FFI RAPPORT

SAMARBEID MELLOM FORSVARET OG INDUSTRIEN INNEN PROGRAMOMRÅDET INI

SKOGSTAD Arne K, WARBERG Erik Normann

FFI/RAPPORT-2006/01620

SAMARBEID MELLOM FORSVARET OG INDUSTRIEN INNEN PROGRAMOMRÅDET INI

SKOGSTAD Arne K, WARBERG Erik Normann

FFI/RAPPORT-2006/01620

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-2006/01620	UNCLASSIFIED	63
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFI-I/1024/911	-	

4) TITLE

SAMARBEID MELLOM FORSVARET OG INDUSTRIEN INNEN PROGRAMOMRÅDET INI

COLLABORATION BETWEEN THE ARMED FORCES IN NORWAY AND INDUSTRY WITHIN PROGRAM AREA ICT

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

SKOGSTAD Arne K, WARBERG Erik Normann

6) DISTRIBUTION STATEMENT

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

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) ICT Policy	a) IKT policy
b) Defence ICT organisation	b) Forsvarets hovedaktører innen IKT
c) ICT Portfolio	c) IKT porteføljen
d) National competence	d) Nasjonal kompetanse
e) Industrial cooperation	e) Samarbeid med industri

THESAURUS REFERENCE:

8) ABSTRACT

This report is focused on the Defence Information and Communication infrastructure (INI). The Ministry of Defence Policy guidelines are quite ambitious regarding the further development of INI, and focus on the importance of centralized management. The Defence Organisations responsible are diversified, and the roles and authority seems diffuse. The national industries have been heavily involved in development of the legacy, and should be further used in developing the legacy for the future. The Defence Forces and Industry possesses complementary competence, and for some niches a long-term agreement between the parties is regarded as a future-oriented solution. The legal opportunity set is described along with possible initiatives.

9) DATE	AUTHORIZED BY	POSITION
	This page only	
2006-05-22	Einar Willassen	Director of Research

ISBN 82-464-1004-0

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

INNHOLD

SAMARBEID MELLOM FORSVARET OG INDUSTRIEN INNEN PROGRAMOMRÅDET INI

1 BAKGRUNN

Informasjons- og kommunikasjonsteknologi (IKT) har siden begynnelsen av 90-tallet vært et kompetanse- og satsningsområde for Forsvaret og norsk forsvarsindustri. På midten av 90-tallet utgav Forsvarsdepartementet (FD) en "Nasjonal strategi for norsk forsvars- og forsvarsrelatert industri", som trakk opp retningslinjene for hvordan samarbeidet mellom myndigheter og industrien best kunne ivareta de nasjonale strategiske interessene. Dette bidro til et godt og tett samarbeid mellom Forsvaret og industrien på en rekke områder og med en rekke produkter av høy internasjonal klasse.

Etter år 2000 har det skjedd en rekke endringer, bl a gjennom stortingsdokumenter, som gjør at den nasjonale strategien ikke lenger anses som gjeldende. Forsvaret har i samme periode hatt en sterk omstilling med lite penger til nyinvestering. Det har også vært en utbredt oppfatning om at en ikke skulle utvikle ting nasjonalt, men kjøpe utstyr som andre nasjoner har tatt fram. Dette medførte at den nasjonale industrien, som har levert en stor del av den arven Forsvaret har innenfor sin informasjonsinfrastruktur (INI), er i ferd med å avvikle sitt engasjement. Dette vil få store konsekvenser for videreføring av arven innenfor INI.

Basert på denne bakgrunnen har FD gitt i oppdrag til Forsvarets forskningsinstitutt (FFI) å se på hvordan samarbeidet mellom Forsvaret og nasjonal industri igjen kan styrkes. Oppdraget er strukturert som følger:

Foreta en gjennomgang og analyse av:

1. *Forsvarets IKT – portefølje for å avklare hvilke systemer som bør vedlikeholdes/videreutvikles i samarbeid med industrien. Arbeidet skal skje i samarbeid med Programområde INI.*
2. *Hvilken nasjonal kompetanse som er nødvendig innen dette feltet, herunder hvilke kapasiteter (kunnskap og volum) Forsvaret må besitte og hvilke som kan settes ut til industrien når det gjelder både vedlikehold og videreutvikling av arven.*
3. *Hvilke kriterier som må etableres for å skille industriens rolle som leverandører og rådgivere slik at en unngår en blanding av disse.*
4. *Hvilke firmaer som er de mest aktuelle for utvikling av et samarbeid. I denne sammenheng skal de mest kritiske prosjektene prioriteres.*
5. *Behovet for en avtalestruktur mellom forsvaret og industrien for de mest tidskritiske prosjektene, samt utarbeide forslag til intensjonsavtaler.*

Oppdraget er gjengitt i sin helhet i Anneks A

2 METODIKK

I arbeidet med rapporten har vi tatt utgangspunkt i ”Policy for militær tilpasning og anvendelse av informasjons- og kommunikasjonsteknologi i Forsvaret”, utgitt av FD i september 2005. Her er det blant annet beskrevet et tjenesteorientert arkitektur som en referansemodell for INI. Denne modellen er lagt til grunn ved utarbeidelse av den overordnede materiellplanen for programområde INI, utgitt vinteren 2006, og som beskriver i generelle termer de områdene en vil satse på gjennom de neste fire årene. Dette representerer det viktigste grunnlaget for å besvare punkt 1 i oppdraget.

Videre har det vært nødvendig for å kunne si litt om den nasjonale kompetansen, spesielt innad i Forsvaret, å innledningsvis se på hvilke miljøer som er hovedaktører innenfor IKT-virksomheten.

Det er videre utarbeidet 3 andre FFI rapporter som berører spørsmål 3 og 5. Disse ser hhv på industriens rådgiverrolle, bruk av industri i internasjonale operasjoner samt forslag til fremtidig avtalestruktur innenfor IKT området.

3 SAMMENDRAG

I kapittel 4 gjennomgås det utgitte policy dokument for IKT sektoren i Forsvaret. Som det fremgår her, kan ikke betydningen av IKT for Forsvaret undervurderes. Dette gjelder både for den interne effektivisering av Forsvaret, samt å oppnå effektgevinster i et moderne operativt nettverksbasert Forsvar.

Bærende elementer for å oppnå disse mål, er behovet for sentral styring av IKT området i Forsvaret noe denne rapporten slutter seg helhjertet til. Det pekes likevel på at dagens organisering og ansvarsfordeling kan synes fragmentert. Et annet og viktig verktøy som policydokumentet viser til, er å få til en effektiv læringsprosess. En slik prosess må involvere alle aktører både interne og eksterne. Vi er enige i dette, men det kan fortsatt gjøres en del håndgrep for å få til en mer effektiv kunnskapsdeling internt i Forsvaret samt med relevante eksterne aktører.

I kapittel 5 gjennomgås nærmere organiseringen av Forsvarets IKT virksomhet. Som allerede indikert i kapittel 4, synes det å være svært mange aktører som har forskjellige og til dels overlappende roller/ansvar. Gjennomgangen viser at det utover det formelle ansvar som FD har, er 2 sentrale hovedaktører, hhv FK KKIS og FLO/IKT. FK KKIS har konfigurasjonsansvaret for tjenestestrukturen, mens FLO/IKT har konfigurasjonsansvaret og er fagmyndighet for den tekniske infrastrukturen. Det er selvfølgelig mye kommunikasjon og samarbeid mellom de ulike aktørene. De tildels svært spredte miljøene med ansvar innen dette feltet, gjør det likevel vanskelig å få til en effektiv ressursbruk.

I kapittel 6 gjennomgås Forsvarets IKT-portefølje. Denne er stor og omfattende, og inneholder systemer og teknologier som er utviklet og anskaffet over lang tid. Utviklingen har stort sett foregått i de enkelte forsvarsgrenene, skreddersydd for å ivareta de spesielle behov som de enkelte operative og logistiske miljøene måtte ha. Dette har ført til gode løsninger for den enkelte bruker, men i arbeidet mot visjon om nettverkbasert Forsvar i 2014. er det behov for en betydelig samordning og sentral styring av framtidige investeringer.

Vi ser at det er særdeles viktig å ha nasjonal kompetanse både om strukturen i arven, og om hvilke trender som kan forventes i framtiden. Ved modernisering av deler av strukturen må en kunne holde oversikt over hvilke implikasjoner dette får for andre deler av strukturen, samtidig som en skal ivareta kravene til interoperabilitet på alle nivåer, nasjonalt og internasjonalt.

I Forsvaret opererer en i dag med perspektiv fram til 2014, med et delmål for 2008. For å kunne arbeide målrettet mot en framtidig struktur er det derfor nødvendig med strukturert og bred tilnærming, noe FDs policydokument (1) legger opp til. Industrien sitter på dyptgripende kompetanse om store deler av arven innenfor INI, samtidig som de er oppdatert på teknologiutviklingen innen dette feltet, både nasjonalt og internasjonalt. Vi ser således det slik at industrien vil kunne være viktig bidragsytere med hensyn til å gjøre de riktige fremtidsrettede valg. En forutsetning for å få dette til er at Forsvaret klarer å skape rammevilkår omkring et slikt samarbeid som gjør det interessant for industrien å engasjere seg.

I kapittel 7 gjennomgås nasjonal kompetanse innenfor nøkkelområder. Det heter seg at teknologi er universell. Det er kun på anvendelse av teknologien at vi skiller mellom sivil og militære applikasjoner. I FDs policy (1) påpekes nettopp dette.

Den nasjonale IKT-kompetansen er betydelig, og på enkelte områder er norske bedrifter ledende i verden. Det er også en betydelig innovasjon innenfor dette feltet, der IKT-løsninger stadig tas i bruk på nye måter og områder. Dette innebærer mange muligheter, men også nye trusler for bruk av IKT i Forsvaret. De viktigste utfordringene er først og fremst koblet til krav til sikkerhet, helhetlig arkitektur, fleksibilitet og kapasitet.

Skal Forsvaret kunne nyttiggjøre seg ekstern IKT kompetanse, må en være betydelig mer åpen i sin kommunikasjon med industrien enn tilfellet har vært hittil. På sikt kreves det en noe mer deskriptiv kommunikasjon og en enda mer involverende holdning og langsiktig samarbeid til industrien for å få gevinst for alle parter. Et sentralt grunnlag for en slik tilnærming er at Forsvaret besitter tilstrekkelig kompetanse til å forstå og utnytte de muligheter som ligger i markedet, og har tilstrekkelig kompetanse til å opptre som en likeverdig partner for industrien.

I kapittel 8 gjennomgås bruk av industri i en mer detaljert grad. Man redusere risikoen ved anskaffelser betydelig ved å involvere kompetent industri i konseptarbeidet og kravformulering før myndighetene godkjenner prosjektene for gjennomføring. Til tross for mange klart uttalte målsettinger om å satse på tidlige faser i prosjektene, blir ikke industrien invitert til deltagelse før kravspesifikasjonen er skrevet. Det bør derfor ses på i hvilken utstrekning en kan etablere en struktur for på en bedre måte å ta vare på teknologiutvikling knyttet til Forsvarets egne systemer. Dette setter krav til informasjonstilgangen i tidlig fase av prosjekter, ikke bare i forhold til selve prosjektet, men også tilhørende systemer som det nye systemet skal integreres

mot, noe som er relevant innenfor IKT området.

Behovet om informasjons- og kunnskapsdeling i tidligfase krever en eller annen form for tett samarbeid, enten det er kalt partnerskap, allianse, governance contracting eller partnering[1]. Konseptuelt følges dette opp i FD sitt konsept for Offentlig Privat Partnerskap (OPP), hvor Partnering er et sentralt virkemiddel. Et samlet leveranseansvar i hele livssyklusen gir leverandøren mulighet til å planlegge langsiktig og komme med innovative løsninger til beste for begge parter.

Gjennom ARF[2] har FD gitt de overordnede rammebetingelser for gjennomføring av fremskaffelser. FD har vide fullmakter og rammer for gjennomføring av anskaffelser utenfor EØS området. Når det gjelder bruk av eksterne rådgivere som deltar i kravspesifikasjonsarbeid, skal disse være leverandøruavhengige. Siden Forsvarsmarkedet er snevert, tas det høyde for å likevel kunne bruke rådgivere med leverandørtilknytning/leverandører. For å kunne gjøre dette, er det et krav om at slike rådgivere benyttes på en måte som ikke påvirker konkurranseforholdet mellom framtidige tilbydere. Videre skal kravspesifikasjonen utarbeidet med assistanse fra slike rådgivere, bli gjort tilgjengelig for et utvalg leverandører for kommentering før den endelige forespørselen/anbud sendes ut.

Denne muligheten er tatt inn i ARF for i større grad kunne utnytte leverandørenes kunnskap for å utarbeide kosteffektive krav uten å ødelegge konkurransemomentet, og er en oppmykning fra tidligere regler. Det presiseres at FD kan foreta ytterligere hensiktsmessige og saklige avvik fra dette ut fra næringspolitiske hensyn.

Hittil synes man å ha hatt en altfor ad-hoc messig og kortsiktig tilnærming til porteføljen av forsvarsrelevante IKT systemer. Siden Forsvaret i tillegg har mistet mye kompetanse, er det et klart behov for å skape en arena hvor Forsvarets gjenværende ekspertise innenfor både operativ, forskning og teknisk område kommer sammen med relevant industri. I denne sfære er det en nødvendighet i å etablere et langvarig forhold til en systemintegrator som både kan opptre som rådgiver og som leverandør avhengig av omstendighetene. Vi foreslår å inngå en Partnerskapsavtale med en overordnet systemintegrator/rådgiver. En mulighet her er å bygge videre på CCIS House avtalen med nødvendige justeringer.

4 POLICY FOR IKT OMRÅDET I FORSVARET

Høsten 2005 ga Forsvarsdepartementet ut *Policy for militær tilpasning og anvendelse av informasjons- og kommunikasjonsteknologi i Forsvare* (1). Dette er et viktig og godt dokument for den videre utviklingen av informasjonsinfrastrukturen. Hensikten med policyen er *å skape grunnlag for en felles virksomhetskultur i Forsvaret for militær tilpassing og anvendelse av informasjons- og kommunikasjonsteknologi (IKT). Dette innebærer spesielt å synliggjøre et*

[1] I den sammenheng viser vi til UK MOD sitt White Paper som klart poengterer viktigheten og den suksess de hittil har hatt med å implementere Partnering for de rette prosjekter, se spesielt s.31 og 134

[2] Anskaffelsesregelverk for Forsvaret

felles målbilde, samt å gi sentrale føringer. Således har policyen både en forklarende og en styrende funksjon.

En viktig føring i policy-dokumentet er avsnittet om sentral styring:

IKT er et sentralt virkemiddel i den ønskede transformasjonen mot nettverksorienterte operasjonsformer. For å unngå betydelige utgifter gjennom suboptimal anvendelse og mangel på helhetlig gevinstplanlegging, kreves sentral styring av området på strategisk nivå med fokus rettet mot spesielt tre områder:

- *Helhetlig planlegging og strukturering av militær tilpasning og anvendelse av IKT i Forsvaret.*
- *Overordnet styring og kontroll av IKT-investeringene og –drift.*
- *Rådgivning til politisk og militær ledelse i forhold til muligheter og begrensninger hva angår militær tilpasning og anvendelse av IKT.*

Styring av militær tilpasning og anvendelse av IKT skal gjøres gjennom anvendelse av arkitekturer. Fokus skal legges på å identifisere de viktigste egenskapene ved Forsvarets virksomhet, samt grensesnitt og informasjonsflyt mellom ulike deler av virksomheten.

Poenget med sentral styring er ikke så vanskelig å forstå. Ser en på informasjonsinfrastrukturen som et system der ulike komponentene skal spille sammen, må det være noen som har konfigurasjonskontroll. Men det er mange aktører i dette bildet. Det er ikke lett å se hvem som sitter med den hele og fulle oversikten til å kunne sies å ha konfigurasjonskontroll over det totale system..

Sett fra utsiden, er det heller ikke lett å se de formelle ansvarslinjene i organisasjonen med ansvar for IKT. Dette har også blitt bekreftet gjennom samtaler med de ulike miljøene i Forsvaret og ved FFI. Selv om FLO/IKT formelt sett er fagmyndighet for i hvert fall den tekniske IKT-strukturen, med hardware og applikasjoner, er det en rekke utredninger og beslutninger som fattes på høyere nivå i organisasjonen uten at de er med. Kontakt med fagmiljøer utenfor Forsvaret, det være seg industri eller FoU miljøer, synes å skje fra alle aktørene som er beskrevet nedenfor.

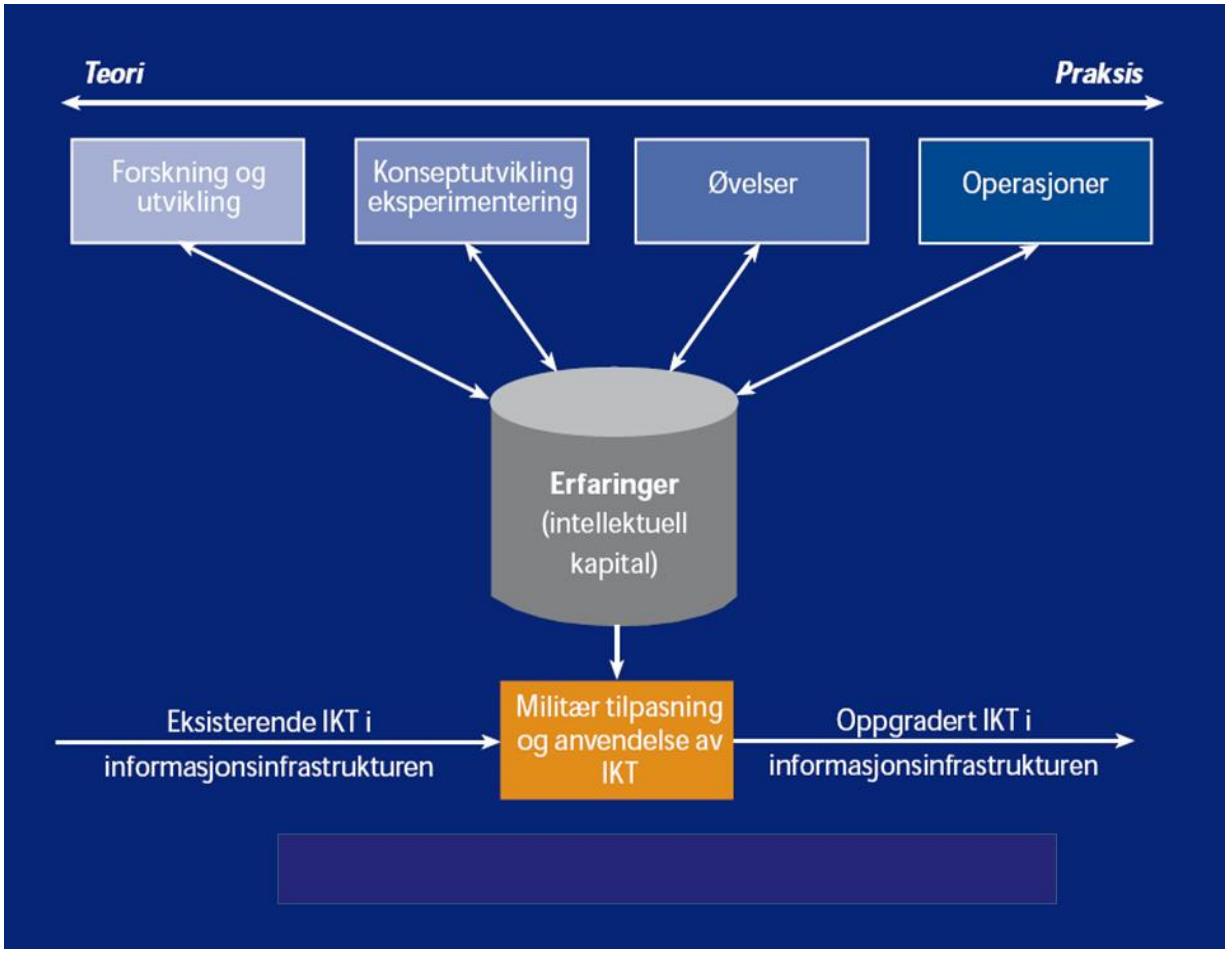
Nedenfor vil vi gå igjennom de sentrale hovedaktører innenfor IKT området, og prøve å beskrive deres forskjellige roller.

