FFI Forsvarets forskningsinstitutt

23/00409

FFI-RAPPORT

Forsvarets IKT

– utvalgte anbefalinger

Joakim Flathagen
Ann-Kristin Elstad
Monica Endregard
Bodil Farsund
Ole Ingar Bentstuen
Ketil Lund
Anders Mykkeltveit
Trude Bloebaum

Forsvarets IKT
– utvalgte anbefalinger

Joakim Flathagen
Ann-Kristin Elstad
Monica Endregard
Bodil Farsund
Ole Ingar Bentstuen
Ketil Lund
Anders Mykkeltveit
Trude Bloebaum

Forsvarets forskningsinstitutt (FFI) 30. mars 2023

Emneord
IKT
Sourcing
Sikkerhet
Kompetanse
Satellittkommunikasjon
5G

FFI-rapport
23/00409

Prosjektnummer
1643

Elektronisk ISBN
978-82-464-3466-7

Engelsk tittel
Norwegian Armed Forces ICT – selected recommendations

Godkjennere
Jan Erik Voldhaug, *forskningssjef*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Moderne informasjons- og kommunikasjonsteknologi (IKT) er sentralt for å kunne understøtte Forsvarets operative evne. Det er også viktig at Forsvaret kontinuerlig utvikler organisasjonen, slik at teknologien til enhver tid utnyttes på en best mulig måte.

Forsvaret har ambisjoner om en omfattende digitalisering av virksomheten. Samtidig har tidligere undersøkelser avdekket at Forsvaret per i dag har utfordringer med å fremskaffe og nyttiggjøre seg av IKT. Det tar lang tid fra et behov oppstår og til det er dekket. Forsvarssektoren har nå iverksatt flere strategiske grep for kunne å nå ambisjonene og møte utfordringene. Blant annet er det startet store virksomhetsprogrammer for å anskaffe og anvende ny IKT.

Denne rapporten er ment å hjelpe Forsvaret ved å gi anbefalinger om IKT-virksomheten og om hvordan IKT kan anvendes. Anbefalingene er basert på studier som allerede er gjennomført av FFI, hovedsakelig i perioden 2020–2022.

Vi har valgt ut følgende fem hovedtema som vi mener er viktige på kort sikt:

1. *Kvalitet i beslutningsprosessene.* Vi har spesielt studert hvordan en kan oppnå bevisst og målrettet anvendelse av IKT. Vi anbefaler blant annet at Forsvarets beslutninger bør være sporbare og at Forsvaret i størst mulig grad bør styre etter prinsipper om strukturert fleksibilitet.

2. *Sourcing og strategisk partnerskap.* Vi beskriver faktorer som bør inngå i forbindelse med sourcing av Forsvarets IKT. Vi anbefaler spesielt å belyse transaksjonskostnader og implikasjoner for krigens folkerett når strategiske partnerskap inngås.

3. *Forsvarssektorens kompetanseutvikling innen IKT-området.* Vi omtaler de ulike typene av digital kompetanse og strategisk IKT-kompetanse som forsvarssektoren har behov for. Vi anbefaler at Forsvaret utarbeider et målbilde om hva slags IKT-kompetanse sektoren må ha selv, og en strategi for hvordan kritisk IKT-personell kan rekrutteres og beholdes.

4. *Forsvarlig sikkerhet*. Vi presenterer et verdihierarki som utgangspunkt for risikobaserte vurderinger. Vi anbefaler at Forsvaret definerer sikkerhetskrav for IKT. Disse må kontinuerlig oppdateres slik at et forsvarlig sikkerhetsnivå kan ivaretas.

5. *Digital grunnmur.* Vi poengterer hvor viktig det er å få på plass en digital grunnmur og at det bør utarbeides strategier for noen sentrale teknologier som satellitt- og mobilkommunikasjon.

Rapporten er primært skrevet for Forsvarsstabens IKT-avdeling (FST J6), men anbefalingene som er gitt i rapporten vil også være relevante for øvrige beslutningstakere og personell som jobber med investering og strategisk styring av IKT-virksomheten.

Summary

Information and communication technology (ICT) is crucial to support the Norwegian Armed Forces operations as well as the future development of the organization. The Armed Forces have recently implemented several strategic measures and have initiated large business programs to improve, acquire and use new ICT.

This report intends to help the Armed Forces' ICT organization by providing recommendations regarding the use of ICT. We base the recommendations on studies that have already been carried out by FFI, mainly during the period 2020–2022. The report covers these five areas:

1. *Quality in the decision-making processes*, where we have particularly looked at how to achieve conscious and targeted use of ICT within the organization.

2. *Sourcing and strategic partnership,* where we consider several factors that should be taken into account when considering sourcing of the Norwegian Armed Forces' ICT.

3. *ICT competence*, where we discuss the different types of digital competence and strategic ICT competence that the Armed Forces needs.

4. *Appropriate level of security*, where we present a value based hierarchy as a starting point for risk-based assessments.

