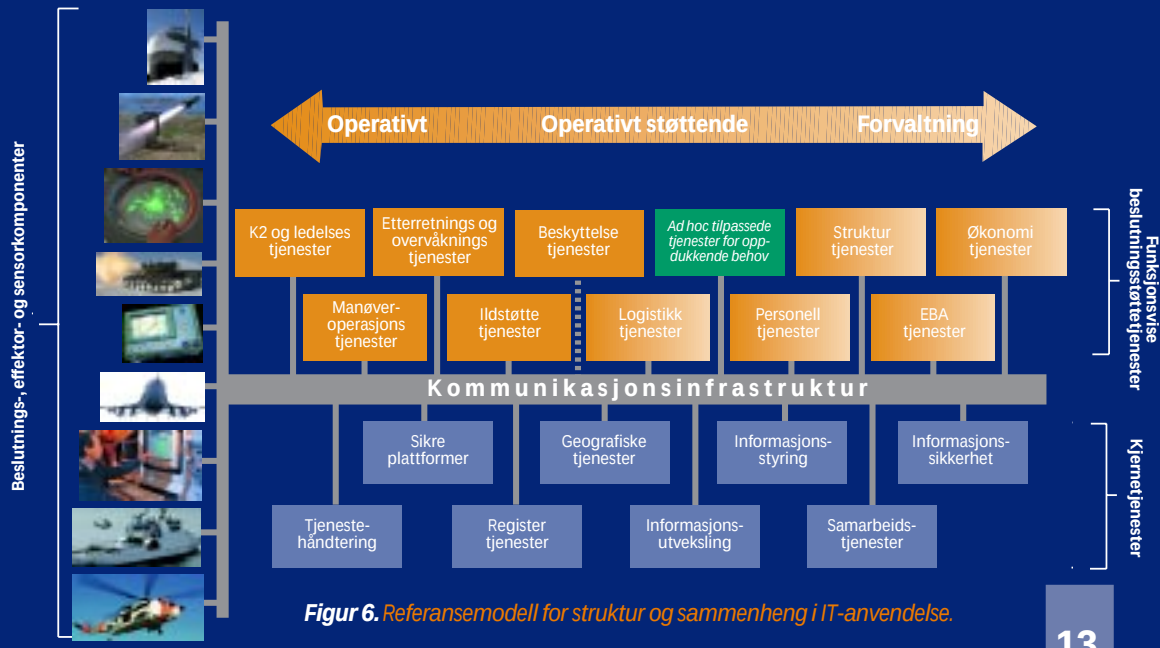
- *Sammenhengen og strukturen i teknologianvendelsen, samt de standarder som legges til grunn, må bidra til at Forsvaret effektivt kan operere sammen med nåværende og nye samarbeidspartnere, både nasjonalt og internasjonalt.*

- *Nye løsninger må utvikles med mulighet for kontinuerlig tilpasning og oppgradering, ikke bare for total utskifting. Fleksibilitet må være et bærende prinsipp, blant annet gjennom løpende evaluering av nye løsninger.*

- *Det må legges vekt på å etablere samvirkende moduler som kan organiseres slik at de muliggjør rask og fleksibel støtte i henhold til forskjellige behov.*

- *Det må tilstrebes en utvikling der typen og antallet informasjons- og kommunikasjonsløsninger reduseres og samordnes bedre både innenfor og på tvers av graderingsdomener. Dette vil i seg selv utgjøre et viktig bidrag til interoperabilitet.*

Figur 6 viser en mulig referansemodell for hvordan informasjonsteknologi kan brukes til å bygge opp en felles infrastruktur for elektronisk informasjon.