4.1 Prosess for militær tilpasning av IKT

I policydokumentet (1) fremheves betydningen av å ta lærdom av både positive og negative erfaringer, og forvalte erfaringene på en måte som kommer den enkelte medarbeider og Forsvaret til gode. For planlegging av investeringer gir dokumentet følgende føringer:

Ved planlegging av investeringer i IKT skal alternative fremskaffelsesstrategier alltid vurderes, for eksempel ulike løsninger for offentlig privat partnerskap. Det må likeledes under

planleggingen klarlegges hvilke drifts- og vedlikeholdskostnader som bevilgningsfinansieres, og hva som vil bli dekket gjennom horisontal samhandel.



Figur 4.1 viser en generell prosessmodell for hvordan forskning, eksperimentering, konseptutvikling, øvelseserfaring og operasjoner gjensidig bidrar til å utvikle kunnskap om hvordan moderne IKT kan tilpasses og anvendes militært.

Figur 1 viser hvordan en ser for seg å utnytte kunnskapen fra hele verdikjeden til å videreutvikle eksisterende INI til framtidens INI. Slik det er framstilt, kan det tolkes slik at kunnskap ervervet gjennom forskning, konseptutvikling og eksperimentering, til erfaringer gjennom øvelser og skarpe operasjoner, skal samles og deles med aktørene. Den intellektuelle kapital en på denne måten erverver seg, skal så brukes til å designe og utvikle fremtidens struktur. Dette er et viktig og nødvendig prinsipp for å henge med i og helst ligge i forkant av den teknologiske utviklingen.

Den teknologiske utviklingen innen IKT har medført store endringer i måten å gjennomføre militære operasjoner på, og det er kun gjennom å beherske hele verdikjeden en kan klare å utnytte denne muligheten optimalt, og derved få best avkastning for sine investeringer. Dette anses av de fleste nasjoner å være så viktig at de ønsker å ha en egen kompetanse på dette feltet for å kunne henge med i utviklingen, og være i stand til å tilpasse sin egen struktur til den nye

måten å operere på. Det norske forsvaret har inntil nylig løst dette ved å avsette egne midler til prøver og forsøk. Den økonomiske situasjonen i Forsvaret de to siste årene har imidlertid ikke muliggjort dette, noe som blant annet har ført til stagnasjon og forringelse av den betydelige IKT arven som forvaltes.

Gjennom at flere bygger opp kompetanse på dette feltet, vil muligheten for tradisjonell eksport bli redusert. Derimot vil muligheten for konstruktivt flernasjonalt samarbeid kunne oppnås, og derigjennom standardisering og interoperable løsninger.

Gjennom arbeidet som lå til grunn for revisjon av de teknologiske kompetanseområdene for Forsvaret og norsk forsvarsindustri, som FD presenterte for Stortinget i St prp 1 (2005-2006), ble det fra Forsvarets side påpekt at en satsning innen IKT, både i Forsvaret og i industrien, er helt avgjørende for å kunne lykkes med implementering av NbF konseptet. Det er viktig å understreke at den intellektuelle kapitalen ikke bare forvaltes av Forsvarets eget personell, men i like stor grad finnes i industrien. En viktig forutsetning for å kunne nyttiggjøre seg denne kompetansen, er at Forsvaret åpner opp for informasjonsdeling med industrien.

Det er pr i dag ingen strukturert prosess der industrien bringes inn i diskusjon om fremtidig utvikling og valg av fremtidsrettede løsninger for å få til en helhetlig informasjonsinfrastruktur. Å skape en arena for tettere samarbeid og bygging av tillit mellom Forsvaret og de industrielle aktørene, vil trolig være den investeringen som alene vil kunne gi den størst avkastning, både på kort og lang sikt. I kapittel 8 gjennomgår vi nærmere de praktiske forhold rundt det å skape en slik arena.

Hoveddelen av INI er og vil også i fremtiden bli levert av industripartnere. Erfaringene viser også at det ofte er behov for å gjøre endringer og tilpasninger under operasjoner. Dette er betydelig lettere om kompetansen og kapasiteten forefinnes internt i Forsvaret, eller hos nasjonal industri, enn om en må søke støtte fra utenlandske leverandører. Dette forholdet er mer utførlig omtalt i FFI/Rapport 2006/01115 Industriens rolle som både leverandør og rådgiver – muligheter og begrensninger (6).

5 ORGANISERING AV IKT-VIRKSOMHETEN I FORSVARET

5.1 Hovedaktører i IKT-prosessene

Selv om det formelt sett ikke er en del av oppdraget, ble det vurdert som nødvendig å se på hvordan Forsvaret har organisert IT-virksomheten innad i egen organisasjon, og kartlegge de forskjellige hovedaktører og deres roller. Dette er kort beskrevet i de etterfølgende avsnitt. Hovedpoenget er at en effektiv organisering er avgjørende for å lykkes innenfor et såpass komplekst område som IKT. Sett fra utsiden er det ikke lett å orientere seg om hvem som sitter med ansvaret for hva i Forsvarets organisasjon. Det er heller ikke lett å få øye på hvor ansvars- og myndighetslinjene går mellom de ulike aktørene. Spesielt blir dette viktig i relasjon til eksterne leverandører. Det kan virke som om det er mange innfallsporter til Forsvaret, med de

fordeler og ulemper det måtte medføre.

5.2 Programområdet informasjonsinfrastruktur (INI)

Programområdet INI som er organisert under FD IV 3 Teknologiutvikling og IKT, har et overordnet ansvar for å planlegge og styre utviklingen innen IKT-feltet. For å kunne gjøre dette på en forsvarlig måte er det nødvendig å holde god kontakt med brukermiljøene, representert av FOHK og Forsvarsgrenene. I tillegg må INI være i stand til å identifisere de viktigste faktorene i forhold til valg av fremskaffelsesløsning basert på strategier og trender innen sivil og militær IKT.

Ideelt sett bør også valg som berører IKT-området på våpensystemer og plattformer koordineres med programområdet. Ikke minst må INI være i stand til å følge med i den organisatoriske og ressursmessige utviklingen av Forsvaret for at de valg og disposisjoner som INI gjør kan bli realisert og få den forventede effekt.

I og med at IKT griper inn i de aller fleste områdene, fra ren fredsforvaltning til den ytterste spisse ende, blir INIs arbeidsfelt svært stort og bredt. Hvis en så legger til at området fortsatt preges av en rivende utvikling, der det hele tiden vil være behov for tilpasninger til den operative strukturen, gir det seg selv at det kreves en svært god innsikt og kunnskap i tillegg til kapasitet for å leve opp til forventningene.

I FFI Rapport ”Operative beslutningsstøttetjenester – fremtid NBF” (5) hevdes det at *en fremtidig K2IS løsning må speile organisasjonens behov og ønske om tilpasningsdyktige strukturer. Ny kapasiteter (sensorer) må kunne plugges inn, og interoperabilitet med logistikk- og støttevirksomhet vil også bli stadig viktigere. Dermed står vi ovenfor en transformasjon av dagens løsninger, slik at informasjon (både strukturert og ustrukturert) kan deles mellom langt flere enn i dag, og på tvers av organisasjonen. En viktig faktor vil være å få alle kommunikasjonsnettverk til å spille sammen (interoperabilitet på datanivå), men dette er ikke alltid nok. For å få best mulig tilgang til informasjon, må vi også ha interoperabilitet på informasjonsnivå.*

Videre sies det at *en god løsning for K2IS i 2014 bør være fleksibel, slik at den er godt rustet til å imøtekomme nye behov som ikke fantes da systemutvikling begynte. Løsningen vil måtte støtte et mangfold av ulike utvekslingsformater, protokoller, nettverksteknologier og ytelsesbegrensninger, både i nettverk og på maskiner. Interoperabilitet med andre organisasjoner, også frivillige, blir et viktig behov som nye løsninger må støtte. Det vil da være viktig å kunne filtrere informasjon som ikke skal deles med andre, avhengig av hvordan dette til enhver tid er definert.*

I tillegg er det viktig å kunne tilpasse systemets funksjonalitet til gjeldende oppdrag og styrkesammensetning, noe som kan endres relativt raskt, i hvert fall i forhold til tiden det kan ta å rekonfigurere et system. En løsning bør kunne støtte håndholdte terminaler så vel som server-baserte kommandoplasser som har et eget lokalnett. I tillegg vil gjenbruk av programvarekomponenter være viktig, dette for å spare kostnader på lang sikt, ved for eksempel

å gjenbruke rammeverk for kartbaserte applikasjoner.

Bruk av åpne standarder blir stadig viktigere for å sikre interoperabilitet med et mangfold av samarbeidspartnere. Det finnes mange definisjoner av en åpen standard.. Vi gir her et sammendrag av elementer som inngår i flere definisjoner:

En åpen standard blir utviklet i en åpen, inkluderende prosess der enhver organisasjon, bedrift eller offentlig enhet kan delta. En slik standard er ikke-proprietær og teknologinøytral, og er fritt tilgjengelig for distribusjon.

Med denne skissen til fremtidige utfordringer, ser en klart hvilke enorme utfordringer INI står ovenfor når de skal utforme konsepter og definere anskaffelser.

5.3 Forsvarsstaben – FST

Forsvarsstabens underlagte avdelinger vil spille en sentral rolle i å styrkeprodusere og sette opp kjernekapasiteter for hele FMO. Forsvarsstaben består av i alt seks staber: Fellesstaben, Personell-, økonomi- og styringsstaben (PØS), Sjøforsvarsstaben, Hærstaben, Luftforsvarsstaben og Heimevernstaben.

Fellesstaben har i denne sammenheng kundeansvar for felles IKT-tjenester, og er foresatt for FK KKIS. Fellesstaben har også etablert et eget endringsråd for Forsvarets SATCOM-infrastruktur og tjenester. Generalinspektørene med sine staber har ansvar for styrkeproduksjon, inklusive materiellanskaffelser til egen forsvarsgren (Totalprosjektansvarlig). Selv om mye av det som anskaffes innenfor IKT er felles, vil det alltid være behov for spesielle tilpasninger mot plattformer og utstyrsanskaffelser innenfor den enkelte forsvarsgrens domene. Forsvarsgrenene er derfor sentrale aktører som må trekkes inn i arbeidet med INI.

5.4 Forsvarets kompetansesenter for kommando og kontroll informasjonssystemer - FK KKIS

I visjonen for FK KKIS heter det at de gjennom innovasjon og samarbeid skal skape helhetlig infostruktur og kompetanse for et nettverksbasert og alliansetilpasset forsvar. Konkret er FK KKIS en sentral aktør i planprosessen på strategisk nivå, og utøver helhetlig styring og ledelse innen virksomhetsområdet INI i Forsvaret. I tillegg skal FK KKIS ha kapasitet til å stille en integrert KKIS enhet som skal støtte norske styrker nasjonalt og internasjonalt iht gjeldende operative krav, og er ansvarlig for å utarbeide konsept for anvendelse av INI i militære operasjoner.

FK KKIS har ansvar som funksjonell kravstiller til tjenesteinnholdet i INI. Under ledelse av FK KKIS er det igangsatt et arbeid med å etablere et konsept/regime for styring og ledelse av INI, herunder konfigurasjonsstyring og endringshåndtering. Sentrale aktører i dette arbeidet er blant annet FD, FK KKIS, FLO/IKT og FFI.

Det er også etablert et ”Endringsråd for Forsvarets SATCOM- infrastruktur og tjenester”, som er

et rådgivende organ i forhold til INI. Dette er sammensatt av representanter for FOHK, FLO/I, FLO/S, FLO/IKT og FST under ledelse av FK KKIS.

5.5 Fremskaffelsesorganisasjonen FLO/I

Alle større nyanskaffelser, uansett materielltyper går gjennom tre faser i henhold til prosjektmodellen PRINSIX: Konseptfasen, definisjonsfasen og framskaffelsesfasen. Mens de to første fasene er ansvaret til FD IV, gjennomføres selve fremskaffelsen av FLO/I med FD V som overordnet ansvarlig. . FLO/I besitter egne ressurser for prosjektledelse og -styring men skal selv ikke ha fagressurser med hensyn til det faglige innholdet i materiellet som anskaffes. Her skal de knytte til seg ekspertise fra fagmiljøene i FLO, i IKT-sammenheng i hovedsak fra FLO/IKT. I tillegg blir FFI brukt noen ganger.

5.6 FLO/IKT

FLO/IKT har en sentral IKT rolle i Forsvaret med ansvar blant annet å levere IKT tjenester til Forsvaret med hovedfokus på å styrke operativ evne, herunder sikre en helhetlig og sammenhengende utvikling av IKT i Forsvaret. Videre skal FLO/IKT sikre en helhetlig teknisk IKT-arkitektur som skal understøtte hele Forsvarets funksjonelle og sikkerhetsmessige behov. Avdelingen har ansvaret for å forvalte Forsvarets IKT-systemer og sørge for forsvarlig drift og vedlikehold. FLO/IKT har også ansvaret for å utvikle og fremskaffe de IKT-tjeneser som Forsvaret har bruk for gjennom outsourcing eller ved egen produksjon. Tjenesten skal for Forsvaret være kostoptimal med vekt på tilgjengelighet, sikkerhet og kvalitet.

FLO/IKT er Forsvarets fagmyndighet innen IKT og konfigurasjonsansvarlig for den tekniske delen av strukturen. Til tross for dette, og en betydelig kompetanse innen sitt ansvarsområde, hevdes det at FLO/IKT gis liten mulighet til å utøve rollen og være faglig rådgiver til for eksempel FST og FD. FLO/IKT er på områdene IKT teknologi og –tjenester kanskje Forsvarets viktigste portal inn mot forsvarsindustrien nasjonalt og internasjonalt. De bør derfor i større grad tas med på råd i arbeidet med utvikling av konsepter for nye løsninger.

5.7 Forsvarets fellesoperative hovedkvarter – FOHK

FOHK er den sentrale fellesoperative kommandoen, og har ansvaret for å planlegge og lede Forsvarets operasjoner i fred, krise og krig. I tillegg har FOHK ansvaret for Concept Development and Experimentation (CDE) og Norwegian Battlelab and Experimentations (NOBLE). Både gjennom operasjoner, øvelser og eksperimentering, vil det være en rekke behov og tilpasninger som dukker opp. FOHK er derfor en viktig premissgiver for den mer operative utvikling av INI. Arbeidet som utføres i regi av NOBLE og CDE er også av stor interesse i forhold til industrielt samarbeid.

5.8 FFI

Som forskningsinstitusjon og rådgiver for FD spiller FFI en aktiv rolle i utviklingen av INI. Instituttet er i aktivt samarbeid med ledende institusjoner i inn- og utland, og har en betydelig kompetanse på området. Pr i dag har FFI tre større prosjekter direkte relatert til problemstillinger knyttet til NbF og INI, og som har til formål å støtte Forsvaret i arbeidet innen feltet. Disse er:

- NbF-grid: Formålet med prosjektet er å understøtte Forsvaret i arbeidet med å etablere en informasjonsinfrastruktur for fremtidig NbF. Prosjektet vil arbeide med infrastrukturen, fra fysisk nivå til transportmekanismer på applikasjonsnivå. De overordnede føringene for utvikling av infrastrukturen vil bli utarbeidet for nettstruktur, sikkerhetskonsepter og en migrasjonsstrategi for utvikling av Forsvarets nett. Detaljerte tekniske problemstillinger innenfor områder der Forsvaret har krav som krever militære løsninger blir belyst.

- NbF i Operasjoner: Prosjektet vil bidra til å belyse hvordan den praktiske transformasjonen fra dagens forsvar til et fremtidig nettverksbasert forsvar bør skje. Det legges vekt på felles/joint problemstillinger. Fokus ligger på taktisk nivå, men alle nivåer vil kunne berøres.

- NbF Beslutningsstøtte: Prosjektets fokus ligger i å utforske grunnleggende elementer i tjenesteinfrastrukturen og anvende dette på informasjonstilgang og –deling i omgivelser som krever ad hoc organisering av informasjonsflyt. Prosjektets rolle vil være å utvikle et målbilde i et 10-årsperspektiv samtidig som resultater underveis bringes inn i videreutvikling av dagens systemer.

Disse tre prosjektene har fram til nå produsert et 40-talls rapporter som Forsvaret har lagt til grunn i sitt arbeide med å utvikle strukturen. I forhold til samhandling med industrien kan det være et problem at mange av de publiserte rapportene er graderte.

5.9 Delkonklusjon

INI berører alle aktiviteter og alle ansatte i Forsvaret på en eller annen måte. Det er derfor ikke unaturlig at det er mange aktører involvert i prosessen med utvikling av området. Men med hensyn til direkte funksjonelt ansvar for selve strukturen er det likevel kun tre hovedaktører:

- FD gjennom Programområdet INI har ansvaret for overordnet planlegging og styring av IKT-virksomheten

- FK KKIS er Forsvarets virksomhetsarkitekt innen IKT med ansvar blant annet å beskrive Forsvarets funksjonelle behov og krav til IKT tjenester.

- FLO/IKT er Forsvarets IKT tjenestetilbyder og har forvaltningsansvaret for Forsvarets IKT systemer. FLO/IKT er Forsvarets fagmyndighet innen IKT med ansvar blant annet å sikre en helhetlig teknisk IKT-arkitektur som skal understøtte hele Forsvarets funksjonelle og

sikkerhetsmessige behov.

I tillegg til disse tre, er FLO/I myndighet for fremskaffelsesfasen for prosjekter, med FD V som overordnet godkjenningsmyndighet.

Selv om det selvfølgelig er en god del kommunikasjon og samarbeid mellom de ulike aktørene, kan det synes som om de mange og tildels svært spredte miljøene med ansvar innen dette feltet gjør det noe vanskeligere å få til en effektiv ressursbruk. Det er som sagt tidligere, ikke lett for en utenforstående å få øye på hvor skillelinjene med hensyn til ansvar og myndighet går mellom hovedaktørene. Selv om den formelle beskrivelsen av ansvars- og myndighetsområdet virker grei nok, er det vårt inntrykk at det hersker en viss usikkerhet internt om hvem som har ansvaret for hva. Det anbefales derfor at det gjennomføres en grenseoppgang der ansvar og myndighet til den enkelte klarlegges og holdes opp mot de øvrige aktørene, slik at en unngår uklarhet. Alternativt bør en se på muligheten av å samle hovedaktørene i en organisasjon.

6 FORSVARETS IKT-PORTEFØLJE

6.1 Arven

Forsvarets IKT-portefølje er stor og omfattende, og inneholder systemer og teknologier som er utviklet og anskaffet over lang tid. I tillegg har utviklingen stort sett foregått i de enkelte forsvarsgrenene, skreddersydd for å ivareta de spesielle behov som de enkelte operative og logistiske miljøene måtte ha. Dette har stort sett ført til gode løsninger for den enkelte bruker, men i arbeidet mot visjon om nettverkbasert Forsvar i 2014, er det behov for en betydelig samordning og styring av framtidige investeringer.

INI er svært sammensatt, og preges samtidig av at det er en rivende utvikling innen området. Det er derfor særdeles viktig å ha kompetanse både om strukturen i arven, og om hvilke trender som kan forventes og som det bør satses på i framtiden. Ved modernisering av deler av strukturen må en kunne holde oversikt over hvilke implikasjoner dette får for andre deler av strukturen, samtidig som en skal ivareta kravene til interoperabilitet på alle nivåer, nasjonalt og internasjonalt.

