Policy for militær tilpasning
og anvendelse av

informasjons- og kommunikasjonsteknologi

i Forsvaret

Godkjent 1. september 2005 - 2. opplag

Innhold

1. Hensikt

Hensikten med denne policyen er å skape grunnlag for en felles virksomhetskultur i Forsvaret for militær tilpasning og anvendelse av informasjons- og kommunikasjonsteknologi (IKT). Dette innebærer spesielt å synliggjøre et felles målbilde, samt å gi sentrale føringer. Således har policyen både en forklarende og en styrende funksjon.

Policyen er en videreføring av intensjoner og styringssignaler gitt i tidligere langtidsmeldinger og proposisjoner, med økt fokus på tilpasning og anvendelse av IKT i en operativ ramme.

2. Virkeområde

Denne policyen gjelder for all militær tilpasning og anvendelse av IKT i Forsvaret. Policyen (IKT-policy) er veiledende når IKT utelukkende brukes til forskning, utvikling og eksperimentering.

Behov for revisjon vil bli vurdert årlig.

3. Målbilde

Bruk av teknologi, og da spesielt IKT, er et sentralt virkemiddel for transformasjon av Forsvaret. Gjennom sikker deling og utveksling av informasjon på tvers i nettverk, får våre styrker et mer fullstendig og oppdatert beslutningsgrunnlag. Vi får dermed mulighet til å handle raskt, synkronisert, og med riktig virkemiddel i forhold til det situasjonen krever.

Nye løsninger innenfor IKT skaper et 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 begrensninger i typene og antall av eksisterende løsninger og en bedre samordning av disse, vil gi store gevinster.

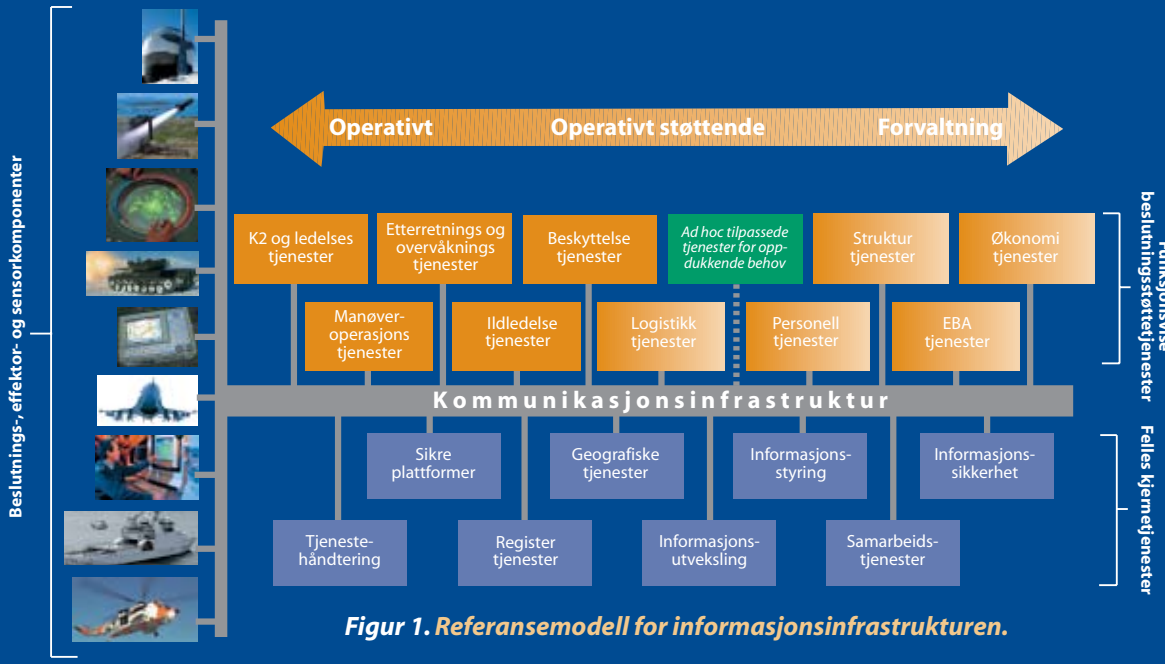
Kjernen i militært tilpasset og anvendt IKT benevnes forsvarets informasjonsinfrastruktur. Den omfatter informasjon, prosesser, standarder og teknologi, samt menneskene som drifter og vedlikeholder den. Fremtidens informasjonsinfrastruktur skal understøtte nettverksbaserte operasjonsformer gjennom å muliggjøre organisering av Forsvarets ressurser i samvirkende nettverk, fra strategisk til stridsteknisk nivå, både nasjonalt, med allierte styrker og koalisjonspartnere, samt med relevante sivile instanser. Hensynet til interoperabilitet er derfor den viktigste føringen for informasjonsinfrastrukturen. Videre skal forbedringer innenfor viktige operative egenskaper som fleksibilitet, reaksjonsevne og deployerbarhet tillegges vekt.