5. *Digital backbone,* where we emphasize the importance of building a digital backbone. Further, we point out that for some key technologies in the backbone, such as satellite and mobile communications, separate strategies should be drawn up.

The recommendations given in the report are relevant for decision-makers and personnel who work with strategic management of ICT.

Innhold

1 Innledning

Norge og våre allierte står overfor et stort spekter av krevende sikkerhetsutfordringer og Forsvaret spiller en avgjørende rolle for at Norge skal kunne håndtere disse. For at Forsvaret skal kunne opprettholde og forbedre sin evne til å løse sine oppgaver er det viktig at organisasjonen kontinuerlig fornyes og videreutvikles. Moderne informasjons- og kommunikasjonsteknologi (IKT) er en viktig del av denne fornyingen, noe som understrekes i langtidsplanen for forsvarssektoren, der det uttrykkes at moderne IKT-løsninger er «nødvendig for å understøtte operativ evne og for effektiv gjennomføring av virksomheten i forsvarssektoren».[1]

1.1 IKT – betydning for Forsvaret

Begrepet «Informasjons- og kommunikasjonsteknologi» (IKT) er en samlebetegnelse for teknologi for innhenting, overføring, bearbeiding, lagring og presentasjon av informasjon. Forsvarssektoren anvender IKT innenfor både rene administrative kontorsystemer, i operativ sammenheng, integrert i kampplattformer, samt integrert i bygg og anlegg i form av industrielle IKT-systemer.

Forsvaret har ambisjoner om omfattende digitalisering og har uttrykt sin satsing gjennom en egen digitaliseringsstrategi.[2] IKT-utviklingen går i dag raskt. I dag er IKT innebygget i produkter og tjenester, i samhandling med ulike interessenter og i arbeidsprosesser, noe som gjør det stadig vanskeligere å definere hva merverdien av IKT er for Forsvaret og hva den bør være.[3] Implementering av ny IKT kan potensielt føre til endringer, både i Forsvarets organisasjon og i de prosessene hvor teknologien anvendes. Ny IKT kan også gjøre at det må etableres nye prosesser. De teknologiske endringene som skjer gjennom digitalisering vil derfor forme Forsvarets organisasjon og arbeidsprosesser, og vil skape nye utfordringer som må håndteres.[4]

For å oppnå effekt av IKT fordrer det en systematisk kobling mellom teknologien, organisasjonens mål og strategier samt den bevisste målrettede anvendelsen.[5] IKT har isolert sett liten verdi, det fordres at den benyttes i en eller annen arbeidsprosess. «Benyttes» vil, i denne sammenheng, omhandle selve IKT-løsningen, sluttbrukerens anvendelse og hvordan organisasjonen og dens interessenter er innrettet for å støtte opp om disse faktorene.[6] Investering i de nyeste og beste IKT-løsningene vil derfor ikke automatisk føre til at Forsvaret løser sine

[1] Forsvarsdepartementet. (2020a). Prop. 14 S (2020–2021) *Evne til forsvar – vilje til beredskap*. Langtidsplan for forsvarssektoren.
[2] Forsvarsstaben. (2018). *Digitaliseringsstrategi for Forsvaret*.
[3] Paré, G., Guillemette, M. G., Raymond, L. (2020). IT centrality, IT management model, and contribution of the IT function to organizational performance: A study in Canadian hospitals. *Information & Management*, 57(3), 103198.
[4] Cortellazzo, L., Bruni, E., Zampieri, R. (2019). The Role of Leadership in a Digitalized World: A Review. *Frontiers in Psychology*, 10(1938).
[5] Elstad, A. K., Lund, K., Kristiansen, S., Bloebaum, T. H. (2022a). *Informasjonsdeling i Forsvarets beslutningsprosesser – kritiske suksessfaktorer* (FFI-rapport 22/00146). Forsvarets forskningsinstitutt.
[6] Ibid.

oppgaver mer effektivt. Som vi skal se i kapittel 2 har vi identifisert fem kritiske suksessfaktorer[7] som sammen med IKT kan bidra til bedret organisatorisk effektivitet.[8] For at IKT skal kunne bidra til dette må den sees i kontekst med de prosessene og den organisasjonen den skal inkluderes i.

For å hente mest mulig effekt ut av digitaliseringen, må IKT-utvikling være driveren for endringer i både prosesser og organisering.[9] I forsvarssektoren satses det betydelig innenfor IKT-området og i perioden fra 2022 til 2029 er det planlagt investeringer på rundt 20 milliarder kroner under programområde Informasjonsinfrastruktur (INI).[10] Forsvaret anskaffer også IKT ut over dette for kampplattformer som ubåter, kampfly og kampvogner. I tillegg til investeringskostnader kommer driftskostnader knyttet til IKT på om lag 3,5 milliarder kroner årlig.[11]