I Forsvaret opererer en i dag med perspektiv fram til 2014, med et delmål for 2008. For å kunne arbeide målrettet mot en framtidig struktur er det nødvendig med strukturert tilnærming, noe FDs policydokument (1) legger opp til.

6.2 Arkitektur

Fra (1) beskrives informasjonsinfrastrukturen: *Kjernen i militært tilpasset og anvendt IKT benevnes Forsvarets informasjonsinfrastruktur. Denne omfatter informasjon, prosesser, standarder og teknologi, samt menneskene som drifter og vedlikeholder den.*

Referansemodellen for informasjonsinfrastrukturen er gjengitt i fig 6.1. Som det framgår her,

består denne av funksjonsvise beslutningsstøttetjenester og kjernetjenester, bundet sammen av en kommunikasjonsinfrastruktur.

På sikt ønsker en å utvikle seg i retning av en tjenesteorientert arkitektur som på engelsk kalles for Service Oriented Architecture (SOA). En SOA er en arkitektur som består av en samling løst koblede tjenester, som igjen er en samling av funksjonalitet. Tjenester kan sammenlignes med komponenter, da disse også er basert på et klart grensesnitt, samt en datamodell for informasjonsutveksling. Tjenester kan konfigureres sammen, slik at systemet utfører den ønskede funksjonalitet til enhver tid, basert på de virksomhetsprosesser som systemet skal støtte. Det er viktig at tjenester er basert på åpne standarder, slik at interoperabel kommunikasjon kan oppnås til tross for forskjellig maskinvareplattformer, operativsystem og programmeringsspråk. Kommunikasjon må kunne gå over et nettverk.

I de føringer som er gitt i (1) skal informasjonsinfrastrukturen være et samvirkende nettverk fra strategisk til stridsteknisk nivå, både nasjonalt, med allierte styrker og koalisjonspartnere, samt med relevante sivile instanser. Interoperabilitet og sikkerhet anses som den viktigste føringen for videre utvikling av informasjonsinfrastrukturen. Dette krever en sentral styring av området på strategisk nivå.

I arbeidet med å kartlegge Forsvarets IKT-portefølje har vi tatt utgangspunkt i den inndelingen som er gitt i referansemodellen for informasjonsinfrastrukturen:

- Funksjonsvise beslutningsstøttetjenester med underliggende systemer
- Kjernetjenester med underliggende systemer
- Kommunikasjonsinfrastruktur

I kartleggingen har vi sett på i hvilken grad Forsvaret og industrien samarbeider om å ta fram gode løsninger, og hvordan dette samarbeidet fungerer i praksis.

Feil! Objekter kan ikke lages ved å redigere feltkoder.

Figur 6.1 viser referansemodellen for informasjonsinfrastrukturen. Den er basert på modelleringsarbeid i Forsvaret og tilsvarende arbeid hos allierte og i sivil sektor. Militær tilpasning og anvendelse av IKT skal fokusere løsninger som er så nær opp til referansemodellen som det er teknisk og økonomisk forsvarlig på realiseringstidspunktet.

6.3 Funksjonsvise beslutningsstøttetjenester

De funksjonsvise beslutningsstøttetjenestene understøtter grupper av brukere med felles informasjonsbehov og prosesstøtte.

6.3.1 K2 og ledelse

Dette er tjenester for å planlegge, lede og kontrollere Forsvarets virksomhet. Eksempler er

tjenester for utvikling av planer, ordrer og oppdrag, samt for simulering og analyse.

I henhold til overordnet materiellplan for perioden 2005- 2008 (3) planlegges variantbegrensning og modularisering av eksisterende operative beslutningsstøttetjenester iverksatt tidlig i planperioden med varighet på maks to år. Fokus flyttes fra applikasjon til løsninger som gjør informasjon og tjenester tilgjengelig gjennom standardiserte grensesnitt.

Tjenesten støtter seg i dag på en rekke systemer og applikasjoner. En viktig applikasjon er NORCCIS II som opererer på NORDIS-S/N-II plattform. Dette er løsninger som er tatt fram av FLO/IKT i tett samarbeid med Teleplan. Plattformen planlegges erstattet av FISBasis/H, som også utvikles av FLO/IKT i samarbeid med Teleplan, mens selve applikasjonen vurderes sammen med NORTaC-c2IS, der KDA, Thales og Ericsson er systemleverandører.

6.3.2 Manøveroperasjon

Tjenester for gjennomføring av militær virksomhet, dvs til støtte for de ulike typene operasjonsformer (land-, luft-, maritime- og amfibieoperasjoner, luft og missilvern, informasjons- og spesialoperasjoner samt krisehåndtering).

I (3) beskrives dette området under overskriften ”Beslutningsstøttetjenester for stridsteknisk nivå”:

Hensikten med denne typen beslutningsstøttetjenester er å legge til rette for å kunne utnytte nettverkseffekter i operasjoner på lavere nivåer i hele Forsvaret. Dette gjelder ned til enkeltenheter som fly, fartøy og kjøretøy, samt for relevante enheter ned til enkeltmann. Strategien er å gjøre grunnleggende tjenester tilgjengelig for mange, kontra mer avanserte løsninger til noen få.

Plattformer (fly, fartøy osv), som allerede har beslutningstøttetjenester, skal bindes sammen med nye løsninger til en helhetlig beslutningsstøttetjeneste for stridsteknisk nivå. I tillegg til samvirke og utveksling av informasjon innad i stridsgrupper, skal utveksling av informasjon og samhandling være mulig vertikalt i kommandokjeden og til sideordnede enheter. Styrkekomponenter, som inngår i internasjonale styrker, må kunne utveksle nær sanntid statusinformasjon til overordnede og sideordnede enheter fra andre land gjennom avtalte grensesnitt.

Tiltak innenfor dette området vil bli iverksatt fra tidlig i planperioden.

NORTaC-C2IS, inkludert interim Battle Management System (BMS) (for Hæren), er et sammensatt K2-system som støtter flere tjenesteområder, som K2, manøveroperasjoner, ildstøttetjenester og etterretning og overvåkning. Utviklingen er i sin helhet ivaretatt av CCIS House (THALES, KDA, Ericsson) som også har ansvaret for at løsningene fungerer. I praksis er KDA hovedleverandør.

6.3.3 Etterretning og overvåkning

Dette er tjenester for å bygge situasjonsbildet, f. eks tjenester for etterretning, rekognosering,

overvåkning og sensorstyring. Det omfatter et stort nettverk som produserer situasjonsbildet. Blant annet ligger hele kyst- og luftovervåkningssystemet med alle sine sensorer, styringssystemer, rapportgeneratorer, meldingstjeneste, linksystemer etc bak tjenesteproduksjonen for dette området. I tillegg kommer Hærens systemer for etterretning og overvåkning.

Norsk industri har bidratt til å ta fram mange delsystemer som i stor grad representerer ”limet” i denne strukturen.

Under overskrifte NATO Beslutningsstøttetjenester, beskriver (3) utviklingen i NATO med betydning for Norge:

Innføringen av Air Command and Control Systems (ACCS) er utsatt på grunn av forsinkelser i NATO-prosjektet, men det vil bli avsatt ressurser til forberedelser mot slutten av planperioden.

NATO Alliance Ground Surveillance (AGS) er planlag med initial operativ kapasitet i 2010. Norge må vurdere anskaffelse av eventuelle bakkestasjoner for å kunne ta ned innformasjon.

Utvikling og innfasing av Strategic Commanders Operations and Transformation Action Information System (BI-SC AIS) vil pågå i planperioden. Løsningen vil bl a ta opp i seg funksjonalitet som i dag dekkes av Maritim Command and Control System (MCCIS). Det vil være nødvendig å følge utviklingen på NATO siden for å sikre tilstrekkelig interoperabilitet.

6.3.4 Ildstøtte

Dette er tjenester for å styre og synkronisere ulik typer ild, f eks tjenester for lokalisering, målprosessering, målengasjement, valg av effektor og virkningsanalyse.

Dette området er ikke gitt noen beskrivelse i materiellplanen utover det som er sagt under sammensatte løsninger, tidskritiske sensor- og ildledelsestjenester, ref avsnitt 6.6.3

6.3.5 Beskyttelse

Tjenester for ARBC, fortifikasjon og andre beskyttelsestiltak. Det finnes i dag ingen oversikt som viser hvilke systemer/applikasjoner som støtter dette området.

I den overordnede materiellplanen for 2005-2008 (3) påpekes det:

Videreutvikling og eventuell fremskaffelse av operative beslutningsstøttetjenester f eks til de militære kapasitetene ARBC[3], NCAGS[4] og militære informasjonsoperasjoner. Slike tjenester skal tas frem med utgangspunkt i de variantbegrensede og modulariserte operative beslutnings-støttetjenestene.

Videreutvikling og eventuell fremskaffelse av operative beslutningstøttetjenester til de militære kapasitetene Atomic, Radiological, Bilogicaal and Chemical (ARBC), Naval coorination and

[3] Atomic, Radiological, Biological and Chemical

[4] Naval Coordination and Guidance of Shipping

Guidance of Shipping (NCAGS) og militære informasjonsoperasjoner skal tas frem med utgangspunkt i de variantbegrensede og modulariserte operative beslutningsstøttetjenestene, og at tiltak vil bli iverksatt fra midten av perioden.

6.3.6 Logistikk

Tjenester for å fremskaffe og opprettholde materiell stridsevne.

6.3.7 Personell

Tjenester for rekruttering, utvikling, anvendelse og avvikling av personell.

6.3.8 EBA

Tjenester for håndtering av eiendom, bygg og anlegg. Eksempelvis tjenester som støtter etablering og nedrigging av camp.

6.3.9 Økonomi

Tjenester for lønn og regnskap.

Logistikk, personell, EBA og økonomi kan sammenfattes under begrepet operativ støtte og forvaltning. Disse systemene ivaretas gjennom programområdet LOS (tidligere GOLF). Bruk av denne type tjenester i operasjoner, og dermed tjenester for informasjonsflyt, må vurderes som en del av programområde informasjonsinfrastruktur (INI).

For disse tjenestene har en valgt SAP som system, og har inngått en strategisk avtale med IBM Norge knyttet til utvikling og implementering av modulene. Selv om SAP er en av verdens store leverandører av denne type forvaltningssystemer, vil det alltid være behov for skreddersøm for den enkelte løsning. I tillegg vil det være behov for å trekke informasjon fra disse systemene over i de operative beslutningsstøttesystemene, kanskje spesielt innenfor logistikk.

6.3.10 Ad hoc tilpassede tjenester

Denne type 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.

Erfaringer fra ulike typer operasjoner tilsier at det alltid vil oppstå behov for tilpasning av systemene og tjenestene. I slike situasjoner er det viktig at Forsvaret selv besitter, eller har lett tilgang til tilstrekkelig systemkunnskap og kapasitet til å gjennomføre de tilpasninger som måtte være nødvendig.

6.4 Kjernetjenester

Kjernetjenestene er felles, og angir hvilken grunnleggende informasjons- og prosesstøtte som

kan leveres av informasjonsinfrastrukturen. At tjenestene er felles betyr ikke at alle har alt, men at tjenestene er standardiserte for hele Forsvaret.

6.4.1 Tjenestehåndtering

Dette er tjenester for eksempelvis systemovervåkning, sikring av tilgjengelighet og ulike typer callcentre (helpdesk)

Fra (3) henter vi: *Det er behov for konsolidering samt nye og mer hensiktsmessige løsninger innenfor områdene tjenesteadministrasjon, –orkestrering, –overvåkning og –rapportering. Bedret evne til styring, kontroll og overvåkning av tilgjengeligheten og kvaliteten på interne og eksterne tjenester bidrar både til kosteffektiv drift og effektiv utnyttelse av tjenestene i informasjonsinfrastrukturen.*

Det er en målsetting at tiltak som iverksettes skal bidra til å sikre effektivisering av ressursbruk. Tiltak innenfor dette området vil bli iverksatt i hele planperioden.

6.4.2 Sikre plattformer

Sikre kjøremiljøer med standard støtteverktøy (FISBasis Hemmelig/NATO Secret og FISBasis Begrenset/Ugradert).

Det fremgår av (3): *I perioden 2005-2008 vil innføring av FISBasis Hemmelig/NATO Secret sikre Forsvaret et sammenhengende system som utgjører felles kjernetjenester av typene sikker plattform på nasjonalt skjermet HEMMELIG nivå og NATO SECRET nivå. I første omgang skjer dette for prioriterte brukersteder, og legger forholdene til rette for videre arbeid med å standardisere og variantbegrense typen og antallet IKT løsninger i og på tvers av graderingsdomener.*

I 2006 vil deler av vedlikeholdet av FISBasis begrenset/ugradert bli håndtert i en eksisterende fremskaffelse. Fra og med 2007 skal drift og vedlikehold for denne sikre plattformen håndteres over drift/horisontal samhandel. Tilsvarende gjelder for FISBasis hemmelig/NATO Secret etter innføringen.

Videreutvikling av Forsvarets sikre plattformer skal skje i en felles aktivitet for alle graderingsnivåer. Fokus skal være på kostnadsreduksjoner for den stasjonære strukturen samt standardisering av sikre plattformer for deployerbare og mobile enheter. Dette vil skje mot slutten av planperioden.

Driften av FISBasis/Begrenset/Ugradert har vært ivaretatt av Siemens Business Services, men denne aktiviteten vil forskjellige grunner bli tilbakeført til Forsvaret i løpet av året. Forsvaret står selv som hovedansvarlig for utvikling av FISBasis/Hemmelig, og ser denne aktiviteten i sammenheng med at en bygger opp igjen kompetansen på FISBasis/B-U. Effektiv drift, med stadige oppdateringer og utskiftninger, krever bl a en god oppfølging av markedet med hensyn til tilbud, pris og kvalitet.

Tilbakeføring av driften av FISBasis U/B betinger en tilførsel av kompetanse og kapasitet ved

FLO/IKT. Med de begrensninger som ligger i bruk av årsverk innen FLO, er det et åpent spørsmål om hvilken annen aktivitet dette vil gå ut over, og om man i tilstrekkelig grad evner å prioritere ressursene optimalt.

6.4.3 Registertjenester

Forvaltning og formidling av tjenester i informasjonsinfrastrukturen. Et eksempel kan være oppslagstjeneste (”elektroniske gule sider”).

I (3) fremgår det: *Registertjenester er viktig for å forvalte og formidle informasjonen og tjenestene i informasjonsinfrastrukturen.*

For å håndtere en stor mengde tjenester, potensielt med dynamikk i tilgjengeligheten, er det viktig å kunne gjøre oppslag i et tjenesteregister. Et slikt tjenesteoppslag vil være basert på metadata om tjenester. Et slikt register kan ha flere former, og kan sammenlignes med gule sider eller en ”matchmaker-tjeneste”.

Akkurat som tjenester, vil søk etter (ofte ustrukturerte) informasjon være viktig. For å få til informasjonsoppslag, trengs metadata som beskriver innholdet i et informasjonsobjekt. Slike metadata bør eksistere ved siden av selve informasjonen (filer og dokumenter), og kan f eks inneholde informasjon om geografisk område, informasjon om tid og sikkerhetsklassifisering, samt lokasjonen til selve informasjonen.

En første versjon av et register for tjeneste- og informasjonsoppslag, vurderes innført mot slutten av planperioden.

Dette er et felt hvor det finnes tilgang til høy nasjonal kompetanse. Målighetene for å realisere målsettingen vil trolig kun være knyttet til økonomi og visse sikkerhetsmessige aspekter.

6.4.4 Geografiske tjenester

Tjenester for forvaltning og bruk av geografisk informasjon. Eksempelvis kartmotor med evne til å vise militær symbolikk, overlegghåndtering og grunnleggende tracking.

Omtalen i (3) er:

Eksisterende geografiske tjenester vil i planperioden bli etablert på Forsvarets standard sikre plattformer.

Forsvaret benytter i dag den digitale kartapplikasjonen MARIA, utviklet av Teleplan.

6.4.5 Informasjonsutveksling

Standarder og løsninger for informasjonsutveksling nasjonalt, med allierte styrker og koalisjonspartnere samt med relevante nasjonale instanser. Eksempler på denne type tjenester er meldingshåndtering, epost, datalinker og replikering.

Den videre utvikling beskrives som følger i (3):

Forsvaret har allerede en standardisert militær meldingstjeneste som er innført i deler av strukturen. Denne skal tilpasses behovene og begrensningene på taktisk nivå og erstatte andre eksisterende meldingsløsninger. Strategien er å gjøre denne tjenesten felles for de som planlegger, støtter, gjennomfører og leder operativ virksomhet. Dette gir Forsvaret en grunnleggende evne til informasjonsutveksling både nasjonalt og internasjonalt samt mot andre deler av Totalforsvaret.

Det skal etableres et felles sett av tjenester for informasjonsutveksling som sikrer interoperabilitet og fleksibilitet internt i Forsvaret, til andre nasjonale aktører samt til NATO og koalisjoner. Så langt som det er hensiktsmessig, skal disse fellestjenestene spenne på tvers av tjenesteområder, domener (operativt, operativt støttende og forvaltning) og på tvers av graderingsnivåer. Dette innebærer også informasjonsutveksling med effektor- og sensorkomponenter. Av disse to komponenttypene prioriteres i første omgang sensorer for å gi et mest mulig oppdatert datagrunnlag for beslutningskomponentene. Dette fordrer særlig tett kobling mellom programområdet informasjonsinfrastruktur og programområder som har ansvaret for sensorkomponenter.

Strategien er å etablere nye utvekslingsmekanismer som felles tjenester i form av moduler som kan gjenbrukes av ulike funksjonsvise beslutningsstøttetjenester. Fokus for disse tjenestene skal være deling av informasjon ved, så langt som det er hensiktsmessig, å benytte åpne produkt- og leverandøruavhengige industri- og allianse standarder og -modeller snarere enn å standardisere på lagringsmodeller og proprietære løsninger.

For å ivareta eksisterende løsninger, herunder taktiske datalinker, er det nødvendig å kartlegge hvilke formater som benyttes. Dernest skal det i samråd med sentrale brukere utarbeides en konsolidert liste over hva som er nødvendig å videreføre og hva som kan variantbegrenses.

Tiltak innenfor dette området vil bli iverksatt i hele planperioden.

Dette er et stort og sentralt område, med direkte kopling opp mot Forsvarets operativ evne. Innføring av Link 16 på flere av våre viktigste plattformer vil være et viktig skritt for å oppnå den foreskrevne interoperabilitet, både nasjonalt og internasjonalt. Gjennom den nylig inngåtte kontrakten på Link 16 bakkeinfrastruktur, vil Thales være en sentral leverandør for Forsvaret. Utbygging av mobil bakkeinfrastruktur for Link 16 er et nybrottsarbeid, som vil kunne gi ringvirkninger i flernasjonalt materiellsamarbeid, og derigjennom styrke den nasjonale kompetansen på området.

Integrasjon av linksystemene på plattformene for å sikre riktig og sømløs informasjonsflyt mellom de ulike sensor- og beslutnings- og effektorkomponentene er en meget utfordrende oppgave, som krever god systemkunnskap og integrasjonskompetanse.

Innenfor meldingshåndteringssystemer har Thales levert systemer som også er i bruk i NATO.

6.4.6 Informasjonsstyring

Tjenester for fangst, lagring, fusjonering og korrelering, gjenfinning og utnyttelse av informasjon.

I (3) gis følgende omtale:

Tilgang til store informasjonsmengder krever løsninger for håndtering av både strukturert og ustrukturert informasjon og ikke minst effektive tjenester for utnyttelse av denne. Felles tjenester for fangst, lagring og utnyttelse av ustrukturert informasjon vil stå i fokus og bør i størst mulig grad baseres på eksisterende IKT.