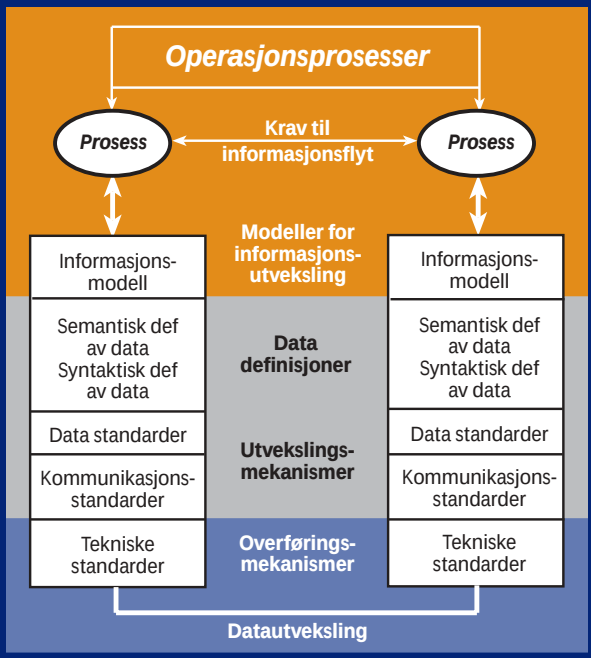


Figur 6. *Referansemodell for struktur og sammenheng i IT-anvendelse.*

Referansemodellen deler opp infrastrukturen i funksjonsvise beslutningsstøttetjenester og felles kjernetjenester bundet sammen av kommunikasjonsinfrastrukturen. Disse vil hver for seg bestå av ulike typer IKT, men den samlede militære tilpasningen og anvendelsen av IKT må sees som en helhet i tråd med referansemodellen. Det er sentralt å merke seg at kjernetjenestene er felles, mens de mer spesialiserte beslutningsstøttetjenester adresserer ulike brukergrupper med felles behov for beslutningsstøtte i form av elektronisk informasjon. Kommunikasjons-infrastrukturen binder det hele sammen med kvalitetssikrede mekanismer for forbindelse mellom beslutningsstøtte- og kjernetjenestene, samt koblingen mellom disse og de ulike beslutnings-, effektor- og sensorkomponentene.

5.6 Interoperabilitet

Konsept for nettverksbasert forsvar sier at en viktig premiss for å utvikle Forsvaret i en nettverksbasert retning, er at det legges til grunn en todimensjonal interoperabilitet som danner grunnlaget og muligheter for integrerte beslutnings-, effektor- og sensor-nettverk. Todimensjonal interoperabilitet innebærer at grenvise komponenter er interoperable på tvers av forsvarsgrener, og med komponenter hos allianse- og koalisjonspartnere. Figur 7 viser en mulig referansemodell for interoperabilitet i informasjonsdomenet:



Figur 7. *Referansemodell for interoperabilitet i informasjonsdomenet.*

Til grunn for all utvikling av interoperabilitet i informasjonsdomenet, ligger de operative prosessene som ønskes gjennomført. Som tidligere nevnt, er det helt sentralt at Forsvarets prosesser tilrettelegges for elektronisk flyt og deling av informasjon. Dette modelleres som behov for (elektronisk) informasjonsflyt mellom prosesser, noe som videre danner grunnlag for ytterligere nedbrytning i så vel en semantisk[1] som syntaktisk[2] datadefinisjon. Basert på data- og kommunikasjonsstandarder, defineres en egnet utvekslingsmekanisme. Dataene utveksles så gjennom tekniske overføringsmekanismer basert på avtalte tekniske standarder. En motsatt prosess hos aktuelle mottakere rekonstruerer informasjonen slik at denne kan inngå i aktuelle prosesser.

5.7 Sikkerhet

Konsept for nettverksbasert forsvar setter informasjon i sentrum, og avhengigheten av sikkerhet knyttet til informasjonsobjektene blir derfor betydelig større enn i dag. Fleksibel og rask tilgang til riktig og rett informasjon blir således en avgjørende faktor i forhold til hvorvidt et nettverksbasert forsvar lar seg realisere eller ikke. Følgende overordnete forhold gjelder:

- *Sikring av informasjon bør i mindre grad være knyttet til fysiske kommunikasjonsløsninger.*

- *Informasjon med forskjellig graderingsnivå bør kunne håndteres samtidig og uavhengig av fysisk tilknytning.*

Sikkerhetsløsningene er i dag stort sett knyttet til fysiske kommunikasjonsløsninger. For å oppnå tilstrekkelig fleksibilitet i utnyttelse av informasjon, bør sikkerhetsløsningene i større grad knyttes til selve informasjonsobjektene. En dreining mot innholdsbaserte sikkerhetsløsninger vil frigjøre bindinger, og muliggjøre bruk av mange ulike typer underliggende kommunikasjonsløsninger.

---

[1] Semantikk vil si forholdet mellom språklige tegn og det tegnene står for, refererer til eller betyr.
[2] Syntaks vil si de formale relasjonene mellom tegnene selv.

Dette eliminerer ikke behovet for sikkerhet innen fysisk kommunikasjon, men gir slik sikkerhet en noe annen rolle, mer rettet mot sikring av tilgjengelighet eller en form for informasjonsgaranti.

Gjennom løsninger for forvaltning og formidling av elektronisk informasjon, skapes grunnlag for økt situasjonsforståelse hos hver enkelt medarbeider. Dette eksponerer oss for at en motstander vil forsøke å utnytte enkeltmennesker. Det er derfor essensielt at tilgangsstyring oppfattes som en integrert del av dette med styring av elektronisk informasjon. Effektiv og robust håndtering av sikkerhetsinformasjon for så vel informasjonsobjektene som for medarbeidere, organisasjons-elementer, effektor- og sensorkomponenter, samt selve tjenestene i informasjonsinfrastrukturen, er derfor et område som må vektlegges. Dog kan vi ikke alene gjennom tekniske mekanismer og prosedyrer håndtere dette sikkerhetsaspektet. Personlige egenskaper, holdninger, kultur og motivasjon er sentrale momenter i denne sammenhengen.