Gjennom Forsvarets tildelingsbrev for 2022 er Forsvaret pålagt å frigjøre minst 1,9 milliarder kroner innen utgangen av 2024 gjennom målrettede moderniserings- og effektiviseringstiltak.[12] IKT kan bidra til dette, for eksempel ved å automatisere og forenkle manuelle arbeidsoppgaver. Men det må påpekes at kostnadseffektivisering ikke er den eneste gevinsten med IKT. IKT kan også utnyttes til å gjennomføre prosesser på måter som gir operative gevinster.[13] Et eksempel på dette er hvordan ny kommunikasjonsteknologi kan legge til rette for bedre og helt nye samhandlingsformer mellom sensor, beslutningstaker og effektor, noe som gjør at disse funksjonene kan distribueres. Dette kan gi helt nye operative muligheter for Forsvaret.[14]

I «Forsvarsanalysen 2022»[15] undersøkes status i Forsvaret i dag og i hvilken grad det er balanse mellom Forsvarets oppgaver, økonomi og struktur. Én av hovedutfordringene som rapporten identifiserer er at det i dag er:

«… sårbarheter i evnen til å kommunisere og utveksle data over lange avstander i scenarioer der dette blir aktivt motarbeidet fra en motstander.»

Å løse denne komplekse utfordringen stiller store krav til Forsvarets bruk av IKT, og det vil sannsynligvis være nødvendig med tiltak både når det gjelder hvordan Forsvaret fremskaffer og opprettholder sin IKT, hvordan IKT-løsningene til Forsvaret settes sammen, og hvilke IKT-løsninger Forsvaret velger å bruke og hvordan de velger å bruke dem. Som vi også skal se i

[7] Kritiske suksessfaktorer gjelder både kontrollerbare faktorer, kalt beslutningsvariabler, og ikke-kontrollerbare variabler.
[8] Organisatorisk effektivitet handler om å gjøre de riktige tingene gjennom bedre styring, mer effektiv kommunikasjon og informasjonsdeling, samt bedre beslutningsstøtte m.m.
[9] Forsvarsstaben. (2021). *Forsvarets IKT-strategi. Økt operativ effekt gjennom robust IKT i kontinuerlig utvikling – IKT for morgendagens forsvar.*
[10] Forsvarsdepartementet (2022b). *Framtidige anskaffelser til forsvarssektoren 2022–2029*. Kap. 4.5 Cyberdomenet.
[11] Arnfinnson, B., Elman, E., Eriksen. H.S. (2020). *Hvor mye bruker forsvarssektoren på IKT?* (FFI-rapport 20/00806) (BEGRENSET). Forsvarets forskningsinstitutt.
[12] Forsvarsdepartementet (2021a). *Tildelingsbrev for Forsvaret 2022.*
[13] Elstad et al. (2022a).
[14] Diesen, S. (2022). *Teknologiutviklingens påvirkning på militære styrker og bruken av militærmakt.* (FFI-rapport 22/01682). Forsvarets forskningsinstitutt.
[15] Skjelland, E., Berg-Knutsen, E., Arnfinnsson, B., Diesen, S., Glærum, S., Guttelvik, M. S., Kvalvik, S., Mørkved, T., Olsen, K. E., Sellevåg, S. R., Sendstad, C., Strand, K. R., Voldhaug, J. E. (2022). *Forsvarsanalysen 2022.* (FFI-rapport 22/00659). Forsvarets forskningsinstitutt.

denne rapporten er digital kompetanse, hensiktsmessig organisering, og et godt samarbeid med eventuelle strategiske partnere andre viktige faktorer for å løse utfordringen.

1.2 Noen utfordringer for IKT-området i forsvarssektoren

Store statlige investeringer, som Forsvaret har mange av, er i seg selv kompliserte prosesser med høy risiko. Riksrevisjonen pekte i 2022 på risiko knyttet til leveranser og måloppnåelse i Forsvarets to store IKT-programmer Mime og MAST.[16]

Det er dessuten identifisert flere utfordringer når det gjelder Forsvarets evne til å nyttiggjøre seg av ny teknologi.[17] Én utfordring er at det tar lang tid fra et behov oppstår til behovet er dekket.[18] FFI undersøkte i 2018 fremdriften i Forsvarets materiellanskaffelser og fant at IKT-prosjekter, som typisk hadde en planlagt tidsbruk på tre år, hadde en gjennomsnittlig forsinkelse på over to år.[19] Det ble også funnet vesentlige forsinkelser i materiellinvesteringsporteføljen da den på ny ble undersøkt i 2021.[20] En av årsakene til forsinkelsene kan ligge i at en stor andel av IKT-prosjektene er utviklingsprosjekter, der nye komponenter må utvikles for å møte Forsvarets behov og krav.[21] Det er naturligvis vanskeligere å beregne tidsbruken for et utviklingsprosjekt enn for et prosjekt som anskaffer hyllevare.

I tillegg til at forsinkelser kan være et problem, finnes det også mange eksempler på at kostnadene i statlige IKT-anskaffelser kan bli betydelig høyere enn planlagt.[22]

Selv om digitaliseringsprosjekter har stor oppmerksomhet på å levere spesifisert funksjonalitet, til avtalt tid og uten overskridelse av budsjett så har en tradisjonelt hatt liten oppmerksomhet på det å planlegge, styre etter og evaluere realisert nytte.[23] Den senere tiden har imidlertid nyttestyring blitt viet større oppmerksomhet, også innen forsvarssektorens IKT-programmer.