Når informasjon blir tilgjengelig fra mange ulike kilder, vil det oppstå overlapp og inkonsistens i informasjonsgrunnlaget. Det er derfor nødvendig med ytterligere tjenester for fusjonering og korrelering av informasjon slik at informasjonsgrunnlaget og ulike presentasjoner av dette blir mer konsistente og komplette.

Tiltak innenfor dette området vil bli iverksatt fra midten av planperioden.

Også på dette feltet er det rikelig med tilgang på kompetanse i den nasjonale sivile dataindustrien.

6.4.7 Samarbeidstjenester

Tjenester for lyd- og videotelefoni og annen online samhandling.

Denne typen tjenester gjør det mulig å jobbe smartere og mer effektivt sammen også for geografisk spredte og mobile enheter. Det finnes i dag kommersielle løsninger, som på flere områder trolig imøtekommer Forsvarets behov. Typiske eksempler på slike løsninger dette er videokonferanser, chat og dokumentdeling. Det må sikres at løsninger for slike tjenester, i tillegg til interoperabilitet internt i Forsvaret og til andre nasjonale aktører, gir interoperabilitet til NATO og koalisjoner. Videre må det sikres at Forsvarets behov imøtekommes på områder som for eksempel sikkerhet og sporbarhet.

Tiltak innenfor dette området vil bli iverksatt med pilotinstallasjoner i perioden.

Sentrale industriaktører innenfor dette tjenestefeltet er Nera Networks, Siemens, THALES; Tandberg med flere.

6.4.8 Informasjonssikkerhet

Området dekker Public Key Infrastructure (PKI), GSM kryptotelefoni, IP kryptering og andre typer tjenester for sikring av konfidensialitet, integritet og tilgjengelighet.

Området gis en utførlig beskrivelse i den overordnede materiellplanen (3):

Det er utfordringer knyttet til sikker informasjonsutveksling i et Nettverksbasert Forsvar. Spesielt gjelder dette sammenkopling av ulike nasjoners systemer, og informasjonsutveksling på tvers av sikkerhetsdomener. Innenfor planperioden skal Forsvaret frembringe og vurdere nye konsepter og arkitekturer for sikkerhet, samt prøve ut ulike former for sikkerhetsløsninger. Utviklingen av nye løsninger må skje i nær forståelse med våre nærmeste allierte. Målet på sikt (utover planperioden) er å ta frem nye sikkerhetsløsninger i informasjonsinfrastrukturen.

Tidlig i perioden starter innføring av en felles PKI (Public Key Infrastructure) løsning i Forsvaret. Dette gir en felles tjeneste for informasjonssikkerhet som støttes av applikasjoner tilgjengelig i markedet. Det er allerede valgt tekniske løsninger i Forsvaret (f eks FISBasis hemmelig/NATO Secret og FIF) som krever digitale sertifikater og PKI for å kunne operere. En felles løsning for PKI er viktig både med tanke på å sikre interoperabilitet og ikke minst for å spare investerings– og spesielt driftsmidler.

Forsvaret har tidligere brukt betydelige ressurser i samarbeid med nasjonal industri på utvikling av algoritmer og teknologiske løsninger for IP-kryptering. Dette gjør det nå mulig å oppgradere til en lang høyere ytelse for IP-basert kryptering. En slik oppgradering vil bli foretatt i midten av planperioden.

Sikkerhetsløsninger for å muliggjøre mobilitet ned til enkeltmannsnivå vil bli vurdert og innføring vil sannsynligvis bli startet opp i siste halvdel av planperioden.

Norsk kryptoindustri er verdensledende innenfor sine nisjer. Dette er resultat av et mer enn 50 år langt samarbeid mellom Forsvaret, sikkerhetsmyndighetene og industrien. Bl a har Thales i internasjonal konkurranse blitt valgt som leverandør av NATOs standard løsning for IP-krypto på alle graderingsnivåer. KDA har tilsvarende utviklet og levert en kryptert GSM telefon godkjent for hemmelig. Det tradisjonelt gode samarbeidet mellom Forsvaret og nasjonal industrien innen dette feltet, har resultert i at Norge ligger i forkant på dette området. Ingen andre nasjoner håndterer dette bedre enn oss, så dette bør være en nisje som det bør satses videre på. God sikkerhet er helt avgjørende for å kunne høste av de fordelene som nettverksbaserte løsninger byr på.

NATO tar sikte på å innføre SCIP (Secure Communications Interoperability Protocol) for å bedre interoperabilitet mellom deltagende nasjoner i internasjonale operasjoner. Utstyret skal dekke sikker tale og lavhastighets datatrafikk. Norge deltar i SCIP spesifikasjonsarbeid med NSM, FLO samt KDC og Thales fra industrien. SCIP er også det mest aktuelle alternativ for erstatning av NSK200 og TCE500. Dette er et aktuelt område å samarbeide med industrien.

6.5 Kommunikasjonsinfrastruktur

Kommunikasjonsinfrastrukturen tilbyr kvalitetssikrede mekanismer for forbindelse mellom beslutningsstøtte- og kjernetjenestene, samt koblinger mellom disse og de ulike beslutnings-, effektor- og sensorkomponenter. Det er de funksjonsvise beslutningstøtte- og fellestjenestene og i hvilke lokasjoner disse må være tilgjengelig som bestemmer egenskapene til kommunikasjonsinfrastrukturen. Tilsvarende må tjenestene ta hensyn til tekniske og fysiske begrensninger i den tilgjengelige kommunikasjonsinfrastrukturen.

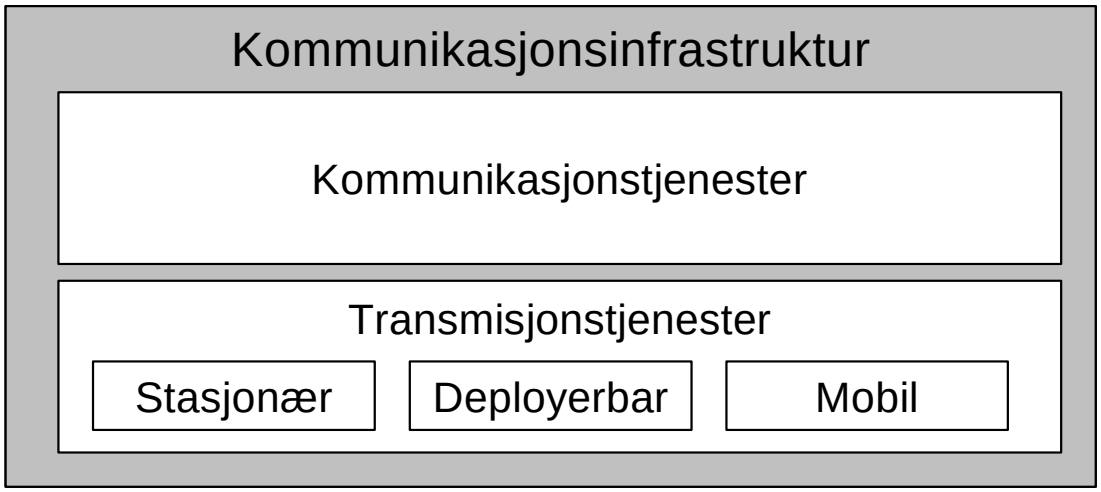


Fig 3 viser oppedling av kommunikasjonsinfrastrukturen

6.5.1 Felles integrerende kommunikasjonslag

I henhold til ”Overordnet materiellplan for programområde informasjonsinfrastruktur” (3) skal Forsvaret skal migrere til et felles integrerende kommunikasjonslag basert på IP-teknologi:

Forsvaret skal migrere til et integrerende kommunikasjonslag basert på IP-teknologi. Eksisterende løsninger som skal videreføres, skal migreres over til en infrastruktur basert på IP-teknologi når og hvis det er økonomisk hensiktsmessig ut fra levetidskostnader. Nye tjenester og plattformer skal støtte IP-teknologi når disse innføres.

Dersom kritiske tjenester ikke lar seg realisere med IP-teknologi (av økonomiske eller tekniske årsaker), kan andre løsninger implementeres med sameksistens og samtrafikk med en IP-basert infrastruktur.

Tiltak for å migrere til IP-teknologi vil bli iverksatt i hele planperioden.

IP er i seg selv ikke en målsetting, men et middel for å oppnå den fleksibiliteten som kreves. IP-teknologien er en aksessprotokoll som fungerer på tvers av forskjellige typer sambandssystemer, slik at den muliggjør enkel sammenkobling og interoperabilitet mellom deltakende enheter. Vi registrerer at svært mye forskning og utvikling innen nettverksløsninger med tilhørende tjenester og applikasjonsutvikling skjer innen IP teknologien. Utfordringen ligger i å etablere et fullt funksjonelt IP-nett med nødvendig sikkerhet, mobilitet og tjenestekvalitet. Det vil også være en utfordring å sjekke ut at de tjenester og applikasjoner som benytter kommunikasjonsinfrastrukturen støtter IP.

Industrien leverer alt utstyr til kommunikasjonsinfrastrukturen. Mange leverandører (blant annet Thales, Nera, Siemens, Cisco, Ericcson, KDC med flere) er involvert med delleveranser som Forsvaret setter sammen til en helhetlig kommunikasjonsinfrastruktur.

Oppgradering av arven til å møte de nye krav er en av de viktigste oppgavene i årene som kommer. Ettersom en stor del av kommunikasjonsinfrastrukturen er levert fra norsk industri, vil det være behov for et nært samarbeid mellom flere industriparter og Forsvaret for å finne

kostoptimale løsninger. Sammen med variantbegrensning, er dette sannsynligvis det området som i størst grad vil berettige en langsiktig avtale med et "Systemhus"

6.5.2 Stasjonært nett

Hovedelementene i det stasjonære nettet er Forsvarets stasjonære transmisjonsnett, FDN's IP-nett (InterLAN), FDN telefonnett, FDN punkt-punkt nett, Sivile linjer, NATO SAATCOM, Sivil satellitt, HF kringkaster, UHF radio, VHF radio, Mobiltelefoni (sivilt), Tetra, WLAN (sivilt), Trådbunnet LAN, Trådbunnet PABX.

Behovet i Norge for fastnett som møter spesielle militære krav vil være begrenset til et antall prioriterte militære installasjoner. Tilgjengelighet, krav til oppetid og sikkerhet samt pris vil være avgjørende for hvorvidt Forsvaret skal konkurranseutsette deler av sin kommunikasjonsinfrastruktur. (Migrasjonsrapporten side 16-17).

I den overordnede materiellplanen (3) beskrives den videre utviklingen som følger*:*

Forsvarets stasjonære nett må omstruktureres i tråd med endrede økonomiske rammer og operative behov. En sterkere grad av samordning med sivil teleinfrastruktur, kombinert med bruk av moderne teknologi som gir bedret kapasitet, er momenter som må utredes nærmere.

Mekanismer for effektive samhandling og integrasjon mellom militære og sivile kommunikasjonsløsninger skal innføres i løpet av planperioden.

Funksjonalitet for differensiering av tjenestekvalitet må innføres tidlig i perioden da dette bidrar til at de brukerne med høyest krav til kvalitet og sikkerhet ikke blir kostnadsdrivende for det stasjonære nettet totalt sett.

Forsvarsstaben gav i januar 2005 oppdrag om etablering av Forsvarets Felles Radio-organisasjon (FFR). Det konseptuelle grunnlaget baserer seg på at FFR skal opereres og driftes fra en hovedstasjon og en alternativt bemannet radiostasjon. Resterende bemannede nasjonale militære radiostasjoner legges ned. Muligheter for ytterligere samordning og effektivisering av radiotjenesten i Forsvaret må utredes nærmere.

Det legges med andre ord opp til en del utredningsarbeid på dette feltet. Industrien bør generelt inviteres til å bidra i arbeidet med å finne fram til gode og fremtidsrettede løsninger.

6.5.3 Deployerbart nett

TADKOM, MRR/MOT, Deployerbar kommunikasjonsmodul (DKM), WLAN (sivilt), Trådbunnet LAN, Trådløs PABX og Trådbunnet PABX. .

I (3) beskrives utviklingen de nærmeste årene som følger:

Militære operasjoner kan ha global utbredelse og enkeltoperasjoner dekker større områder enn tidligere. Dette setter nye krav til kommunikasjonsinfrastrukturen i forhold til hva dagens løsninger er designet for. For eksempel kan satellittkapasitet være nødvendig for å knytte sammen operasjonsområder i et felles nett.

Transportable løsninger er en forutsetning for å deployere kommunikasjonsinfrastrukturen. Et antall slike løsninger skal fremskaffes for å dekke behovet ved deployering i Norge og i internasjonale operasjoner.

Dagens områdenett (TADKOM) må migreres til IP-teknologi og få høyere kapasitet. Løsningen må ha stor fleksibilitet med hensyn til fysiske transmisjonssystemer, fra satellitt og militære radiosystemer (inkl radiolinje) til kommersielle løsninger.

Tiltak innenfor dette området vil bli iverksatt i hele planperioden. Dette innebærer også en studie av muligheter og løsninger for tiden etter TADKOMs levetid i løpet av planperioden.

Dette er løsninger som i stor grad er levert av norsk industri (KDA, Thales). Ved overgang til IP-teknologi i TADCOM, vil bl a dagens luftvernapplikasjoner måtte modifiseres for å kunne fungere tilfredsstillende

6.5.4 Mobilt nett

Består av elementene MMR/CNR, UHF-radio, VHF-radio og eleverte plattformer som f eks UAV og Aerostat. I (3) beskrives utviklingen som følger:

Tilnærming til et nettverksbasert forsvar vil kreve mer kapasitet enn dagens løsninger kan levere. I tillegg viser erfaringer fra internasjonale operasjoner og øvelser at det er behov for kommunikasjonskapasiteter med lang rekkevidde og EK-beskyttelse. Disse vil bestå av både militære teknologier med god beskyttelse og rekkevidde for å ta seg av det kritiske minimumsbehovet, og kommersielle teknologier som dekker de store kapasitetsbehovene. Militære sjø- og luftfartøyer må til enhver tid være utrustet i henhold til internasjonale sivile krav.

Flere av dagens radioløsninger har en begrenset gjenværende levetid. Videreføringer, oppgradering og erstatninger for disse må vurderes i hele perioden, herunder bruk av Software Defined Radio og forskjellige typer bredbåndsradioer. Likeledes må videreføring og erstatning for spesielle løsninger som følger av internasjonale avtaler og operasjoner vurderes.

Standardisering av kommunikasjonsløsninger for aktivitet som har noe mindre krav til sikkerhet i transmisjonen (f eks internt basenett, stridsdommernett, skytebanetjeneste etc) vil bli vurdert i løpet av planperioden.

Tilgang til det nasjonale nødnettet vil bli håndtert gjennom fremskaffelse av standardisert sluttbrukermateriell i et omfang tilpasset Forsvarets behov for å samhandle med nødetatene. En anskaffelse vil bli iverksatt dersom standardisert sluttbrukermateriell blir tilgjengelig i løpet av planperioden.

Norsk industri, i første rekke KDA og Thales, har levert systemer til denne delen av strukturen. KDA har tatt fram og levert MRR/LFR. Thales har sammen med FFI utført en del CDE-aktivitet rundt ad-hoc IP-nett.

6.5.5 Satellitt

Området består av NATO SATCOM og sivile satellitter.

Fremtiden for dette området beskrives som følger i (1):

Satellittkommunikasjon gir god fleksibilitet og kan brukes både som aksess for deployerte styrker inn til Forsvarets stasjonære nett, for mobile enheter og for å binde sammen segmenterte nett. Tilgang til sikkert romsegment, samt enhetlige og kosteffektive løsninger for tilgang til satellittkommunikasjon skal vurderes for hele Forsvaret sett under ett. Dette forventes å redusere kostnadene samt å gi bedre tjenester.

Tiltak innenfor dette området vil bli iverksatt fra midten av planperioden.

Norsk industri representert med KDA, Thales og Nera Networks har god kompetanse innenfor satellittkommunikasjon. Men satellittkommunikasjon må ses i sammenheng med den øvrige kommunikasjonsinfrastrukturen, der norsk industri har et godt fotfeste.

6.6 Sammensatte løsninger

Sammensatte løsninger består av elementer fra mer enn en av kategoriene over.

6.6.1 Taktisk datalink

Fra (3) henter vi følgende beskrivelse:

Taktisk datalink 16 implementeres på prioriterte plattformer i Forsvaret. Fremskaffelsen ivaretar de samlede behov for Link 16 utover FN-klasse fregatt, Skjold-klasse MTB og den initiale anskaffelse til F-16, og er en forutsetning og støtte for anvendelsen av disse. Dette inkluderer kapasiteter for å kunne øve Link 16 operasjoner i utvalgte områder, evne til å etablere Link 16 dekningsområder med mobile bakkestasjoner under øvelser og i internasjonale operasjoner, nettverk management, resterende terminaler til F 16, terminaler til luftvern og integrasjon til Forsvarets beslutningsstøttetjenester.

Link 16 fremskaffelsen pågår i hele planperioden.

Gjennom hard internasjonal konkurranse har Thales Norge fått oppdraget med å etablere Link 16 Bakkeinfrastruktur i Norge. Thales har derved tatt steget fullt ut som systemintegrator i det norske Forsvaret. KDA har fått ansvaret for å integrere Link 16 på NASAMS og på fregattene. Det kan derfor hevdes med en viss tyngde at vi har nasjonal kompetanse på dette feltet som Forsvaret kan støtte seg på.

6.6.2 Transportable IKT-løsninger

Fra (3) henter vi følgende beskrivelse:

Transportable IKT-moduler er en fellesbetegnelse på ulike IKT-løsninger beregnet på

avdelinger som deployerer nasjonalt og internasjonalt. Et minimum antall slike løsninger skal fremskaffes for å dekke deployerte enheter og avdelinger på høy beredskap samt en reserve som kan fungere som kombinert utdanningsmateriell og byttereserve.

Tiltak innenfor dette området vil bli iverksatt i hele planperioden.

De transportable modulene som Forsvaret har i dag, og som brukes som en deployerbar forlengelse av det stasjonære nettet, er satt sammen av moduler, produkter og del-systemer som er levert av et bredt spekter av norske leverandører, bl a KDA, Teleplan, Thales, Telenor, Siemens og Nera. I tillegg til selve kommunikasjonsutstyret vil det være behov for containere av forskjellige typer (Uniteam, TAM m fl), kabling, kraftforsyning, batterier, air condition osv. Alt dette skal settes sammen til et funksjonelt hele, noe nasjonal industri er fullt ut i stand til å ivareta.

6.6.3 Tidskritiske sensor- og ildledelsestjenester

Dette beskrives i (3):

Forsvarets sitter i dag med visse autonome systemer som opererer i sann tid. NADCORE, NASAMS og ODIN er eksempler på slike systemer. Fellestrekket er at de knytter sammen tilstrekkelig sensorinformasjon og beslutningsinformasjon til nær sanntid ledelse og avfyring av våpen.

For å realisere økt slagkraft skal felles tjenester innen området utredes. Det skal spesielt legges vekt på løsninger som er interoperable med NATO og viktige samarbeidspartnere. Det skal også vektlegges å etablere mobile fremfor statiske løsninger.

Teleplan, Thales, KDA og CCIS House er hovedaktørene bak de omtalte systemene. Løsningene representerer på sine områder høy internasjonal standard. F eks har KDA gjennom sitt samarbeid med Raytheon, USA, solgt NASAM Battle Management System i ulike varianter til en rekke land, og har også kontrakt med US Army for utvikling av tilsvarende system for deres luftvern.