4. Referansemodell for informasjonsinfrastrukturen

Figur 1 viser den nye 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 på løsninger som er så nær opp til referansemodellen som det er teknisk og økonomisk forsvarlig på realiseringstidspunktet.

Informasjonsinfrastrukturen består av funksjonsvise beslutningsstøttetjenester og kjernetjenester, bundet sammen av kommunikasjonsinfrastrukturen.

- *De funksjonsvise beslutningsstøttetjenestene understøtter grupper av brukere med felles informasjonsbehov og prosesstøtte. De skal benytte kjernetjenestene.*



Figur 1. Referansemodell for informasjonsinfrastrukturen.

- *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.*

- *Kommunikasjonsinfrastrukturen tilbyr kvalitetssikrede mekanismer for forbindelse mellom beslutningsstøtte- og kjernetjenestene, samt koblingen mellom disse og de ulike beslutnings-, effektor- og sensorkomponentene.*

Prinsipielt er alle tjenestene uavhengige av hverandre, og av løsninger for kommunikasjon. Det er de ulike tjenestene som skal representere grensesnittet mellom informasjonsinfrastrukturen og beslutnings-, effektor- og sensorkomponentene.

Tjenestene i referansemodellen er nærmere forklart på side 11.

5. Føringer for militær tilpasning og anvendelse av IKT

5.1 Sentral styring

IKT er et sentralt virkemiddel i den ønskede transformasjonen mot mer 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-investeringer 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 bruk av arkitekturer. Fokus skal legges på å identifisere de viktigste egenskapene ved Forsvarets virksomhet, samt grensesnitt og informasjonsflyt mellom ulike deler av virksomheten.

5.2 IKT som katalysator for endring og gevinstrealisering

Informasjonsinfrastrukturen skal sette Forsvaret i stand til å øke effekten av andre investeringer og skape muligheter for kostnadsreduksjoner. For å oppnå full effekt av moderne IKT, kreves det også at Forsvaret samtidig endrer de prosesser og organisasjonsstrukturer som omgir teknologien.

Moderne IKT kan være kostbart isolert sett, og bidra til å øke kostnadene i enkelte deler av Forsvarets IKT virksomhet. Ved bevisst å bruke innføring av IKT som en integrert del av en bredere omlegging, vil man likevel oppnå en samlet gevinst gjennom uttak av gevinster i andre deler av virksomheten.

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 satsinger på dette området.

5.3 Brukerfokus

Tjenestene i informasjonsinfrastrukturen skal i størst mulig utstrekning ha et enhetlig brukergrensesnitt. Tjenestene skal tilby relevant brukerveiledning, og må være robuste i forhold til mulige brukerfeil. Nye tjenester skal være godt testet før innføring, og nødvendig tid avsatt til kompetansebygging.

Det er sentralt at brukernes kompetanse følger med i takt med utbredelse og økning av tjenestespekteret i informasjonsinfrastrukturen. Dette omfatter blant annet evnen til å ta i bruk de mulighetene som finnes i moderne IKT, og å utnytte dem kritisk og innovativt til læring og arbeid.