1.3 Strategiske grep som er tatt innen IKT-området

Forsvarssektoren har iverksatt strategiske grep for å møte utfordringene som er nevnt over. Et av grepene er at Forsvaret i 2021 overtok ansvaret for å utøve og videreutvikle den strategiske

[16] Riksrevisjonen. (2022). *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner* (Ugradert versjon av Dokument 3:3 (2022−2023)).
[17] Forsvarsdepartementet. (2019). *IKT-strategi for forsvarssektoren - Hoveddokument* (Godkjent av Forsvarsministeren 27. mars 2019.).
[18] Ibid.
[19] Presterud, A. O., Øhrn, M., Waage, K., Berg, H. (2018). *Effektive materiellanskaffelser i Forsvaret – kartlegging av tidsbruk, forsinkelser og gjennomføringskostnader* (FFI-rapport 18/00231). Forsvarets forskningsinstitutt.
[20] Presterud, A.O., Lien, B., Voldhaug, J.E. (2022). «*Porteføljestyring i forsvarssektoren – status i leveranseoppfølgingen*». (FFI-rapport 22/01167). Forsvarets forskningsinstitutt.
[21] Berg, H., Waage, K. (2020). *Effektive materiellanskaffelser i Forsvaret – øker andelen hyllevarekjøp.* (FFI-rapport 20/03147). Forsvarets forskningsinstitutt.
[22] Finne, H. (2019). *Styring og gjennomføring av store statlige IKT-prosjekter. Ekspertenes erfaringer og vurderinger*. Concept-rapport nummer 56.
[23] Berg, H., Holgeid, K., Jørgensen, M., Volden, G. H. (2021). *Hvordan lykkes med digitalisering? En undersøkelse av nyttestyring i IT-prosjekter i offentlig sektor.* Concept-rapport nummer 64.

IKT-styringen i forsvarssektoren.[24] Forsvaret opprettet samme år IKT-avdelingen i Forsvarsstaben (FST J6). Sjef FST J6 fungerer som forsvarsledelsens rådgiver innenfor IKT og styrer IKT-virksomheten[25] i forsvarssektoren innenfor rammer gitt av Forsvarsdepartementet.[26] FST J6 har blant annet ansvar for å:

- Lede oppfølging av IKT-strategien og videreutvikle forsvarssektorens IKT-styringsmodell.
- Anbefale utvikling og modernisering av IKT-området.
- Koordinere arbeidet med IKT-porteføljen, herunder ivareta programeierrollen for IKT-programmene MAST og Mime.
- Lede og koordinere arkitektur- og sikkerhetsstyring for IKT i forsvarssektoren.
- Koordinere forsvarssektorens kompetanseutvikling innenfor IKT-området.
- Videreutvikle forsvarssektorens IKT-styringsmodell og IKT-strategi.
- Koordinere IKT-løsninger for å understøtte offentlig digitaliseringsarbeid.
- Anbefale utrangering eller sanering av IKT-materiell som ikke lenger skal brukes.

FST J6 har gitt ut en IKT-styringsmodell for forsvarssektoren, som reflekterer de sentrale styringsområdene til IKT-virksomheten.[27] Ett av styringsområdene er porteføljestyring, der det foreslås en ny innretning for IKT-finansiering, drift og investering. FST J6 har i 2023 utgitt en digital reguleringsplan (DRP), som på et strategisk nivå regulerer hvordan IKT skal prioriteres, utvikles, forvaltes og driftes. I denne DRP-en er det identifisert åtte innsatsområder, hvor det er utarbeidet mål både på kort, mellomlang og lang sikt samt prinsipper.[28].

Etableringen av FST J6, ny IKT-styringsmodell, DRP og ny modell for porteføljestyring, kan medføre endringer i IKT-virksomheten for forsvarssektoren. Det planlegges også med å inngå strategiske partnerskap, noe som også vil påvirke IKT-virksomheten.

1.4 Rapportens tema og avgrensning

Denne rapporten gir noen utvalgte anbefalinger knyttet til IKT-virksomheten og hvordan Forsvaret bør anvende IKT. Utvalget er basert på anbefalinger gitt i studier som allerede er gjennomført av FFI, med hovedvekt på perioden 2020–2022. Naturlig nok er det flere områder innen IKT som ikke er studert av FFI, og anbefalingene i denne rapporten dekker på ingen måte alle aspekter av IKT i Forsvaret.

[24] Forsvarsdepartementet (2020b). Tildelingsbrev for Forsvaret 2021.
[25] IKT-virksomheten er ifølge Forsvarets IKT-strategi «…de personer og organisasjoner som produserer varer, tjenester eller utfører aktivitet innen utvikling, drift, vedlikehold og forvaltning av Forsvarets IKT; være seg Forsvarets og forsvarssektorens egne eller andre offentlige og private.»
[26] Forsvarsstaben. (2022a). *Stående ordre for Forsvarsstaben*, sjef Forsvarsstaben, september 2022.
[27] Forsvarsstaben. (2022b). *IKT-styringsmodell for forsvarssektoren*.
[28] Forsvarsstaben. (2023). *Digital reguleringsplan*. BEGRENSET.