6.6.4 NATO infrastruktur i Norge

Fra (3) henter vi:

NATO har fremdeles en del kapasiteter på norsk jord, vesentlig kostdelt med Norge. Trenden er at denne infrastrukturen får mindre fokus i NATO, og det er planer om å redusere spesielt på driftssiden. Eventuelle nasjonale behov knyttet til slike kapasiteter må klarlegges.

BRASS er et NATO prosjekt som tar for seg eksisterende radioressurser. Prosjektet vil ha aktivitet i Norge innenfor planperioden, og nasjonal utnyttelse av denne kapasiteten må klarlegges.

Eventuelle tiltak innenfor dette området vil foregå i hele planperioden.

6.7 Områder for samarbeid med norsk industri

Som det fremgår av ovennevnte gjennomgang, er ikke den overordnede materiellplanen spesifikk og konkret på tiltak, men skisserer områder der en har planer for de kommende fire år. Det vil heller ikke være riktig å være helt spesifikk i hvilke prosjekter som bør gå til de enkelte delene av industrien, da dette er avgjørelser som skjer gjennom fremskaffelsesprosessen. Det vil likevel være grunnlag for å peke på hvilke hovedområder der det synes å ligge tilrette for et *fortsatt* samarbeid med nasjonal industri, ettersom den har levert større deler av strukturen gjengitt i referansemodellen i INI.

6.7.1 Forvaltningssystemer

For forvaltningssystemene har en valgt å gå for SAP-løsning med IBM Norge som sentral støttespiller i utforming og leveranse av systemene. Gjennom dette valget har man inngått en langsiktig, strategisk allianse med leverandøren (SAP), selv om en fortsatt står fritt med hensyn til å bruke konsulenter som har SAP-godkjenning. Det antas dog at karakteren av samarbeidet med IBM Norge for design og implementering, utgjør et naturlig grunnlag for fortsatt samarbeid i lang tid framover. Alternativet vil være at Forsvaret bygger opp en egen organisasjon for å håndtere drift og vedlikehold av disse systemene etter at program LOS er avsluttet.

6.7.2 Operative beslutningsstøttetjenester

Innen de operative beslutningsstøttetjenestene er hovedsystemene både på strategisk og taktisk nivå utviklet i samarbeid med norsk industri. Det snakkes her om variantbegrensing og modularisering i de kommende fire år. Hovedelementer her vil være systemer som NORCCIS II, NORTaC og ildledelsessystemer som ODIN II og NASAMS. Alternativet til å videreutvikle disse systemene i samarbeid med leverandørene, er å foreta en total utskiftning med de konsekvenser det måtte medføre for helheten i strukturen.

Fordelen med å bruke nasjonal industri til utvikling og understøttelse av den operative strukturen, er mange. Ikke minst ser vi dette gjennom den understøttelse som industrien gir ved oppdukkende behov i skarpe operasjoner, senest demonstrert gjennom tilpasning av BMS-system for våre styrker i Afghanistan.

6.7.3 Kjernetjenester

Mange av områdene innenfor kjernetjenester har ren sivil karakter, og det finnes mange potensielle leverandører på de ulike områdene. Spesielt dersom Forsvaret selv velger å være systemintegrator. Området ”sikre plattformer” vil Forsvaret ta hånd om selv gjennom FISBasis B/U og FISBasis H/NS. Blant de øvrige områdene er der noen som peker seg spesielt ut for langsiktig samarbeid med forsvarsrelatert industri:

- ”Geografiske tjenester” er basert på kartapplikasjonen MARIA, som er utviklet av Teleplan, og som i perioden skal implementeres på Forsvarets standard sikre plattformer.

- ”Informasjonsutveksling” er sentralt i forhold til interoperabilitet både internt og eksternt, og har en sterk kopling mellom informasjonsinfrastrukturen og programområder som håndterer effektor- og sensorkomponenter. Nasjonal forsvarsrelatert industri har vært og er sterkt engasjert i utvikling av dette området, og det vil være naturlig å følge opp dette samarbeidet.
- ”Informasjonssikkerhet” er et område av stor viktighet i den militære informasjonssikkerheten. Løsninger som Forsvaret benytter i dag er i stor grad utviklet nasjonalt, og har også vunnet internasjonal anerkjennelse. Dette er en nisje som Forsvaret bør satse videre på i samarbeid med nasjonal industri.

6.7.4 Kommunikasjonsinfrastruktur

I henhold til den overordnede materiellplanen skal Forsvaret migrere til et felles integrerende kommunikasjonslag basert på IP-teknologi. Oppgradering av arven til å møte dette nye kravet blir kanskje den viktigste oppgaven på dette feltet i årene som kommer. Dette er i tillegg et område hvor det er behov for et nært samarbeid mellom flere industripartnere og Forsvaret for å finne kostoptimale løsninger. Sammen med variantbegrensning er det nok dette området som i sterkest grad nødvendiggjør et langsiktig samarbeid med et ”Systemhus” Her ligger alle forhold tilrette for å videreutvikle samarbeidet med norsk industri, både som systemintegrator, systemleverandør og delsystemleverandør. Samarbeidet med industrien vil også fortsette innen de underliggende transmisjonstjenester.

6.7.5 Konseptutvikling

I den overordnede materiellplanen for programområdet INI, sies det under flere av tjenesteområdene at det er behov for videre utredning før en kan beslutte veivalg og fremskaffelse. Dette åpner for muligheten til å trekke med industrien i utrednings- og planarbeid.

Konsept for fremskaffelse av materielle kapasiteter i forsvarssektoren, som FD utarbeidet i 2004, har som hovedpoeng at det skal legges betydelig økt vekt på de tidlige faser av fremskaffelsesprosessen. Dette medfører større ressursbruk tidlig i overensstemmelse med god prosjektteori og erfaring. Det skal også legges vekt på gjennomgående integrerte arbeidsprosesser, der ”*samtlige aktører innenfor investeringsvirksomheten vil få nye og bedre muligheter til å påvirke utvikling og resultat gjennom hele prosessen på en mer direkte og formålstjenlig måte”*.

Som påpekt tidligere, sitter industrien på en dyptgripende kompetanse om store deler av arven innenfor INI, samtidig som de er oppdatert på teknologiutviklingen innen dette feltet, både nasjonalt og internasjonalt, og vil kunne være viktig bidragsytere med hensyn til å gjøre de riktige fremtidsrettede valg. En forutsetning for å få dette til er at Forsvaret virkelig ønsker et langsiktig samarbeide med industrien og klarer å skape rammevilkår omkring et slikt samarbeid som gjør det interessant for industrien å engasjere seg. Mangelen på åpenhet fra Forsvarets side er kanskje den største hindringen for å få til et nasjonalt engasjement.

7 NASJONAL KOMPETANSE

Forsvaret anskaffer et bredt spektrum av elektroniske komponenter, produkter og systemer. Et utbredt anslag sier at elektronisk hardware og software utgjør ca 80 % av verdien av dagens militære plattformer og våpensystemer. Denne verdien vil sannsynligvis øke i takt med den teknologiske utviklingen. En tilsvarende utvikling ser vi på sivil side. De aller fleste produktene har et stort innslag av IKT i seg, og ikke minst er IKT det viktigste hjelpemidlet et moderne samfunn har til å effektivisere sin virksomhet og opprettholde sin globale konkurransekraft. Sett i dette lys, synes det åpenbart at det er et stort behov for å opprettholde en høy nasjonal kompetanse på dette feltet.

7.1 Sivil og militær teknologi

Det heter seg at teknologi er universell. Det er kun på anvendelse av teknologien at vi skiller mellom sivil og militære applikasjoner. I FDs policy (1) påpekes nettopp at *"Militær tilpasning med påfølgende anvendelse skal gis prioritet framfor utvikling av egne løsninger. Informasjonsinfrastrukturen skal således i størst mulig grad baseres på eksisterende teknologi, tilpasset og anvendt for å dekke Forsvarets behov. Forsvarets prosesser skal om nødvendig tilpasses slik at standardprosesser og standard programvare kan benyttes der dette er mulig."*

Videre fremgår det av dokumentet at *"Staten satser på å gjøre hverdagen enklere for innbyggere og næringsliv gjennom bruk av IKT. Elektroniske tjenester fra Forsvaret mot innbyggere og næringsliv, skal bidra inn i det offentliges satsning på dette området."*

Den nasjonale IKT-kompetansen er betydelig, og på flere områder er norske bedrifter ledende i verden. Det er flere grunner til dette. Norge har gjennomgående høy teknologisk kompetanse og profesjonelle brukere som vet å utnytte IKTens muligheter og som er innovative mht videre utvikling. Markedet er relativt sett lite og oversiktlig med brukere som er kjøpekraftige og investeringsvillige. Det er også en betydelig innovasjon innenfor dette feltet, der IKT-løsninger stadig tas i bruk på nye måter og områder. Norge ansees i denne sammenheng av mange som en viktig arena hvor industrien kan teste ut nye konsepter, produkter og tjenester. Det gjelder så vel innenfor sivil som militær IKT. Det er en rekke mindre bedrifter som har spesialisert seg innen nisjer, der de i stor grad nyttiggjør seg standardisert teknologi i sine applikasjoner. Med den store etterspørsel og bruk av IKT-løsninger i det sivile samfunn, er det nettopp sivil sektor som er hoveddriveren innenfor IKT-utvikling. Behovet for å utvikle proprietære IKT-systemer for Forsvaret har gradvis avtatt. Dette innebærer mange muligheter, men også nye trusler for bruk av IKT i Forsvaret. De viktigste utfordringene er først og fremst koblet til krav til sikkerhet, helhetlig arkitektur, fleksibilitet og kapasitet.

Skal Forsvaret kunne nyttiggjøre seg denne kompetansen, må en være betydelig mer åpen i sin kommunikasjon med industrien enn tilfellet har vært hittil. Vi anser det som et viktig skritt i riktig retning at FD har lagt ut det som i denne rapporten er omtalt som"Overordnet materiellplan for programområdet informasjonsinfrastruktur" (3) på sine hjemmesider. Dette gir industrien en grov innsikt i hvilke områder Forsvaret arbeider med i de kommende fire årene. Men på sikt kreves det en noe mer deskriptiv kommunikasjon og en enda mer involverende

holdning og langsiktig samarbeid til industrien for å få gevinst for alle parter. Et sentralt grunnlag for en slik tilnærming er at Forsvaret besitter tilstrekkelig kompetanse til å forstå og utnytte de muligheter som ligger i markedet, og har tilstrekkelig kompetanse til å opptre som en likeverdig partner for industrien.

7.2 Forsvarets kompetansebehov

Som beskrevet under kapittel 5, har Forsvaret mange kompetansemiljøer, og en ansvarsstruktur som ikke er lett synlig. Gjennom samtaler med representanter for flere av miljøene har nettopp dette forholdet blitt fremhevet. Kombinasjon av fragmenterte fagmiljøer og en uklar ansvars- og rollestruktur skaper lett motstridende interesser og ineffektivitet i organisasjonen.

Den høye turnover Forsvaret har på personellsiden er også en stor utfordring. Kompetansen er i liten grad institusjonalisert og forankret i den formelle organisasjonen, men knyttet til den enkelte medarbeider. Dette gjør det problematisk å bygge opp langsiktig kompetanse knyttet til et ansvarsområde. I tillegg er Forsvaret i stor grad styrt på tildelte årsverk. Gjennom den store omstillingen Forsvaret har vært gjennom de siste årene, har bemanningen blitt kraftig redusert. En slik stor og rask omstilling er neppe mulig å gjennomføre uten at det går ut over den samlede kompetanse og kapasitet.

En av forutsetningene for personellreduksjonene var at en skulle sette bort en del av den virksomheten som Forsvaret drev internt. Dette har i ikke funnet sted i tilstrekkelig grad, og gjør at den reduserte organisasjonen ikke klarer å håndtere alle oppgavene den stilles ovenfor.

Alle disse faktorene medfører at det må foretas noen grep for å sikre at Forsvaret kan fortsette moderniseringsprosessen samtidig som en utvikler den operative evne. En sentral mulighet er å etablere langsiktig strategisk samarbeid eller partnerskap med enkelte industriaktører. Dette vil kunne sikre at en har tilgang på kompetanse på kjerneområder. Vi beskriver dette nærmere under kapittel 8.

Det er viktig å erkjenne at Forsvaret trenger en profesjonell IKT organisasjon. Utfordringen blir å balansere innenfor hvilke deler av IKT området hvor Forsvaret selv skal være profesjonell (Forsvarets IKT kjernekompetanse) og hvor en skal overlate til forsvarsindustrien å være profesjonell (ekstern IKT kjernekompetanse).

Generelt kan en si at Forsvaret må ha kompetanse inne tre hovedområder:

- Sentral styring
- Fremskaffe IKT-løsniger
- Forvalte og drifte IKT-løsniger som fyller særskilte forsvarsmessige behov

7.2.1 Sentral styring

I henhold til (1) skal fokus for sentral styring rettes mot tre hovedområder:

- Helhetlig planlegging og strukturering av militær tilpasning og anvendelse av IKT i Forsvaret
- Overordnet styring og kontroll av IKT-investeringer og –drift
- Rådgivning til politisk og militær ledelse i forhold til muligheter og begrensinger hva angår militær tilpasning og anvendelse av IKT

En viktig del av den overordnede styringen vil være å utvikle en helhetlig strategi for hvordan Forsvaret skal utnytte IKT i sin virksomhet. Dette gjelder spesielt for hvordan Forsvarets IKT-systemer skal struktureres og utvikles for innfri de krav til fleksibilitet og introperabilitet som er nedfelt i policy-dokumentet.

Som supplement til referansemodellen for INI som er gjengitt i 6.1, bør det lages en arkitektur for den tekniske og applikasjonsmessige strukturen, slik at en får identifisert de viktigste egenskapene ved systemene, og informasjonsflyt og grensesnitt mellom de ulike delene. Dette er nødvendig for å sikre at kommunikasjons- og informasjonsinfrastrukturen spiller sammen gjennom den kontinuerlige oppdatering og tilpasning som finner sted.

For å kunne utøve god styring, må en også holde oversikt over utviklingen innen sensor-, beslutnings og effektorkomponentene, samt sørge for at framtidige fremskaffelser innen dette feltet er tilpasset den øvrige strukturen. Forsvaret må beherske dette feltet godt, og være så trygg på sin egen kompetanse at en også kan kommunisere åpent med fagmiljøene utenfor egne rekker samtidig som en beholder den reelle styringen og handlefriheten.

Et sentralt element i overordnet styring og kontroll av IKT-investeringer og – drift, er problemstillingen om hvordan Forsvaret skal forholde seg til det eksterne markedet de støtter seg på i sin virksomhet. En egen policy og strategi for hvordan Forsvaret skal samarbeidet med industrien bør utarbeides og være styrende for aktører på alle nivåer. Vi ser det som helt avgjørende for at Forsvaret skal lykkes med å realisere NbF, at det utvikles en strategi for hvordan man anvender sine nøkkelleverandører over tid, spesielt innenfor forsvarsviktige systemer.

7.2.2 Fremskaffe IKT-løsninger

Forsvaret har til enhver tid en aktivitet knyttet til fremskaffelser av nye løsninger, enten det dreier seg om nye systemer eller modifiseringer og oppgraderinger av eksisterende løsninger. Pr i dag anslås det at det er ca 60 prosjekter knyttet til IKT-området alene.

Prosessene skal følge ”Konsept for fremskaffelse av materielle kapasiteter i forsvarssektoren”, som omfatter hele verdikjeden, fra planlegging, gjennom anskaffelse og drift, til avhending. Et hovedpoeng i konseptet er vektleggingen av de tidlige fasene, med økt ressursbruk tidlig. Erfaringsmessig vil suksessen til de enkelte prosjektene avhenge i stor grad av den faglige kompetansen til personellet som leder og deltar, herunder detaljert kunnskap om de systemene som fremskaffes.

Fra Forsvarets side vil fremskaffelsesprosessen krever kompetanse til, helhetlig planlegging,

konkretisering av løsninger, evaluering av alternativer, forvaltning av leverandørforhold og oppfølging/ledelse av fremskaffelsesprosessen. De enkelte prosjektene må planlegges med utgangspunkt i den overordnede styrkestrukturen, og reflektere de operative behov som skal dekkes. I denne delen av prosessen må en ta fram gode overslag på levetidskostnader, og vurdere om en har midler til å gjennomføre ikke bare fremskaffelsen, men også driftingen av fremskaffelsen. Det må også vurderes hvorvidt fremskaffelsen får innvirkning på andre deler av strukturen, og konsekvensene av dette.

For å løse disse behov, er arbeidet i konsept- og definisjonsfasen er særdeles viktig. Gjennom de valg en gjør her, fastlegges levetidskostnadene i stor grad for systemene. Dette understrekes nettopp behovet av å bruke større ressurser i tidligfase. I en del land har en hatt god erfaring med å samarbeide tett med industrien i disse fasene, selv om en nødvendigvis må ha kompetanse og know how til å beholde styringen. Ikke bare kan en få tilgang til alternative løsninger, men en kan også få betydelige bedre kostnadsoverslag gjennom å samarbeide med leverandørene. Men dette krever solid merkantil kompetanse og ryddighet i prosessene slik at en står på trygg grunn i forhold til eksterne leverandører.

7.2.3 Forvalte og drifte IKT-løsninger

Som nevnt tidligere har FK KKIS det overordnede funksjonelle ansvar for tjenestestrukturen, mens FLO/IKT har tilsvarende ansvar for den teknisk og applikasjonsmessige infrastrukturen. Dette ansvaret kan ikke settes bort. Disse to enhetene blir derfor svært sentrale og viktige aktører i enhver prosess som har med forvaltningen å gjøre, inklusive fremskaffelse.

Som fagmyndighet skal en utgi bestemmelser og retningslinjer knyttet til bruk, vedlikehold og drift av materiellet. For å kunne gjøre dette på en tilfredsstillende måte, må fagmyndigheten ha en solid kompetanse knyttet til de enkelte systemene. Dette innebærer ikke et krav om egen spisskompetanse så lenge en har tilstrekkelig egen kompetanse og innsikt til å kommunisere med andre (eksterne) fagmiljøer og vurdere de råd man får.

7.3 Kompetanse som kan forvaltes av industrien

Ved anskaffelser av større plattformer, eksempelvis fly, vil leverandøren bli en strategisk partner for Forsvaret i flyets levetid. Ved alle større modifikasjoner og endringer av systemet, vil det være behov for å konsultere leverandøren, selv om Forsvaret selv er fagmyndighet, og formelt er den som beslutter hva som skal gjøres og hvordan.

I tråd ovennevnte, vil det også innenfor IKT være en rekke områder industrien kan supplere Forsvaret kompetansemessig, uten at Forsvaret på noen måte gir fra seg kontrollen. Stort sett all hardware og alle applikasjoner Forsvaret nyttiggjør seg, har sitt utspring i industrien. Gjenbruk av kompetansen til leverandørindustrien, vil i de fleste tilfeller være regningssvarende. Forholdet blir imidlertid betydelig enklere å administrere dersom en kan knytte langsiktige avtaler med de mest sentrale leverandørene. Eksempler på områder der industrien kan bidra er

- Systemutvikling - og design

- Systemintegrasjon
- Drift og vedlikehold

7.3.1.1 Systemutvikling og design

Grunnlaget for nettverkstenkningen ligger i de muligheter som informasjonsteknologien åpner for. Sammenhengen og strukturen i teknologianvendelsen blir viktig for å kunne holde informasjonsinfrastrukturen sammen, samt å videreutvikle interoperabilitet nasjonalt og internasjonalt. Løsninger som tas fram må kunne spille sammen med den eksisterende strukturen, og være fleksible med hensyn til videre utvikling og tilpasning. For å få til dette, må enten Forsvaret selv utføre systemutvikling, skaffe seg partnere som har innsikt i helheten eller en kombinasjon.

Som påpekt under avsnitt 7.2 var en av forutsetningene for omstillingsprosessen til Forsvaret at en skulle fokusere på den operative delen, og redusere på støtte. Systemutvikling og –design er ikke å betrakte som en militær oppgave, men derimot noe som forbindes med avansert industri.