5.8 Oppsummering

Styring av elektronisk informasjon og kodifisering av kunnskap bidrar til at vi blir i stand til å:

- ***Gjennomføre beslutningsprosesser raskere***
- ***Forbedre kvaliteten på våre beslutninger***
- ***Oppnå organisasjonslæring***
- ***Utvikle motiverte og kunnskapsrike medarbeidere***

6. Iverksetting

Dette konseptet er gjeldende fra og med 1 september 2005. Det erstatter tidligere utgitte versjoner av tilsvarende konsept.

Kort forklaring av tjenestene i referansemodellen

Tjenesteinndelingen av funksjonsvise beslutningsstøttetjenester og felles kjernetjenester kan innholde mangler og overlapp. Det må forventes at omfanget og inndeling av tjenestene vil endres når modellen tas i bruk og erfaringer vinnes.

Funksjonsvise beslutningsstøttetjenester

- **Kommando, kontroll og ledelsestjenester** - Tjenester for å planlegge, lede og kontrollere Forsvarets virksomhet. Eksempelvis tjenester for utvikling av planer, ordre og oppdrag samt for simulering og analyse.
- **Manøveroperasjonstjenester** - Tjenester for gjennomføring av militær virksomhet, dvs til støtte for de ulike typene operasjonsformer (landoperasjoner, luft operasjoner, maritime operasjoner, amfibieoperasjoner, luft- og missilvern, informasjonsoperasjoner, spesialoperasjoner samt krisehåndtering).
- **Etterretnings- og overvåkningstjenester** - Tjenester for å bygge situasjonsbilder. Eksempelvis tjenester for etterretning, rekognosering, overvåkning og sensorstyring.
- **Ildstøttetjenester** - Tjenester for å styre og synkronisere ulike typer ild. Eksempelvis tjenester for lokalisering og målprosessering, målengasjement, valg av effektor og virkningsanalyse.
- **Beskyttelsestjenester** - Tjenester for ARBC, fortifikasjon og andre beskyttelsestiltak.
- **Logistikktjenester** - Tjenester for fremskaffe og opprettholde materiell stridsevne.
- **Personelltjenester** - Tjenester for rekruttering, utvikling, anvendelse og avvikling av personell.
- **Strukturtjenester** - Tjenester for å planlegge, realisere og evaluere strukturer.
- **EBA-tjenester** - Tjenester for håndtering av eiendom, bygg og anlegg. Eksempelvis tjenester som støtter etablering og nedrigging av camp.
- **Økonomitjenester** - Tjenester for lønn og regnskap.
- **Ad hoc tilpassede tjenester** - Denne typen tjenester er tatt med for å indikere at vi må ha fleksibilitet til å kunne lage spesialtilpassede samlinger av tjenester tilpasset et oppdukkende operativt behov.

Felles kjernetjenester

- **Tjenestehåndtering** - Tjenester for eksempelvis systemovervåkning, sikring av tilgjengelighet og ulike typer callsentre (helpdesk).
- **Sikre plattformer** - Sikre kjøremiljøer med standard støtteverktøy (FISBasis Hemmelig/NATO Secret og FISBasis Begrenset/Ugradert).
- **Registertjenester** - Forvaltning og formidlig av tjenestene i informasjonsinfrastrukturen, eksempelvis en oppslagstjeneste («elektroniske gule sider») .
- **Geografiske tjenester** - Tjenester for forvaltning og bruk av geografisk informasjon. Eksempelvis kartmotor med evne til å vise militær symbolikk, overlegghåndtering og grunnleggende tracking.
- **Informasjonsutveksling** - Standarder og løsninger for informasjonsutveksling nasjonalt, med allierte styrker og koalisjonspartnere samt med relevante nasjonale instanser. Eksempler på denne typen tjenester er militær meldingshåndtering, epost, datalinker og replikering.
- **Informasjonsstyring** - Tjenester for fangst, lagring, fusjonering og korrelering, gjenfinning og utnyttelse av informasjon.
- **Samarbeidstjenester** - Tjenester for lyd- og videotelefoni og annen online samhandling.
- **Informasjonssikkerhet** - PKI, IP kryptering og andre typer tjenester for sikring av konfidensialitet, integritet og tilgjengelighet.

Egne notater

Konsept for styring av

elektronisk informasjon

i Forsvaret

Utgitt av
Forsvarsdepartementet

Myntgt 1
Postboks 8126 Dep
0032 Oslo

Telefon: 23 09 80 00
Telefaks: 23 09 61 05

www.forsvarsdepartementet.no

ISBN 978-82-7924-057-0

FORSVARSDEPARTEMENTET