Rapporten er primært skrevet for Forsvarsstabens IKT-avdeling (FST J6), men anbefalingene som er gitt i rapporten vil også være relevante for øvrige beslutningstakere og personell som jobber med investering og strategisk styring av IKT-virksomheten.

1.5 Leseveiledning

Rapporten inneholder fem hovedtema som på forskjellig vis er knyttet til IKT-virksomheten og anvendelsen av IKT i Forsvaret. Hvert tema presenteres i eget kapittel, som avsluttes med en liste over anbefalinger. Rapporten kan leses kronologisk, men det er også mulig å velge de temaene, eller kapitlene, som leseren finner mest interessant og likevel få utbytte av rapporten.

Kapittel 2 omhandler *Kvalitet i beslutningsprosessene*. I dette kapitlet har vi spesielt studert hvordan Forsvaret kan oppnå gjennomgående digital informasjonsdeling gjennom bevisst og målrettet anvendelse av IKT.

Et virkemiddel for å bedre Forsvarets tilgang på teknologi og kompetanse er gjennom *Sourcing og strategisk partnerskap,* som vi behandler i kapittel 3. I dette kapitlet beskriver vi faktorer som bør inngå i forbindelse med sourcing av Forsvarets IKT. Kompetanse er videre behandlet i kapittel 4, *Forsvarssektorens kompetanseutvikling innen IKT-området.* Her omtaler vi de ulike typene av digital kompetanse og strategisk IKT-kompetanse som forsvarssektoren har behov for.

Riktig anvendelse av IKT forutsetter dessuten et forsvarlig sikkerhetsnivå basert på en vurdering av risiko. Kapittel 5 omhandler *Forsvarlig sikkerhetsnivå* der vi presenterer et verdihierarki som utgangspunkt for risikobaserte vurderinger. Kapittel 6 omhandler *Digital grunnmur.* En digital grunnmur er en forutsetning for å oppnå gjennomgående digital informasjonsdeling. Den kan også gjøre det enklere å ta i bruk nye teknologier og kan forenkle ivaretakelse av sikkerheten.

2 Kvalitet i beslutningsprosessene

IKT-strategien for forsvarssektoren hevder at én av årsakene til manglende gevinst fra IKT-investeringer i sektoren er synet på IKT som infrastruktur, heller enn en muliggjører for operativ evne.[29] I stedet for å kun se på IKT som et rasjonaliseringsverktøy og infrastruktur, må det derfor legges vekt på hvordan IKT kan bidra til et operativt fortrinn. For at Forsvaret skal oppnå dette, kreves en systematisk kobling mellom prosess, teknologi og organisasjon. IKT må sees på som en nødvendig, men ikke tilstrekkelig faktor for å oppnå operativt fortrinn. Eksempelvis kan IKT gi Forsvaret bedre tilgang på informasjon, noe som muliggjør at beslutningsprosesser gjennomføres raskere og bedre enn en motstander. Det at IKT muliggjør en slik endring er allikevel ikke tilstrekkelig; operativt fortrinn oppnås først når Forsvaret også gjennomfører nødvendige endringer i tilhørende prosesser og organisasjon.

FFI har, i en studie utgitt i 2022, undersøkt om IKT kan bidra til økt kvalitet i Forsvarets beslutningsprosesser ved å muliggjøre bedre informasjonsdeling. [30] Studien, som dette kapittelet i all hovedsak bygger på, viser at bevisst og målrettet anvendelse av IKT kan bidra til dette. Samtidig viser studien at potensialet for informasjonsdeling gjennom IKT ikke blir utnyttet godt nok, og at IKT alene ikke bidrar til økt kvalitet i beslutningsprosessene. Studien identifiserer fem kritiske suksessfaktorer (KSF) for å oppnå bedret informasjonsdeling i Forsvarets beslutningsprosesser:

- KSF 1, *skape gjennomgående digital informasjonsdeling*, innebærer at informasjon i størst mulig grad deles uten manuelle steg, noe som bidrar til raskere deling og redusert fare for feil.

- KSF 2, *prioritere digital kompetanse*, omhandler initiativ for å sikre god utnyttelse av IKT ved at organisasjonen har digital kompetanse, bestående av digital kunnskap, ferdighet, evner og holdninger.

- KSF 3, *utvikle strategisk IKT-ledelse*, omhandler behovet for tydelighet og enighet om retningen i den videre IKT-utviklingen, inkludert hvilke muligheter IKT gir i dag og også framover for alternative organiseringer og gjennomføringsmodeller.