Det faktum at arven inngår som en dimensjonerende faktor i alt utviklingsarbeid, tilsier at Forsvaret og IKT-industrien burde innlede et tett samarbeid av langsiktig karakter. Forutsetningen for at industrien skal kunne levere optimale løsninger til Forsvaret, er at de har en god kunnskap om arven og de fremtidige operative behov Forsvaret mener å ha. Dette forsterkes ytterligere av at en ønsker et sammenhengende og sikkert informasjonsnettverk som kan anvendes over hele spektret, både nasjonalt og internasjonalt. Et tettere og fortrolig samarbeid vil kunne skape synergi og bygge kompetanse som i dag ikke finnes i tilstrekkelig mengde og kvalitet i noen av leirene.

7.3.1.2 Systemintegrasjon

Systemintegrasjon ble av FD etablert som et nasjonalt kompetanseområde for Forsvaret og norsk forsvarsindustri høsten 2005, se avsnitt 7.4.2. Området har stor betydning for arbeidet med å etablere et nettverksbasert forsvar gjennom INI. Ikke bare for å knytte sammen de ulike tjenesteområdene, men også for å knytte INI opp mot sensor- og effektorstrukturen. En systematisk kompetanseoppbygging innen dette feltet vil gi Forsvaret mulighet til å velge mer fritt med hensyn til den vider utviklingen av strukturen. Det er imidlertid ikke mulig for Forsvaret å selv etablere denne type kompetanse innenfor de rammevilkår en arbeider under, men et langsiktig samarbeid med nasjonal industri vil kunne ivareta Forsvarets behov.

7.3.1.3 Drift- og vedlikehold

Dette området har tradisjonelt vært ivaretatt av Forsvarets egen organisasjon. I forbindelse med omstillingen av Forsvaret, har drift og vedlikehold blitt vurdert som et av de feltene der industrien kunne ta et større ansvar, for på den måten frigjøre ressurser til Forsvarets operative virksomhet. Sett i levetidsperspektivet, er drift og vedlikehold verdifull kompetanse som kan bidra til å videreutvikle og forbedre systemene. Samtidig vil kompetanse knyttet til design og utvikling av systemene kunne gjenbrukes i driftsfasen. Jo mer komplett verdikjede industrien

besitter, jo bedre kan de utvikle og utnytte sin kompetanse.

7.4 Nasjonale kompetanseområder

Høsten 2005 fremmet FD til Stortinget en liste over nasjonale kompetanseområder for Forsvaret og norsk forsvarsindustri som de anser er viktig for den videre utvikling av Forsvaret:

- Informasjons- og kommunikasjonsteknologi
- Systemintegrasjon og arkitektur
- Missilteknologi og autonome våpen- og sensorsystemer
- Undervannsteknologi og – sensorer
- Simuleringsteknologi
- Våpen og rakettmotorteknologi, ammunisjon og militære sprengstoff
- Materialteknologi
- Maritim teknologi

Informasjonsteknologi inngår i de aller fleste våpensystemer på en eller annen måte, og som sådan kunne en kanskje si at alle områdene berøres av dette feltet, men det er tre områder som spesielt peker seg ut med hensyn til IKT: Informasjons- og kommunikasjonsteknologi, Systemintegrasjon og arkitektur og Simuleringsteknologi

7.4.1 Informasjons og kommunikasjonsteknologi

Dette er et stort og viktig område for Forsvaret, og som på mange måter vil være styrende for utviklingen mot et effektivt og tilpassningsdyktig forsvar basert på moderne teknologi. Sterkt forenklet kan basisteknologien som vil realisere fremtidens IKT-produkter og IKT-anvendelser kunne inndeles i tre hovedområder:

- Mikroteknologi
- Kommunikasjonsteknologi, kommunikasjons- og informasjonsinfrastruktur
- Programvareteknologi og informasjonssystemer
- Informasjonssikkerhet

Området anses å være fullt dekkende for de to tidligere satsningsområdene ”Maskin- og programvare for sambands- og kommando-, kontroll- og informasjonssystemer” og ”Radio, satellitt og linjekommunikasjon”, og sammenfallende med produktområdet referert i St prp 59 (1997-98) som ”Kommunikasjons-, kontroll og informasjonssystemer”. Den kompetansen som er bygget opp under tidligere forskning, utvikling og produksjon innen disse områdene må videreutvikles i tråd med fremtidige behov.

I tillegg til å være det mest sentrale område for utviklingen av Forsvaret, regnes IKT globalt som det mest kritiske teknologiområdet for fremtidig næringsutvikling, og det er en formidabel FoU-satsning innenfor alle sentrale teknologiområder. Nettopp av den grunn er det nødvendig å ha en IKT breddekompetanse av høy nok kvalitet til å kunne forstå og dra nytte av de mange teknologiske innovasjoner som gjøres internasjonalt.

Det bør derfor tilstrebes et nasjonalt FoU- og industrimiljø med omfattende og gode internasjonale kontakter. Her bør man i tillegg søke å etablere en tettere kontakt mellom de militære og sivile miljøene.

7.4.2 Systemintegrasjon og arkitektur

Forsvarets materiellstruktur preges i dag av en rekke plattformer i form av ulike fartøyer, kjøretøyer, fly og stasjonære installasjoner som igjen har delsystemer og komponenter fra forskjellige leverandører. Det er ofte behov for å modernisere deler av de installerte systemene med bruk av andre typer teknologier eller sørge for sømløs informasjonsflyt til/fra et nettverk. Dette må kunne gjøres på en slik måte at dataflyten vis a vis øvrige systemer og delsystemer ikke forstyrres eller at det oppstår interferens, og at det kan verifiseres at den ønskede effekt oppnås.

Området krever inngående plattform- og systemkunnskap, og spesiell innsikt hvordan man håndtere og verifisere prosessene. Det vil være naturlig å henføre begrepet systemarkitektur til dette teknologiområdet. Dette kompetanseområdet er etterlyst fra Forsvaret, som ønsker å kunne velge friere mellom leverandører av delsystemer og komponenter for modernisering av Forsvarets materiellstruktur. Dette betinger også at en søker å unngå proprietære løsninger ved anskaffelser av nytt materiell, men klarer å etablere en åpen systemarkitektur med muligheter for ”Plug and Fight”.

7.4.3 Simuleringsteknologi

Militær simuleringsteknologi er i rivende utvikling, og blir anvendt innenfor stadig nye områder av militær virksomhet. Eksempler er eksperimentering, forskning, prosjektering og anskaffelse, utdanning og øving, planlegging og øving i forkanta av operasjoner, beslutningsstøtte i operative systemer og for etteranalyse av operasjoner.

Syntetiske miljø er datamaskinsimuleringer, bemannede simulatorer og/eller instrumenterte militære styrker og kommandosystemer, som opererer i en felles databasert representasjon av et stridsfelt. Et slikt blandet miljø har flere fordeler. Teknologien drar nytte av den raske utviklingen innen innformasjons- og kommunikasjonsteknologi som enten kan utnyttes i økt realisme eller reduserte kostnader. Nettverksteknologi har også resultert i nye muligheter ved å knytte geografisk spredte simuleringer sammen. Dette forventes å få økt betydning når neste generasjons Internett-teknologi tas i bruk for militær simulering.

Flere land og NATO har, eller er i ferd med å etablere syntetiske eksperimenteringsmiljøer. NATO deltar allerede i multinasjonale eksperimenter gjennomført i syntetiske miljøer. NATOs

Joint Warfare Centre i Stavanger vil antagelig få en sentral rolle for NATOs eksperimenteringsmiljø.

Det finnes små og spredte, men kompetente miljøer både i Forsvaret og i industrien som utgjør et solid grunnlag for å utvikle dette området til et nyttig verktøy for Forsvaret. For Forsvaret anses dette området som viktig for å kunne effektivisere tjenesten i nær sagt alle ledd. Samtidig er det av sentral betydning at man er i stand til å henge med i en internasjonal rivende utvikling på feltet.

7.5 Informasjonsdeling

I *Policy for militær tilpasning og anvendelse av informasjons- og kommunikasjonsteknologi i Forsvaret* (2) som har til hensikt å skape grunnlag for en felles virksomhetskultur i Forsvaret for militær tilpasning og anvendelse av informasjons- og kommunikasjonsteknologi sies det under beskrivelse av målbildet:

Nye løsninger innenfor IKT skaper vesentlig potensial for ytterligere effektivisering. Dette gjelder både innenfor operativ virksomhet, og i særlig grad innenfor operativ støttevirksomhet og forvaltning. Økt bruk av standardiserte løsninger, kombinert med begrensinger i typen og antall av eksisterende løsninger og en bedre samordning av disse, vil gi store gevinster.

Videre i *Konsept for styring av elektronisk informasjon i Forsvaret* hevdes det i innledningen følgende:

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

- *Økt deling av informasjon og kunnskap*

Bedre samarbeid

- *Bedre og enklere koordinering og synkronisering*
- *Distribuert og virtuell organisering*

Dersom Forsvaret skal dra full nytte av samarbeidet med industrien innen dette feltet, bør Forsvarets egen policy innenfor utvikling av IKT og den prinsipielle tenkningen omkring NbF også omfatte og legges til grunn for samarbeidet mellom Forsvaret og industrien. Dette er et konsept som en har tatt i bruk med stort hell bl a i Storbritannia.

8 BRUK AV INDUSTRI

INI som et omfattende system, vil hele tiden være gjenstand for oppdateringer slik vi har beskrevet ovenfor. Dette krever nøye konfigurasjonsstyring for at totalsystemet skal kunne fungere etter sin hensikt. Selv om tjenestene som anskaffes er basert på åpne standarder, vil det i et slikt stort system være behov for nøye overvåkning og testing for å verifisere at helheten bibeholdes. Det er samtidig få områder med så stor og rask utvikling som IKT. Det sivile IKT

markedet er stort, og mye av teknologien som Forsvaret utnytter i sine systemer kommer herfra.

Selv om Forsvaret har god kompetanse innenfor IKT-området, kan man redusere risikoen ved anskaffelser betydelig ved å involvere kompetent industri i konseptarbeidet og kravformulering før myndighetene godkjenner prosjektene for gjennomføring. Likevel er dagens anskaffelsesstruktur ikke tilrettelagt for å aktivt involvere industri tidlig. Til tross for mange klart uttalte målsettinger om å satse på tidlige faser i prosjektene, blir ikke industrien invitert til deltagelse før kravspesifikasjonen er skrevet.

Det bør derfor ses på i hvilken utstrekning en kan etablere en struktur for på en bedre måte å ta vare på teknologiutvikling knyttet til Forsvarets egne systemer. Målet må være å sikre at forskning og utvikling innenfor så vel Forsvarets egne organer, som i industrien er målrettet mot planlegging av kapabiliteter, og at den innovasjon som skjer innen det sivile markedet blir utnyttet optimalt til Forsvarets beste. Vi vil nedenfor beskrive noen relevante forhold for å bedre kunne utnytte den industrikompetanse som er nødvendig for Forsvaret på dette området.

8.1 Behovet for tilgang til kompetanse

Kompetansebehovet vil ha mange fasetter, hvor alt fra teknisk, bruker, vedlikeholder, design og annet representerer elementer av kompetansefasetten. Vi anser det som virksomhetskritisk for Forsvaret å ha god tilgang til teknisk- og systemkompetanse for alle faser i levetiden. Selv om reduksjon av kompetansekapasiteten i Forsvaret, og FLO spesielt, fremtvinger nye måter å håndtere og utvikle eksisterende og fremtidige materiellsystemer, har det alltid vært behov for å henvende seg til eksterne leverandører. Leverandører sitter på annen type informasjon og er drevet av andre behov, enn hva myndighetene og dets representanter er.

Nøkkelen til å løse Forsvarets fremtidige kompetansebehov vil antakelig være å samle forskjellig kompetansemiljøer for raskere kunne få frem bedre resultater. Det som, etter vårt skjønn, vil være utfordringen, er tilpasningen på den ene side gode prosjekt og levetidsmodeller med tilhørende konkurransemodeller, og på den annen side offentlige anskaffelsesregler laget for et annerledes marked og kompleksitet.

8.1.1 Organisatoriske forhold i Forsvaret

Forsvaret er en mangefasettet organisasjon. I vår gjennomgang av de organisatoriske forhold, se pkt 4.1.1, er det svært mange aktører internt i Forsvaret relatert til IKT området. Det er viktig i forhold til å gjennomføre gode prosjekter at man har en effektiv organisering, ikke bare mellom kunde og leverandør, men også internt. Vi har laget et bilde, se fig 7.1. som viser et overordnet grensesnitt mot industri.

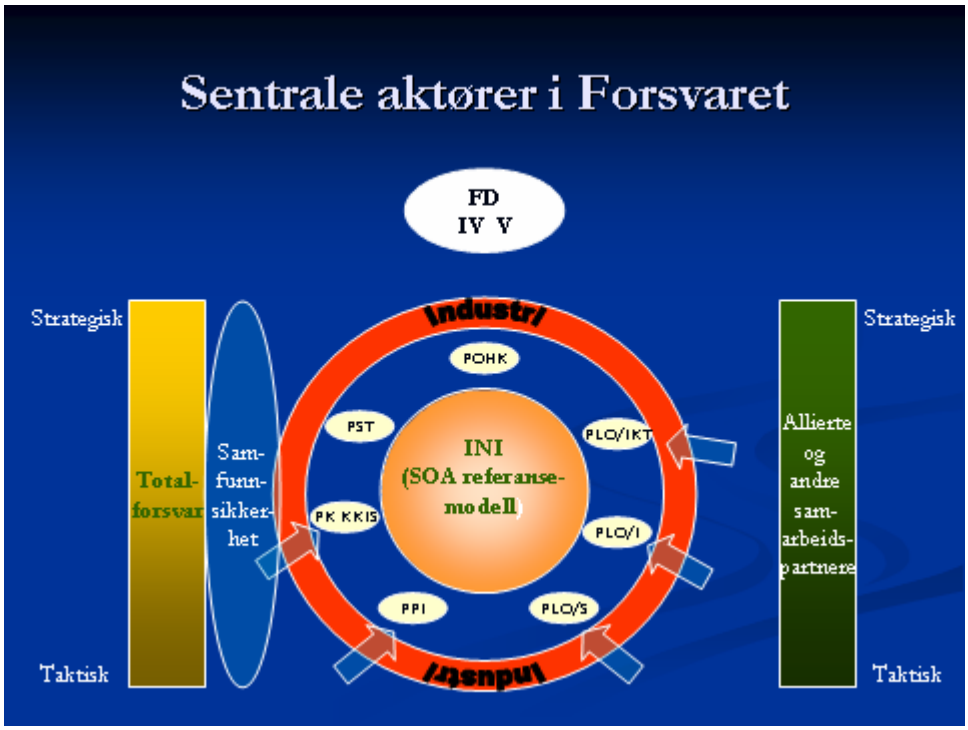


Fig 7.1 Grensesnittbilde mellom Forsvaret og industri for Programområde INI

For å kunne opptre enhetlig og etterrettelig overfor industrien, er det av avgjørende betydning at man har en effektiv intern organisering med klare roller og ansvarsfordelinger. Grensesnittbildet tydeliggjør at samme industribedrift har et spillerom overfor Forsvaret som kan synes stort, og hvor Forsvaret har en utfordring i å koordinere seg internt.

I forbindelse med det nye Investeringskonseptet, anføreres det i høringsrapporten (s.34) at:

"Til grunn for konseptet ligger en forutsetning om tydelige ansvars- og myndighetsforhold. På dette grunnlag vektlegges integrerte arbeidsprosesser i videst mulig forstand innenfor investeringsvirksomheten. Dette innebærer at alt ansvar forutsettes utøves i tett samspill mellom strategisk nivå og etatene både ift. planlegging og gjennomføring."

For at Forsvaret skal lykkes, må dette følges opp nøye. Erfaringer gjennom vårt arbeid, viser at organiseringen og nødvendig rolle- og ansvarsdeling har forbedringspotensiale. Det mest kritiske er en effektiv intern kommunikasjon koblet opp til en kommunisert klar strategi for håndtering av Forsvarets leverandørbase, slik at samspillet blir kosteffektivt for alle aktører. I den sammenheng kan ikke Programstyrenes rolle for de forskjellige programområder, undervurderes.

8.1.2 Beste praksis

Kompleksitet kombinert med lang levetid og krav til høy kompetanse, skaper et stort behov for korrekt informasjon til rett tid, - alltid. Nettopp dette kravet er kanskje det vanskeligste å ta tak i. Kompleksitet gir partene god mulighet for å skjule informasjon. Spørsmålet er hvordan man organiserer seg for å oppveie denne informasjonskompleksiteten.

Vårt utgangspunkt er et imperfekt marked hvor det finnes mye asymmetrisk/skjult informasjon, klassisk for forsvarsmarkedet. Typisk at en leverandør har større kunnskap om arbeidsomfang ved egen utførelse enn kjøper har[5]. Samtidig vil aktørene ikke ha full oversikt over hendelser i fremtiden som kan påvirke anskaffelsesprosjektet, eksempelvis kundens egne langtidsplaner. Utfordringen er i en tidlig fase i prosjekter å få tak i informasjon som også er korrekt. Denne utfordringen vil ikke en kunde klare alene, han må ut på markedet. Undersøkelser viser også at man svært tidlig i prosjekter båndlegger store midler, selv om man formelt ikke har inngått kontrakter (evt kun for små summer). Figur 7.2 illustrerer dette;

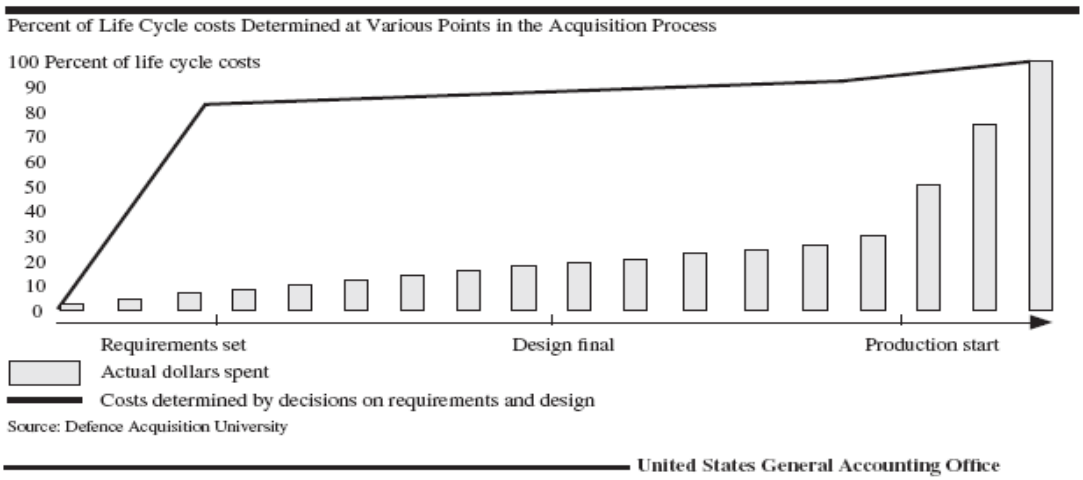


Figure 17: Life cycle costs in the acquisition process.[52]

Figur 7.2: Graf fra rapporten "The Electronic Systems Sector Strategic Plan" fra Defence Materiel Organisation i Australia

Dette setter krav til informasjonstilgangen i tidlig fase av prosjekter, ikke bare i forhold til selve prosjektet, men også tilhørende systemer som det nye systemet skal integreres mot, noe som er relevant innenfor IKT området. For å håndtere behovet om informasjons- og kunnskapsdeling i tidligfase, har man på både privat og offentlig side gjennom de siste 10-15 år hatt et særlig fokus på organiseringer som krever en eller annen form for tett samarbeid, enten det er kalt partnerskap, allianse, governance contracting eller partnering[6]. Behovet for slike konstellasjoner, skyldes mange forhold, men nært samarbeid mellom kunde og leverandør *hvor man deler informasjon* er ansett som et nøkkelkriterium for suksess og for å holde kostnader nede.