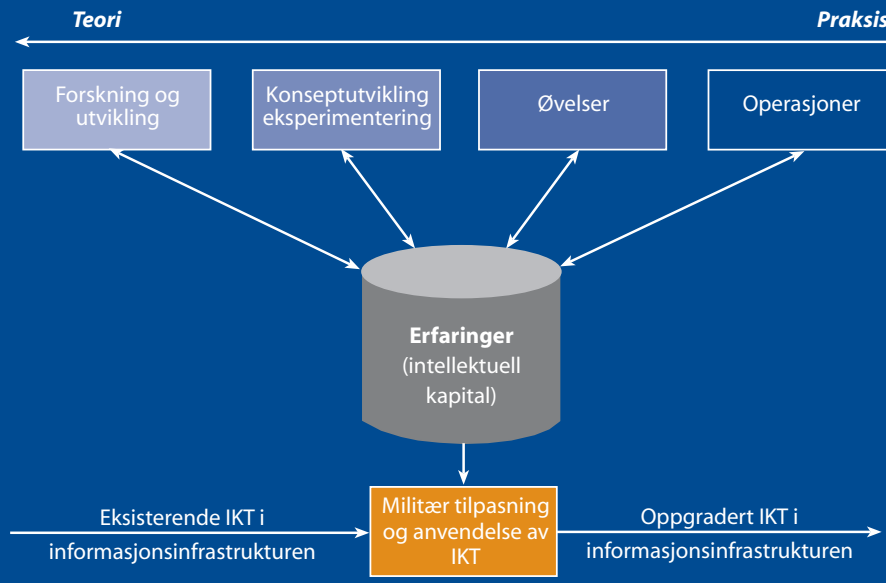
5.4 Tilpasning og anvendelse

Militær tilpasning med påfølgende anvendelse skal gis prioritet fremfor 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.

Normalt skal løsninger som tilpasses og anvendes til militære formål være i produksjon.

5.5 Prosess for militær tilpasning og anvendelse av IKT

Figur 2 viser en generell prosessmodell for hvordan forskning, eksperimentering, konseptutvikling, øvelseserfaringer og operasjoner gjensidig bidrar til å utvikle kunnskap om hvordan moderne IKT kan tilpasses og anvendes militært.



Figur 2. Kultivering av informasjonsinfrastrukturen.

Det er en målsetting at vi tar lærdom av det vi gjør, både det som var bra og det som ikke førte frem, og at vi forvalter dette på en måte som kommer den enkelte medarbeider og Forsvaret til gode.

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.

5.6 Standardisering og variantbegrensning

Det skal tilstrebes en utvikling der typene og antallet av IKT løsninger reduseres og samordnes bedre både innenfor og på tvers av graderingsnivåer. Dette vil i seg selv utgjøre et viktig bidrag til interoperabilitet. Felles løsninger på tvers av forsvarsgrenene har prioritet, og skal benyttes der dette er mulig.

Det skal i større utstrekning benyttes standardisert, lettere, og gjerne også billigere sluttbrukerutstyr, som kan følge med styrker nasjonalt og internasjonalt.

Det skal også søkes en større grad av enighet om innholdet i virksomhetsprosessene.

5.7 Modularitet og standardiserte grensesnitt

For at informasjonsinfrastrukturen skal kunne understøtte nettverksbaserte operasjoner, skal fokus flyttes fra selve applikasjonene til løsninger som gjør informasjon og tjenester tilgjengelig gjennom standardiserte grensesnitt.