- KSF 4, *bygge brukeraksept for digitaliseringsprosessene*, omhandler nødvendigheten av å inkludere berørte deler av organisasjonen i endringsprosessene slik at endringene godtas i praksis. Dette er avgjørende for å sikre at IKT blir brukt som tenkt, og dermed oppnå effekt av digitaliseringsprosessene

- KSF 5, *etablere og videreutvikle prinsipper om strukturert fleksibilitet*, vil si at strategisk ledelse setter rammer og en tydelig retning, samtidig som underliggende enheter har fleksibilitet i hvordan tiltak gjennomføres innenfor de gitte rammene.

[29] Forsvarsdepartementet. (2019).
[30] Elstad et al. (2022a).

Rammene må ikke være til hinder for kreativitet, utprøving og muligheten til å lære gjennom å feile.

Merk at disse fem KSF-ene henger tett sammen, og til dels har gjensidig påvirkning på hverandre. De har også det til felles at de representerer faktorer som organisasjonen selv kan påvirke. I tillegg påvirker faktorer utenfor organisasjonens egen kontroll også kvalitet i beslutningsprosesser, eksempelvis lover, regler, bevilgninger, føringer og andre styrende dokumenter fra myndighetene.

Videre i dette kapittelet vil vi gå nærmere inn på utvalgte aspekter fra denne studien. Disse aspektene er valgt fordi de har spesiell relevans og viktighet for de som skal utøve strategisk styring av IKT-utviklingen i Forsvaret.

I tillegg er de nevnte KSF-ene også relevante for resten av rapporten. KSF 1 blir nærmere behandlet i kapittel 6, som omhandler hvordan den digitale grunnmuren kan legge til rette for digital informasjonsdeling. Prioritere digital kompetanse, KSF 2, er tett knyttet til de andre KSF-ene. Temaet behandles derfor både for seg selv i kapittel 4, samtidig som aspekter ved digital kompetanse også omtales i de resterende kapitlene. KSF 3 og KSF 5 omhandler ulike aspekter ved styring av IKT-utviklingen i Forsvaret, og de veivalgene som må gjøres for at Forsvaret skal få bedret utnyttelse av sin IKT. Begge disse KSF-ene er derfor inkludert i hele rapporten. Det samme gjelder for KSF 4, men denne blir også behandlet nedenfor i kapittel 2.2.

2.1 Begrenset rasjonalitet og sporbarhet

En sentral del av beslutningsprosessene er å prioritere ressurser det er knapphet på mellom interessenter med konkurrerende behov. Et eksempel kan være innenfor sourcing[31], hvor interessenter inkluderer både ansatte internt i organisasjonen og eksterne kandidater som helt eller delvis kan levere tjenester. I en beslutningsprosess vil ulike handlingsalternativer[32] vurderes opp mot hverandre for å se hvilket alternativ som gir best operativ effekt ut fra de gitte rammene.

I en ideell verden vil alle beslutninger være fullstendig rasjonelle. Ved rasjonelle beslutninger har beslutningstakerne perfekt kunnskap ved at (1) alle handlingsalternativer er kjent, (2) konsekvenser ved alternativene er kjent og (3) preferanser for valg av handlingsalternativ er kjente, presise, konsistente og stabile. Det vil si at en beslutningstaker tar valg basert på alternativer, forventninger, preferanser og beslutningsregler.

Beslutningstakere kan generelt sett ikke imøtekomme krav til rasjonelle beslutninger. I virkeligheten vil forskjellige grupper av mennesker bruke forskjellige rammeverk for å forenkle verden. Vi har derfor begrenset kapasitet til å kommunisere og dele kompleks informasjon på tvers av

[31] Sourcing er den strategiske beslutningen som skjer i forkant av kjøp av for eksempel tjenester. Se kapittel 3 for flere detaljer.
[32] For en beslutning ligger det ulike løsningsforslag – såkalte handlingsalternativer – til grunn. Et handlingsalternativ inneholder en begrunnelse og redegjørelse, inkludert fordeler og ulemper ved valg av alternativet.

kulturer og fagområder.[33] Dette gjør det desto viktigere å synliggjøre premissene bak ulike handlingsalternativer gjennom sporbarhet i beslutningsprosessen for ulike interessenter. Sporbarhet gjør det mulig å følge (1) stegene i beslutningsprosessen, (2) hvilke kriterier de ulike handlingsalternativene inkluderer og (3) vurderinger for hvert av kriteriene.

Tar vi sourcing som eksempel kan et handlingsalternativ være å sette ut all IKT-drift til en ekstern partner. Et annet handlingsalternativ kan være å beholde all IKT-drift internt. Mellom disse ytterpunktene finnes det en rekke ulike løsninger, som hver utgjør et handlingsalternativ. Det er en utopi at beslutningstakere vil få oversikt over alle konsekvenser av de ulike handlingsalternativene, og det er derfor ikke mulig med en fullt ut rasjonell beslutning om sourcing.[34]

Utarbeidelsene av handlingsalternativene kan aldri bli ideelle, bare tilfredsstillende. Vi anbefaler derfor at beslutninger er sporbare og gjennomsiktige, for å ivareta kvaliteten i beslutningsprosessen. Sporbarhet og gjennomsiktighet krever skriftlighet og åpenhet knyttet til stegene i beslutningsprosessen, inkludert kriterier for valg av handlingsalternativ og hvilke vurderinger som er gjort i forbindelse med hvert handlingsalternativ. En slik tilnærming gir helhetlig dokumentasjon og sporing i prosessen.