Konseptuelt følges dette opp i FD sitt konsept for Offentlig Privat Partnerskap (OPP), hvor man for Partnering begrepet anfører at begrepet betegner ulike typer gjensidig forpliktende,

---

[5] Som eksempel vises det til Lewis (1995) s.1; *"Our first reaction was to get angry and say, "Why didn't you do this before?" They said, "Because you didn't ask." (Roland Anderson, global purchasing head of Asea Brown Boveri, after a supplier made a part at 30 % lower cost when ABB gave it design responsibility.")*

[6] I den sammenheng viser vi til UK MOD sitt White Paper som klart poengterer viktigheten og den suksess de hittil har hatt med å implementere Partnering for de rette prosjekter, se spesielt s.31 og 134

langsiktige avtaler mellom to eller flere parter hvor integrerte samarbeidsformer ofte anvendes. Det pekes videre på at et samlet leveranseansvar i hele livssyklusen gir leverandøren mulighet til å planlegge langsiktig og komme med innovative løsninger til beste for begge parter. Målet er en best mulig ressursutnyttelse – ved at Forsvaret og den private part utnytter hverandres kjerneressurser til felles beste.

Et godt eksempel på dette er FISBasis prosjektet som ble vedtatt ved Stortingets behandling av *Budsjett-inst. S. Nr. 7 (2000-2001)*. Prosjektets målsettinger er nådd, gjennomført nesten 2 år raskere enn opprinnelig planlagt og med avtalt kvalitet. Brukernes erfaring er gode, dette er dokumentert gjennom undersøkelser av nøytral tredjepart. Prosjektet er overført til drift i Forsvarets logistikkorganisasjon (FLO/IKT). Prosjektet ble gjennomført over 200 MNOK billigere enn planlagt (total kostnad av 1519 MNOK).

8.2 Merkantile forhold knyttet til rådgivning

8.2.1 Mulighetene innenfor Lov om offentlige anskaffelser

FOA[7] § 3-6 åpner for muligheter til å ta i bruk en eller flere leverandørers kunnskap forut for en konkurranse.

Samtidig, hvis en rådgiver vinner kontrakten, kan det være enkelt for de tapende leverandører å hevde at ikke all informasjon er blitt fremlagt, - at den kunnskap som rådgiver har tilegnet om kunden utgjør en fordel som ikke kan erstattes gjennom skriftlig dokumentasjon og det kan finnes etiske betenkeligheter og muligheten for dobbelt roller. En annen fare er også at rådgivningen medfører at andre vil anse det kommersielt uinteressant å delta i en konkurranse hvor vinnermuligheten er liten som følge av slik deltakelse.

Disse forhold kan avhjelpes dersom visse forutsetninger oppfylles:

- *All vesentlig informasjon* av betydning for deltakelse i konkurransen og utforming av tilbud må gjenspeiles i grunnlagsdokumentasjonen og *tilflyte samtlige tilbydere*.
- At leverandørens deltakelse som rådgiver ikke tillegges betydning ved evalueringen av konkurransen, eksempelvis gjennom oppsettet av tildelingskriterier.
- Dersom all vesentlig informasjon videreformidles til interesserte tilbydere gjennom konkurransegrunnlaget, vil fortrinnet i det vesentlige være redusert til *tid*; betydningen av tid som fortrinn reduseres i den grad tilbyderne har *tilstrekkelig* tid. Således må fristene må settes så romslig at deltakelse gir en reell konkurranse. Dette vil gi de andre konkurrenter tilstrekkelig tid til å sette seg inn i forespørselen, selv om de aldri vil kunne innhente rådgiveren.

[7] Forskrift om Offentlige Anskaffelser

- Respektere forskriftens krav vedrørende om fokus på bruk av funksjonelle spesifikasjoner og standarder, og bestemmelsene om kvalifikasjonskrav, samt kravene vedrørende tildelingskriterier.
- Et eventuelt fortrinn kan i tillegg ved forhandlet prosedyre, kunne bli kompensert for gjennom forhandlingene.
- Eventuelle fortrinn, og eventuelle betenkeligheter hos øvrige interesserte tilbydere, og ikke minst risikoen for klage, vil kunne reduseres gjennom befaring/konferanse samtidig med alle.
- For å holde konkurransen oppe, vil det være svært viktig å være åpen om situasjonen og informere om den strategi man har, og ikke minst, følge strategien.

Gitt at dette følges tilpasset den enkelte anskaffelse, skal ikke en rådgivning kunne utelukke konkurransen. Praksis synes å gå langt i å tillate forutgående rådgivning basert på disse hensyn. Anskaffelsens art og markedets oppfatning av slik deltakelses reelle innvirkning på konkurransesituasjonen, er selvsagt også faktorer som bør hensyntas ved avgjørelsen av hvor restriktiv man skal være. Her er det for så vidt et viktig skille mellom forsvarsmarkedet og øvrig sivilt marked.

8.2.2 Mulighetene innenfor Anskaffelsesregelverket til Forsvaret

Forsvarsministeren har det konstitusjonelle ansvar og myndighet for forvaltningen i Forsvaret og kan gripe inn i saksbehandling på ethvert trinn. Gjennom ARF[8] har FD gitt de overordnede rammebetingelser for gjennomføring av fremskaffelser. FD har vide fullmakter og rammer for gjennomføring av anskaffelser utenfor EØS området. Dette underbygges ved at ARF er et internt regelverk.

Et gjennomgående trekk ved ARF er at FD har klare muligheter til å fravike regelverket så lenge man er utenfor EØS området. Unntaksmuligheter i ARF har ofte bakgrunn i næringspolitiske forhold. Det vises til ARF pkt 1.3.1 hvor FD har utarbeidet næringspolitiske retningslinjer for anskaffelser til Forsvaret som fremgår av St. prp. nr. 42 (2003-2004). Det er FD som har ansvaret for at næringspolitiske aspekter blir vurdert ifm fremskaffelser av prioritert materiell

Hovedregelen for bruk av eksterne rådgivere som deltar i kravspesifikasjonsarbeid, er at disse skal være leverandøruavhengige samt ikke ha økonomiske interesser i den påfølgende anskaffelsen. I erkjennelse av at dette kan være vanskelig å oppnå på enkelte teknologiområder, tas det høyde for å kunne bruke rådgivere med leverandørtilknytning, herunder leverandører. For å kunne gjøre dette, er det et krav om at slike rådgivere benyttes på en måte som ikke påvirker konkurranseforholdet mellom framtidige tilbydere. Videre skal kravspesifikasjonen utarbeidet med assistanse fra slike rådgivere, bli gjort tilgjengelig for et utvalg leverandører for kommentering før den endelige forespørselen/anbud sendes ut.

[8] Anskaffelsesregelverk for Forsvaret

Denne muligheten er tatt inn i ARF for i større grad kunne utnytte leverandørenes kunnskap for å utarbeide kosteffektive krav uten å ødelegge konkurransemomentet. Det presiseres at FD kan foreta ytterligere hensiktsmessige og saklige avvik fra dette ut fra næringspolitiske hensyn.

I relasjon til anskaffelsesstrategier som skal utarbeides, gir ARF http://www.odin.dep.no/filarkiv/224849/k296.html - b297anvisning på at næringspolitiske føringer og mål og eventuelt andre politiske føringer skal tas høyde for ved utarbeidelse av en anskaffelsesstrategi. FD kan eksempelvis gi føringer på:

- Hvilke tilbydere som skal få forespørsel,
- Om, og hvilke leverandører som skal delta med forstudier eller delta i tidlig integrerte prosjektorganisasjoner
- Krav til industrisamarbeid/gjenkjøp
- Oppdeling/inndeling av et prosjekt i delprosjekter osv.

Gjennomføringsoppdraget fra FD skal angi de overordnede retningslinjer for en anskaffelse. bl.a. med syn på:

- Alternative anskaffelsesprosedyrer
- Offentlig privat partnerskap
- Oppdeling av anskaffelsen i faser eller sammenslåing av faser (for eksempel utvikling og produksjon)
- Spesifikasjonsmetoder - (funksjon/ytelse/detalj, bruk av standarder osv.)
- Kontraktstyper (kompensasjonsformater)
- Kontraktsvilkår (garantiklausuler, innsyn, insitamenter, opsjoner, osv.)
- Samarbeidsformer med leverandører (f. eks. tidlig integrert samarbeid)

Ovennevnte gir Forsvaret (FD inkludert) brede muligheter i å tilnærme seg IKT industrien med innovative forslag.

8.3 Bruk av industri i internasjonale operasjoner

I forbindelse med utarbeidelse av denne rapporten, har det vært et ønske å få belyst hvorledes industriens rolle kan tas med inn i det operative logistikk begrepet, dvs understøttelse ved internasjonale operasjoner, spesielt innenfor rammen av en væpnet konflikt.

Problemstillingen gjelder hovedsakelig for de logistikkområder som i dag er betjent med militært personell, men også andre virksomhetsområder hvor sivilt personell ansatt i Forsvaret tradisjonelt har reist ut for å betjene operative avdelinger i inn og utland.

Ved å anvende sivile firmaer til slike oppdrag, enten det skjer på enkelte reparasjonsoppdrag, eller ved tilsvarende utestasjonering sammen med den enkelte avdeling, er det et spørsmål om man i fremtiden kan løse de militære behov med bistand fra en leverandør.

Selv om folkeretten til en viss grad tillater bruk av sivilt personell til understøttelse av det militære logistikkapparat, er det visse aspekter som tilsier at man bør bruke en slik mulighet med varsomhet.

En ikke-kombattant vil ikke være autorisert til å anvende makt utover selvforsvarsretten. Kun i den grad det er et ulovlig (rettsstridig) militært angrep, vil den sivilt ansatte kunne nytte selvforsvarsretten. Sivile stilt opp i skarpe situasjoner vil i noen tilfeller ikke ha mulighet for å se noen klar grense mellom lovlige og ulovlige angrep, og når de eventuelt er autorisert til å bruke selvforsvarsretten. En feilbedømmelse fra sivile personer i bruken av selvforsvar kan da medføre straffeforfølgelse for vedkommende. Måten dette vanligvis løses på, er at de væpnede styrker avgir personell til å beskytte de sivile leverandører, noe som vil kunne binde opp viktige ressurser.

For det andre vil man ikke ha noen disiplinær- eller kommandomessige virkemidler overfor leverandører. Dette kan være et problem i urolige områder i forhold til ønsket om å opprettholde stabil logistikk. I motsetning til militære styrker, har man overfor leverandører kun en kontrakt, og det vil være i strid med norsk avtalelov[9] å bl.a. kreve at noen skal utsette seg for krigsfare. De kan reise hjem på kort varsel, uten at Forsvaret kan hindre dette.

Dette bringer oss over på det tredje vurderingstema, *krigsfare*. Som det fremgår, så blir det en viss moralsk vurdering av hvor langt man ønsker å utsette sivile for krigsfare. Det ligger implisitt i folkeretten at man bør skåne ikke-kombattant personell så langt det lar seg gjøre. Samtidig vil Forsvaret være avhengig av en viss støtte fra leverandører. Det er ikke noe fasitsvar, men man bør som utgangspunkt unngå å legge opp til en bruk av leverandører med sivilt personell hvor krigsfare er stor og/eller reell.

Ovennevnte indikerer klart at man bør være varsom med å anvende sivile der det er en reell fare for stridshandlinger. Spørsmålet er om det finnes løsninger som muliggjør en beredskap fra leverandører hvor krigsfare truer. En mulig løsning kan være å både uniformere og bevæpne sivilt personell. De vil da få status som kombattante. Det vil da selvsagt være nødvendig å gi personellet en tilstrekkelig våpenopplæring etc. På den annen side må de for å få status som lovlig stridende, kunne innpasses i det ordinære kommandoapparat og underlegges disiplinærmyndighet. For å kunne få til en løsning, trenger man et fungerende trekantforhold mellom leverandør, Forsvaret og den ansatte.

8.4 Avtalestruktur – behovet for et radikalt skifte

Under det gamle BAF regime, var det stor fokus på kontroll av anskaffelser. Det var lite eller intet som oppmuntret Forsvaret i å tenke innovativt og kosteffektivt ved gjennomføring av

[9] Avtalelovens §§33 og 36 samt Legalitetsprinsippet

anskaffelser enten det skjedde på investerings- eller driftsbudsjettet. Dette har endret seg noe i den nye ARF, se ovenfor under pkt 7.2.2. Spørsmålet er om disse mulighetene faktisk blir brukt av Forsvaret.

Også gjennom det nye investeringskonseptet, fremheves kravet til dynamikk og innovativitet. Et hovedpoeng i konseptet er at det må legges betydelig økt vekt på de tidlige faser av aktivitetene gjennom øke bruk av ressurser i disse faser. Investeringskonseptet sier bl.a. (pkt 2.4):

"For å imøtekomme krav til rask tilgjengelighet, deling av ansvar og utnyttelse av kompetanse og samarbeid, må det legges økt vekt på andre fremskaffelsesstrategier enn tradisjonelt kjøp og utvikling, bl.a. løsninger innenfor rammen av offentlig privat partnerskap (OPP, dvs. bortsetting, partnering og offentlig privat samarbeid) og bruktkjøp."

Dette er etter vårt skjønn en klar oppfordring til å anvende vår verktøykasse i Forsvaret. Forsvaret må tenke helhetlig og kosteffektivt. I denne sammenheng er det avgjørende at man tar inn over seg konsekvenser for hele levetiden. Investeringskonseptet sier i pkt 2.5 at:

"Det skal være mulig å ta eksplisitte beslutninger innenfor investeringsvirksomheten som i et kostnad-nytte-perspektiv totalt sett er mest lønnsomme for Forsvaret og ikke kun potensielt optimalt for investeringskapittelet. Derved legges det til rette for at Forsvaret eventuelt kan bruke relativt mer midler i investeringsfasen, hvis dette medfører at totalkostnadene reduseres."

Et sentralt element, er opprettelsen av programområder. Dette skal sikre en mer helhetlig tilnærming til Forsvarets portefølje av materiell og systemer og gi Forsvaret og FD bedre oversikt og styring.

Spørsmålet vårt er om man har klart å overføre denne helhetlige tilnærming til en faktisk effektuering overfor industrien.

8.4.1 Behovet for en systemintegrator/rådgiver

Som vi har beskrevet tidligere i rapporten, har våre systemer både en lang levetid samtidig som behovet for (løpende) oppdateringer skjer gjennom hele levetiden. Slike oppdateringer er viktige både med hensyn til at norske styrker skal være relevante i internasjonale operasjoner, men også for å skape grunnlag for bedre overlevelse. Hittil synes man å ha hatt en altfor ad-hoc messig og kortsiktig tilnærming til porteføljen av forsvarsrelevante IKT systemer.

Siden Forsvaret i tillegg har mistet mye kompetanse, er det et klart behov for å skape en arena hvor Forsvarets gjenværende ekspertise innenfor både operativ, forskning og teknisk område kommer sammen med relevant industri. Nødvendigheten skyldes det enkle faktum at vi hver for oss ikke besitter nødvendig oversikt og kunnskap om IKT områdets kompleksitet i Forsvaret og med våre øvrige allierte. Skal vi evne å ta i bruk de muligheter som ligger innenfor NbF, trenger vi å stimulere til hurtige og effektive prosesser som bringer nødvendig slagkraft til de operative styrker.

I denne sfære er det en nødvendighet i å etablere et langvarig forhold til en systemintegrator som både kan opptre som rådgiver og som leverandør avhengig av omstendighetene. En nødvendig

støtte for Forsvaret på et overordnet nivå når sammenhenger mellom de forskjellige systemer og plattformer skal vurderes.

Det er klart det vil være en stor utfordring å få eksterne opp på det nivået som skal til for å se på tvers av alle de IKT-systemer Forsvaret har allerede (arven) og hvordan nye systemer passer inn i denne helheten. Erfaringsmessig sitter denne kompetansen i Forsvaret. Faren er selvfølgelig at industrien som har vært inne for å se på totaliteten har typisk kunnet de systemer den bedriften har levert, men ikke sett andre leverandørers produkter inn i helheten. Nettopp derfor er det så viktig at man vurderer en åpen systemintegratorløsning som inkluderer flere bedrifter i en eller annen konfigurasjon, samtidig som Forsvaret også bidrar.

Kravene til en systemintegrator er flere, og vi har følgende forslag til noen krav som bør settes. En systemintegrator bør:

- Kan være en eller flere leverandør(er).
- Lede arenaen hvor alle relevante aktører møtes
- Fremme åpne standarder
- Ha fokus på levetid
- Tilrettelegge for at andre aktører enn leverandøren(e) kan levere og delta i arenaen, dvs fokus på tredjepart og leverandørkjeden
- Hele tiden ha fokus på kunden og sikre en ”best for prosjektet” tilnærming
- Evne å ta i bruk den best tilgjengelige teknologi i markedet, uavhengig om den kommer fra leverandøren(e) eller andre
- Synliggjøre kosteffektiviteten av systemintegrators rolle og arenaen
- Være dyktig på å implementere ”beste praksis” på prosjekt og teknologi områder
- Være dyktig på gjennomføre gode prosjekter på alle nivå og med involvering av alle relevante aktører

Dette er til dels runde begreper som kan være vanskelig å effektuere, i alle fall alle på en gang. Samtidig ser vi behovet for en arena hvor man innen IKT området ikke bare møtes for å diskutrere fremtiden, men faktisk gjennomfører prosjekter til det beste for Forsvaret. Da trenger man antakelig noe mer enn bare en arena. Antakelig er det et behov for å heve leverandørbegrepet til et høyere nivå. Fremtvinge et mer langvarig samarbeid mellom de relevante aktører. Vi tror således at bruk av systemintegrator bør skje gjennom en Åpen Systemintegrator løsning som antakelig den mest farbare vei.

Spørsmålet blir da, hvordan vi implementerer en slik løsning.

8.4.2 CCIS House avtalen

En reell mulighet vi har sett på er en videreutvikling av dagens CCIS House avtale (Huset). Dette er en forhandlet samarbeidsavtale mellom Hærens forsyningskommando og den gang 5 norske IKT leverandører for forsvarsspesifikke IKT systemer. Siden den gang har de norske partnere gjennomgått en transformasjon, og utgjør i dag KDA, Thales og Ericsson.

I pkt 2 i avtalen sies følgende:

"Forsvarsdepartementet har definert K2IS som et satsningsområde for Forsvaret og for norsk industri. HFK ønsker ut i fra dette at norsk industri innen Hærens K2IS opptrer samlet og at industrien medvirker til en helhetlig K2IS løsning over levetiden. HFK ønsker gjennom dette å sikre faglig kompetent større til Hæren i alle prosjektfaser, prosjektgjennomføring, interoperabilitet mellom de enkelte prosjekter, tilegnelse og vedlikehold av kompetanse, gjenbruk av kompetanse og løsninger, kostnadseffektiv drift og vedlikehold av systemet."

Etter vårt skjønn inneholder pkt 2 mye av det vi ser som et behov fremover. Skal likevel bruk av Huset være relevant, vil det høyst sannsynlig være behov for justering av ramme og innhold.

For det første bør man gå vekk i fra den grenvise tilnærming i tråd med den reorganisering man har hatt i Forsvaret, og heve dette opp til å gjøres gjeldende for Forsvaret som sådan på områder hvor det er relevant teknologisk.

For det andre bør samarbeidsform med alle relevante aktører og nødvendig rolledeling beskrives bedre.