Det skal fokuseres på åpne industri- og alliansestandarder som har en minimum kritisk masse av brukere. Standarder må være fleksible og svare på konkrete behov. Oppbygningen av informasjonsinfrastrukturen, samt de standarder som legges til grunn, skal bidra til at Forsvaret effektivt kan operere sammen med nåværende og nye samarbeidspartnere både nasjonalt og internasjo-

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

5.8 Kontinuerlig tilpasning og oppgradering

Nye løsninger skal utvikles med mulighet for kontinuerlig tilpasning og oppgradering, ikke bare for total utskifting. Fleksibilitet skal være et bærende prinsipp, blant annet gjennom en løpende evaluering av nye løsninger. Informasjonsinfrastrukturen utvikles over en lengre tidsperiode, i form av utvidelser, forlengelser og forbedringer av den eksisterende infrastrukturen. Det betyr at videreutvikling av en stor infrastruktur er en kontinuerlig prosess.

Fokus skal rettes mot å anvende militært tilpasset IKT for de som planlegger, støtter, gjennomfører og leder operativ virksomhet, det vil si de elementene som faktisk involveres når militærmakt utøves.

5.9 Tilrettelegging for informasjonsstyring

Informasjonsstyring dreier seg først og fremst om den informasjon de ulike tjenestene gir adgang til og hvordan den behandles og fordeles, og i mindre grad om teknologi. Informasjonsinfrastrukturen må understøtte at også andre enn dataprodusentene får tilgang til mer enn rå fakta - de får informasjon (data med kontekst, et budskap). Tjenester for å beskrive data slik at det skapes sammenheng og relevans er derfor viktige.

Effektiv informasjonsstyring har mye med kultur og holdninger å gjøre. Det må derfor utvikles kompetanse om hvordan man kan gjenbruke og dele informasjon elektronisk, og ikke minst hvordan organisasjonen kan utvikle en delings- og gjenbruksadferd.

5.10 Sikkerhet

Nettverksbaserte operasjoner gir en økt avhengighet av informasjonsinfrastrukturen, og derved en følsomhet for manipulasjon, degradering og tap av denne. Sikkerhet skal derfor håndteres som en

integrert del av informasjonsinfrastrukturen, og innarbeides i tilpasnings- og utviklingsprosesser fra starten. Støtte for sikker drift og vedlikehold, samt evne til deteksjon av sikkerhetsbrudd, incidenthåndtering og gjenoppretting, skal tillegges vekt. Ved valg av løsninger, skal sikkerhetsmessig integrasjon og interoperabilitet vektlegges for å unngå fragmentering av infrastrukturen, med tilhørende brudd i informasjonsflyt og tjenester.

Evnen til å dele informasjon i fleksible og dynamiske nettverk, samt å utnytte tilgjengelige militære og kommersielle kommunikasjonsressurser er forutsetninger for nettverksbaserte operasjoner. Fremtidens sikkerhetsløsninger skal derfor fokusere mer på sikring av konfidensialitet, integritet, autentisering og tilgangskontroll knyttet til informasjon og tjenestene, og noe mindre på det transport mediet de transporteres på. Sikkerheten knyttet til fysisk transmisjon skal rettes mer mot tilgjengelighet og evnen til å bruke alternative kommunikasjonsressurser.

For å sikre tjenester i informasjonsinfrastrukturen, vil bruk av Public Key Infrastructure (PKI) være et vesentlig bidrag. Ved anvendelse av PKI for tjenester som er sikkerhetsgradert, skal kravene fra Nasjonal sikkerhetsmyndighet basert på NATOs «PKI Certification Policy» følges. Forsvaret må videre forholde seg til statens satsning på en sikkerhetsportal for offentlige sektor for relevante tjenester.

6. Iverksetting

Denne policyen iverksettes med virkning fra og med 1. september 2005. Den erstatter tidligere utgitte IKT-policyer.

Kort forklaring av tjenestene i referansemodellen

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

Funksjonsvise beslutningsstøttetjenester

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

Felles kjernetjenester

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

Policy for militær tilpasning
og anvendelse av
informasjons- og kommunikasjonsteknologi
i Forsvaret

Utgitt av
Forsvarsdepartementet
Glacisg. 1
Postboks 8126 Dep
0032 Oslo

www.forsvarsdepartementet.no

ISBN 978-82-7924-055-6

FORSVARSDEPARTEMENTET