2.2 Bygge brukeraksept for digitaliseringsprosessen

Effektiv bruk av IKT er sammensatt og krever at ulike interessegrupper samarbeider, både internt i organisasjonen og eksternt. En kan tenke seg at ulike interessegrupper, eksempelvis FOH og taktiske kommandoer, har ulike forventninger, behov og ikke minst forutsetninger for å håndtere felles IKT på en effektiv måte.

2.2.1 Intendert bruk

Effektiv bruk av IKT krever en helhetlig og målrettet plan eller intensjon om hvordan IKT skal benyttes i en arbeidsprosess – en beskrivelse av såkalt *intendert bruk*. IKT er ofte en forutsetning for gjennomføringen av ulike arbeidsprosesser, og særlig for informasjonsdeling på tvers av prosesser. Derfor anbefaler vi at oversikt over intendert IKT-bruk på et overordnet nivå inkluderes i eksisterende SOP-er[35] og TOR-er[36]. Eksempelvis bør SOP-er klargjøre hvor, hvordan og hvorfor de ulike informasjonsproduktene skal organiseres slik organisasjonen har valgt. Det skal legges til at vi ikke ser for oss en detaljert beskrivelse av selve IKT-bruken, men av obligatoriske IKT-tiltak brukeren må gjøre. Mangel på en slik beskrivelse kan potensielt utgjøre et hinder for informasjonsdeling.

Beskrivelse av intendert IKT-bruk vil også være med på å systematisere, sette retning og gi rammer for organisasjonens utnyttelse av IKT. Samtidig er det behov for fleksibilitet til å benytte IKT innenfor de gitte rammene. For dårlige beskrivelser og potensielt uklare rammer

[33] March, J. (1994). *Primer on Decision Making: How Decisions Happen*. Simon and Schuster.
[34] Elstad, A. K., Endregard, M., Mykkeltveit, A. (2022b). Sourcing for forsvarssektorens IKT-virksomhet – skisse til rammeverk. (FFI-rapport 22/02237). Forsvarets forskningsinstitutt.
[35] *Standard Operating Procedures* (SOP).
[36] *Terms Of Reference* (TOR).

kan føre til at Forsvaret ikke har en helhetlig og omforent bruk av IKT. IKT-anvendelsen kan i sin tur bli opp til den enkelte bruker. På den annen side vil en for detaljert beskrivelse av intendert bruk være et hinder ved at stramme rammer fører til at kreativitet og initiativ kan bli redusert. Vi anbefaler derfor å finne en balanse mellom struktur og fleksibilitet – såkalt strukturert fleksibilitet.

2.2.2 Håndtering av endring

Selv med veldefinert intendert bruk kan ulike faktorer påvirke om brukerne faktisk vil akseptere og gjennomføre arbeidsprosessen som intendert. Et enkelt eksempel kan være at brukeren skal gå fra å lagre dokumenter i en filstruktur til å lagre dem i SharePoint. Om brukeren aksepterer denne endringsprosessen eller ikke vil direkte eller indirekte avhenge av faktorer som intensjon om bruk, tilretteleggende forhold, oppfattet nytte, oppfattet brukervennlighet og sosial påvirkning.[37,38,39] Ulike typer karakteristikker ved informasjon og systemer, som informasjonskvalitet og systemkvalitet, er andre eksempler på slike faktorer.[40]

Ved innføringen av for eksempel obligatoriske IKT-tiltak, endring i IKT-styring og inngåelse av strategiske partnerskap kan motstand oppstå i organisasjonen. Denne motstanden mot endring kan sees på gjennom to faser. Den første fasen omhandler den kognitive og følelsesmessige fasen som resulterer i beslutningen om motstand. Den andre fasen er selve motstandsatferden.[41]

Et tiltak for å hindre motstand mot endring er å sørge for forankring i organisasjonen. Involvering og deltakelse er identifisert som kritiske suksessfaktorer i ulike former for endringsprosesser,[42] og vi anbefaler at de som påvirkes av endringen inkluderes i arbeidet. Effektiv kommunikasjon er en annen kritisk suksessfaktor i endringsprosesser,[43] noe som innebærer å etablere en historie som forteller om fordelene og intensjonen bak de endringene som skjer.

Et eksempel på en endringsprosess kan være inngåelse av strategiske partnerskap. Aktiviteter som tidligere ble gjennomført internt i forsvarssektorens IKT-virksomhet, vil kunne bli helt eller delvis overtatt av en ekstern virksomhet, en strategisk partner. Dette kan i sin tur føre til strukturelle endringer, ved at enkelte deler av organisasjonen blir overflødig. En annen konsekvens kan være endringer i prosesser fordi tjenester helt eller delvis flyttes ut av virksomheten. For eksempel kan det etableres nye samarbeidskonstellasjoner og mekanismer for informasjonsdeling.