For det tredje bør Huset gjennom avtalen fremstå som et åpent overordnet systemhus for relevant norsk forsvarsindustri, på alle nivåer. Ut fra den arv Forsvaret besitter, bør forholdet til Teleplan beskrives av Huset gjennom en oppdatert samarbeidsavtale, enten de trer inn på eiersiden eller at man inngår en annen form for samarbeid.

Den klare fordel med å anvende avtalen med Huset som en plattform, er at den muliggjør en rask oppstart av en Åpen systemintegrator løsning. Nåværende avtales grunnleggende prinsipper er i tråd med hva vi foreslår. I forhold til kritisk kompetanse både nå og i fremtiden, utgjør eiersiden sentrale deler av IKT relatert forsvarsindustri i Norge. De justeringer som foreslås antas å kunne møte aksept hos relevante parter.

Ulempen er at man ikke vet om man kunne å klart å skreddersy en bedre løsning med delvis andre aktører eller en annen modell. Den uvissheten er etter vårt skjønn til å leve med, så lenge den reforhandlede avtale med Huset oppdateres med foreslåtte elementer.

8.4.3 Forslag til avtaleprinsipper for en Partnerskapsavtale

I punktet over har vi anbefalt at man videreutvikler samarbeidsavtalen med Huset. Uavhengig om dette lykkes, eller at man i stedet velger å lage en helt ny Partnerskapsavtale, har vi noen momenter som vi mener bør inn i en oppdatert avtale med Huset, eller en ny Partnerskapsavtale.

Grunnen til at vi fokuserer på de funksjonelle krav til en avtale, er at erfaring viser at tilpassede kontrakter er avgjørende for å kunne oppnå suksess i slike situasjoner. Kaasen-utvalget fra 2000, anfører i sin kritikk mot NORSOK[10] at man i for liten grad tilpasset kontraktene til de samarbeidsmodeller man valgte. NORSOK delrapport nr 3 (16), se s 23 beskriver ytterpunktene i kontraktene på følgende måte;

"DÅRLIGE KONTRAKTER	*GODE KONTRAKTER*
Manglende tillit	*Tillit og ansvar*
Selvsentrerte holdninger	*Motivert til endring*
Dårlig kommunikasjon	*Åpen kommunikasjon*
Rigid	*Fleksibel*
Unødig teknisk kompleks	*Forenklinger*
Motsetninger	*Samarbeid*
Strenge regler og spesifikasjoner	*Funksjonelle*
Etterkrav for endringer, feil, forsinkelser	*Belønning for presise og feilfrie leveranser, risikovillighet, kontinuerlig forbedring"*

Dette viser bare noen av de elementer som vi ser som viktige i gode avtaler. I tillegg er det viktig at begge parter betrakter samarbeidet som viktig for deres egne suksesser. For Forsvaret innebærer dette at avtalen, selv om man inngår et langsiktig forhold til en leverandør, ikke skader Forsvarets omdømme. Tvert i mot bør en slik avtale være med på å bygge opp under Forsvarets omdømme som en god og innovativ kunde hvis aktivitet bidrar til å skaffe Forsvaret kosteffektive løsninger i verdensklasse.

8.4.3.1 Forholdet til organiseringen av samarbeidet og håndtering av eneleverandør situasjoner

Organisering av en Åpen systemintegrator løsning kan være flere, og det finnes ingen fasit. Det som er klart, er at rolledelingen vil være avgjørende for suksessen. Det er i tillegg viktig å være bevisst på gjennomføringsmodellen partene ønsker, herunder ulike oppdrags- og prosjektformer, ansvars- og arbeidsdeling, grader av integrert organisering. Man vil med denne modellen kunne bevege seg inn i slike situasjoner for flere oppdrag/prosjekter.

Det er derfor essensielt at det fra Forsvarets side legges en kontraktsstrategi. For avtalens virkeområde bør det fokuseres spesielt på at;

- *Avtalen skal være konfliktforebyggende, herunder at den beskriver plassering av risiko og ansvar.*

[10] NORSOK (Norsk Sokkels Konkurranseposisjon)

- *Avtalen skal være konfliktløsende, herunder at den bidrar til klarhet.*
- *Den definerer en felles virkelighetsforståelse og referanseramme for arbeidet.*

Forsvaret har retningslinjer for valg av to hovedkontraktstyper; priskontrakter og kostnadskontrakter. Innen disse hovedtypene er det flere underkategorier. I priskontrakter er det leverandøren som bærer risikoen for kostnadene for å fullføre leveransen. I kostnadskontraktene er det Forsvaret (kunden) som bærer denne risikoen. For begge kategorier finnes det en rekke varianter (incentiver etc) og mulighet for å kombinere flere av prismekanismene i samme oppdrag.

Kriteriene for valg mellom disse forskjellige kontraktstypene er i hovedsak basert på i hvilken grad Forsvaret er i stand til å spesifisere omfanget av og kravene til leveransen, og om det kan etableres konkurranse om leveransen samt usikkerhetsnivået i kalkylen. Etter vårt skjønn synes det åpenbart at man ikke vil kunne forholde seg til kun et prisformat for den store variasjon som finnes blant de forskjellige oppdrag og prosjekter. Av den grunn er det viktig for en Partnerskapsavtale at man tillater flere varianter av prismekanismer i henhold til de forskjellige usikkerheter som bl.a. eksisterer.

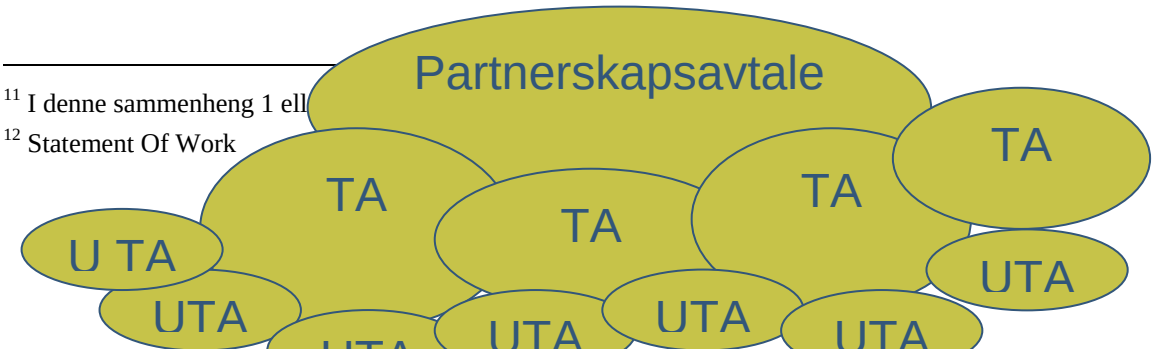
Det er videre viktig at man i et langsiktig forhold, hvor man i flere tilfeller vil være eneleverandør, tillater fullt innsyn i de regnskaper som leverandøren har i tråd med gjeldende regler i ARF. Utover dette, mener vi at man bør tillate en viss form for benchmarking av de ytelser av samarbeidet som sådan samt de ytelser som Forsvaret kontraherer. Dette tror vi er viktig for å dokumentere at man anskaffer kosteffektive tjenester.

8.4.3.2 Forslag til avtalestruktur

Vi har den oppfatning at man bør dele inn en Partnerskapsavtale i flere lag. På toppen dekker Partnerskapsavtalen alt samarbeid mellom FMO/FLO og Leverandøren[11]. På denne måte kan man avtale alt som skal gjelde av felles leveringsbetingelser, samarbeid osv. Dette gir også partene en unik mulighet til å gjennomføre en strategisk oppfølging av nåværende og eventuell fremtidig prosjektportefølje.

Under samarbeidsavtalen skal det være Technical Arrangements (TA) som følger opp samarbeidsavtalen og utfyller den på enkeltsystem nivå. TA skal gi adgang til å inngå SOW[12] for de respektive områder og utgjøre det utførende ledd av Partnerskapsavtalen. Inngåelse av en TA gir partene et verktøy til raskt å iverksette nye prosjekter, og gir partene anledning til å skille vedlikehold/prosjekt samt tilpasse med de riktige prismekanismer. Enten dette skjer ved inngåelse eller senere gjennom kontraktsrevisjon/innsyn i fm incentivordninger.

Under TA kan det inngås Underliggende TA (UTA) overfor tredjepart hvor man involverer andre leverandører etter behov.



[11] I denne sammenheng 1 ell

[12] Statement Of Work

Figur 7.3 Bilde av foreslått avtalestruktur for en Partnerskapsavtale

Med en slik tilnærming sikrer man seg i større grad et helhetlig bilde av de utfordringer man stor overfor i fremtiden. En Partnerskapsavtale bør bl a inneholde følgende forhold:

- Skissere langsiktig felles satsing innen utvalgte områder
- Sikre en minimumsaktivitet på 20-30 % av reell planlagt aktivitet i investerings/drift/oppdateringsplanen til Forsvaret over et lengre tidsom, for å garantere tilgang på relevant kompetanse
- Sikre fleksibilitet for begge parter i en omskiftelig verden
- Regulere kontakt på strategisk nivå hos partene
- Regulere innsats begge veier på arbeidsnivå
- Inneholde forslag til maler for inngåelse av underliggende TA'er
- Sikre hurtig oppstart av nye prosjekter
- Sikre forsvarlig etisk håndtering av avtalen
- Sikre merverdi for partene

FFI har inngått tilsvarende avtale med relevant IKT industri med suksess. I forhold til de temaer som skal behandles i en Partnerskapsavtale og de respektive TA'er , bør man sikre en enhetlig tilnærming innenfor bla følgende fokusområder;

- Kommunikasjon
- Ansvar
- Fremtidig utvikling
- Kvalitet
- Usikkerhet
- Leveringsplan
- Konkurranse

- Samarbeidshåndtering
- Økonomi
- Tid
- Fleksibilitet
- Samarbeidspartnere
- Responsitivitet

Det viktige er at man får så enhetlige standardbetingelser mellom partene som er tilpasset den samarbeidsform som ønskes. Eksempelvis for håndtering av usikkerhet, kan det være mulig å inkorporere en reforhandlingsrett /plikt innen pris/kostnader, eksempelvis ved utsatt fastsettelse av endelig pris etter at incentiver er gjennomført/benchmarking mot ekstern marked. Nærmere beskrivelse av en fremtidig avtalestruktur gjøres i FFI-rapport 2006/01373 - ”Fremtidsrettet avtalestruktur for forsvarsrelevante IKT-systemer og tjenester”.

9 KONKLUSJON OG ANBEFALING

Oppdraget fra FD var konkretisert i 5 problemstillinger som en ønsket å få belyst. Disse er alle gjennomgått i rapporten. Her ønsker vi å oppsummere kort svaret slik det har kommet frem gjennom analysen og arbeidet med rapporten.

9.1 Områder for samarbeid med industrien

Gjennomgang av de enkelte elementene i referansemodellen for INI, viser at norsk industri har levert en stor del arven slik den ser ut i dag. Dette er spesielt belyst i avsnitt 6.7. Forsvaret bør spesielt satse på å få til langsiktige avtaler med industrien knyttet til systemutvikling, systemintegrasjon og påfølgende drift og vedlikehold.

Det er ikke funnet hensiktsmessig å gi en anbefaling knyttet til enkelte prosjekter, da det er en prosess som Forsvaret selv må foreta knyttet til fremskaffelse.

9.2 Nasjonal kompetanse

IKT-området er i en svært dynamisk utvikling. Dette innebærer at en bør ha kompetanse på hele verdikjeden, fra FoU til drift og vedlikehold for å ha muligheter til å henge med i utviklingen. Forsvaret bør ha tilstrekkelig kompetanse til å beholde den overordnede styringen, samt ivareta fagmyndigheten for området. Dette gjelder spesielt for områder som arkitektur, integrasjon, konfigurasjonskontroll og sikkerhet. Det er også viktig for Forsvaret å ha tilstrekkelig kompetanse til å forstå og vurdere de løsninger som industrien tar fram. Industrien bør i større

grad kunne overta rollen som systemutvikler og systemintegrator, samt på enkelte områder overta vedlikehold og drift.

9.3 Kriterier for rådgivning og leveranser

Det er adgang til innenfor EØS området å benytte rådgivere til å utarbeide spesifikasjoner tilsvarende som senere deltar i konkurranse, gitt at visse retningslinjer følges som beskrevet under kapittel 8. For å sikre best mulig konkurranse i slike situasjoner, bør Forsvaret i størst mulig utstrekning anvende funksjonelle spesifikasjoner.

Utenfor EØS området gir ARF anføring på bruk av rådgivere, delvis i tråd med de sivile bestemmelser, men med større fleksibilitet. I den grad man ønsker avvik, kan FD gi dette. Den viktigste beskrankning er at forskjellsbehandling skal være saklig, selv om ARF ikke gir noen rettigheter til tredjepart idet ARF er et internt regelverk hjemlet i LOA.

9.4 Firmaer som er mest aktuelle

Det finnes i dag mange leverandører til Forsvaret. De som er mest aktuelle for langsiktig samarbeidsavtaler, vil være de som er i stand til å utøve rollen som systemutvikler og systemintegrator, og som samtidig har en viss kunnskap om arven. Pr i dag synes dette i første rekke å være KDA, Teleplan og Thales. I tillegg kommer CCIS House, som formelt står bak noen av systemene som Forsvaret har. Andre bedrifter vil etter vår vurdering i større grad være delsystemleverandører. Men det vil til enhver tid være Forsvarets behov som avgjør med hvem en ønsker å bygge langsiktige relasjoner med for videreføring av INI.

9.5 Behov for avtalestruktur

Vi ser et klart behov for en mer langsiktig, bredt og involverende avtalestruktur. Det foreslås å inngå en bred Partnerskapsavtale med relevant industri. I den sammenheng kan nåværende CCIS – House avtale med KDA, Thales og Ericsson danne grunnlag for en videreutvikling. Uansett er det sentrale å få frem en ny arena med en Åpen systemintegrator som den drivende kraft.

9.6 Anbefaling

Oppdraget gikk ut på å analysere konkrete problemstillinger for FD. I tillegg til besvarelsen på oppdraget, tillater vi oss å komme med to konkrete anbefalinger knyttet til området.

9.6.1 Gjennomgang av den interne organiseringen

Det anbefales at det gjennomføres en grenseoppgang mellom FD ved Programområdet INI, FK KKIS og FLO/IKT, der ansvar og myndighet for det enkelte organisasjonsledd klarlegges. Ved overlappende ansvar og myndighet, bør det ryddes opp, slik at en unngår uklarhet. Alternativt bør en se på muligheten av å samle hovedaktørene i en organisasjon.

9.6.2 Etablering av ”Systemhus”

Med utgangspunkt i problemstillingen knyttet til variantbegrensing og migrasjon av kommunikasjonsinfrastrukturen, og i den eksisterende avtalen med CCIS House, anbefales det at Forsvaret tar initiativ til å etablere en ny langsiktig avtale for samarbeid mellom Forsvaret og industrien innen programområdet INI.

Litteratur

(1) Policy for militær tilpasning og anvendelse av informasjons- og kommunikasjonsteknologi i Forsvaret, 1. september 2005

(2) Konsept for styring av elektronisk informasjon i Forsvaret, 1. september 2005

(3) Overordnet materiellplan for programområde informasjonsinfrastruktur (2005- 2008+)

(4) Skogstad Arne K, Warberg Erik N (2005) Revisjon av de teknologiske kompetanse- og satsningsområder for Forsvaret og norsk forsvarsindustri, FFI/Rapport -2005/01678

(5) Gagnes Tommy, Eggen Anders, Hedenstad Ole-Erik, Rasmussen Rolf, Sletten Geir (2005) Operative beslutningsstøttetjenester – fremtid NBF, FFI/Rapport – 2005/03584

(6) Warberg, Erik N (2006) Industriens rolle som både leverandør og rådgiver- muligheter og begrensninger, FFI/Rapport 2005/01115

(7) Warberg, Erik N (2006) Folkerettslige forhold ved bruk av leverandører i internasjonale operasjoner, FFI/Rapport-2006/ 01328-1

(8) Warberg, Erik N (2006), Fremtidsrettet avtalestruktur for forsvarsrelevante IKT-systemer og tjenester, FFI/Rapport 2006/01373

APPENDIKS 1 – OPPDRAG FRA FD

Forsvarets forskningsinstitutt

U Off § 5.2a

Feil! Ukjent dokumentegenskapsnavn. **Feil! Ukjent dokumentegenskapsnavn.** **Feil! Ukjent dokumentegenskapsnavn.**

2005/01782-6/FD IV/OG

PROSJEKT 1024- OPPDRAG TIL FFI SOM LEDD I OPPFØLGINGEN AV SEMINAR MED IKT-INDUSTRIEN

Bakgrunn
FSJ og Sjef FD IV arrangerte tirsdag 16. august 2005 et seminar med IKT-industrien med fokus på kompetansebehov for å ivareta IKT- "arven". Som ledd i oppfølgingen ble det bestemt at en intern arbeidsgruppe (AG) med følgende mandat skulle etableres:

> *"Med bakgrunn i de konkrete innspillene fra industrien vurdere hvilke kapasitets- og kompetansebehov Forsvaret har for ivaretakelse av "arven. Komme opp med forslag til initiativer som er tilstrekkelig for at kjernevirksomheten i allerede anskaffet IKT-kapasitet skal kunne bli vedlikeholdt og oppgradert."*

AG's arbeid er nå avsluttet og gruppens konklusjon som departementet har sluttet seg til er å gi et oppdrag til FFI under prosjekt 1024 "Støtte til materiellanskaffelser og industrisamarbeid". Dette er gjort med utgangspunkt i FFIs rapport vedrørende teknologiske kompetanseområder for Forsvaret og forsvarsindustrien.

Status
Prosjekt 1024 "Støtte til materiellanskaffelser og industrisamarbeid" skal støtte FD i implementeringen av det nye investeringskonseptet. Innen rammen av Prosjekt 1024 vil FFI være en egnet instans til å vurdere og anbefale en håndtering av hvordan vi best kan nytte og videreføre IKT-industriens kapasitets- og kompetansebehov for den delen av "arven" som skal beholdes. Industriens rolle og Forsvarets behov ved drift og vedlikehold av arven er i stor grad uavklart. Det blir hevdet av man står i fare for at kompetansemiljøene forvitrer.

Oppdrag
I tråd med intensjonene i Prosjekt 1024 ønsker departementet at FFI foretar en gjennomgang og analyse av:

- Forsvarets IKT – portefølje for å avklare hvilke systemer som bør vedlikeholdes/videreutvikles i samarbeid med industrien. Arbeidet skal skje i samarbeid med Programområde INI.
- hvilken nasjonal kompetanse som er nødvendig innen dette feltet, herunder hvilke kapasiteter (kunnskap og volum) Forsvaret må besitte og hvilke som kan settes ut til industrien når det gjelder både vedlikehold og videreutvikling av arven.

- hvilke kriterier som må etableres for å skille industriens rolle som leverandører og rådgivere slik at en unngår en blanding av disse.
- hvilke firmaer som er de mest aktuelle for utvikling av et samarbeid. I denne sammenheng skal de mest kritiske prosjektene prioriteres.
- behovet for en avtalestruktur mellom forsvaret og industrien for de mest tidskritiske prosjektene, samt utarbeide forslag til intensjonsavtaler.

På møtet mellom departementet og FFI 20. oktober d.å. ble en enig om prioritering og tidsplan. Oppdraget skal være fullført og rapport foreligge inne 30. april 2006. I arbeidet skal oppdragene under de 3 siste kulepunktene gis førsteprioritet og delrapportene som dekker disse områdene skal leveres Forsvarsdepartementet innen 31. desember 2005.

Kontaktperson i Forsvarsdepartementet er major Lasse Halaas, Programleder INI.

Med hilsen

Pål Bjørseth (e.f.)
avdelingsdirektør

Ole Garshol
Underdirektør

Kopi: Materielldirektøren
FD IV 3