[37] Davis, F. D. (1989). *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. MIS Quarterly, 13(3), 318–340.
[38] Venkatesh, V., Morris, M. G., Davis, G. B., Davis, F. D. (2003). *User acceptance of information technology: toward a unified view*. *MIS Quarterly*, 27(3), 425–478.
[39] For flere detaljer, se f.eks. Elstad et al. (2022a).
[40] DeLone, W. H., McLean, E. R. (2003). *The DeLone and McLean Model of Information Systems Success: A Ten-Year Update*. Journal of Management Information Systems, 19(4), 9–30.
[41] Ferneley, E. H., Sobreperez, P. (2006). *Resist, comply or workaround? An examination of different facets of user engagement with information systems*. European Journal of Information Systems, 15(4), 345–356.
[42] Elstad et al. (2022a).
[43] Ibid.

Det bør gjøres en forankringsjobb for å etablere aksept når slike endringer gjennomføres i IKT-virksomheten. En del av forankringsjobben er å formidle fordelene og intensjonen bak endringene som skjer. Budskapet fra forsvarsledelsen må være omforent og begreper og intensjonen bak valg som er gjort i beslutningen må forklares. Dette henger også sammen med sporbarhet, som beskrevet i kapittel 2.1.

2.3 Anbefalinger

Basert på de foregående delkapitlene har vi følgende råd og anbefalinger:

Kvalitet i beslutningsprosessene – anbefalinger

- Beslutninger knyttet til utviklingen av IKT-området bør være sporbare og gjennomsiktige for å ivareta kvaliteten i beslutningsprosessen.
- Intendert IKT-bruk på et overordnet nivå bør inkluderes i eksisterende prosessbeskrivelser, som for eksempel SOP-er og TOR-er. En SOP bør inneholde hvor, hvordan informasjonsproduktene skal organiseres, samt intensjonen bak denne organiseringen.
- Det bør i størst mulig grad styres etter prinsipper om strukturert fleksibilitet, ved å etablere en balanse mellom autonomi og rammer i gjennomføringen.

3 Sourcing og strategisk partnerskap

Sourcing er den strategiske beslutningen som skjer i forkant av kjøp av for eksempel tjenester. Beslutningen baseres på ulike handlingsalternativer. Eksempelvis kan overordnede handlingsalternativer være intern utførelse av tjenesten, at tjenesten leveres som et tjenestekjøp (transaksjonsbasert), samarbeid med ekstern virksomhet (samarbeidsbasert) og eliminere aktivitet.[44]

Forsvaret arbeider nå med inngåelse av strategisk partnerskap, hvor disse vurderingene inngår. Strategisk partnerskap eksisterer når to eller flere uavhengige organisasjoner samarbeider om utvikling, produksjon eller salg av produkter og tjenester.[45] Strategisk partnerskap kan potensielt ha positiv innvirkning på Forsvaret gjennom kostnadsreduksjon, bedre bruk av menneskelig kapital og bedre tilgang til ny teknologi.[46] På den annen side kan Forsvaret potensielt miste kvalifisert personell og få redusert kontroll og fleksibilitet innenfor sin IKT-portefølje.[47]

FFI har støttet FST J6 sitt arbeid i forbindelse med sourcing, ved å utvikle skisse til rammeverk for sourcing av forsvarssektorens IKT-virksomhet.[48] Rammeverket er en utvidelse av «modell for valg av sourcingstrategi»[49] som også er utviklet av FFI. Rammeverket foreslår syv faktorer som bør inngå i forbindelse med sourcing av Forsvarets IKT. Disse faktorene er: operativt fortrinn, forsvarlig sikkerhetsnivå, krigens folkerett, transaksjonskostnader, kompetanse, begrenset rasjonalitet og risiko for opportunisme. Dette kapittelet tar for seg fire av disse faktorene overordnet (kapittel 3.1–3.5). Faktoren begrenset rasjonalitet blir i hovedsak behandlet i kapittel 2, og faktorene kompetanse og forsvarlig sikkerhetsnivå i henholdsvis kapittel 4 og 5. Vi anbefaler at Forsvaret utvikler og vedlikeholder en sourcing-strategi for IKT som tar hensyn til disse faktorene.

3.1 Operativt fortrinn

Den første faktoren i det nevnte rammeverket er operativt fortrinn. I sammenheng med sourcing og strategisk partnerskap blir spørsmålet om Forsvaret får et operativt fortrinn ved å gjennomføre ulike aktiviteter knyttet til IKT-virksomheten internt i Forsvaret eller om det bør gjøres i samarbeid med eller av strategisk partner eller eksterne leverandører. Denne problemstillingen er kompleks, og vil i hvert tilfelle kreve grundige og helhetlige analyser og vurderinger, inkludert drøftinger av følgende spørsmål:[50]

[44] Direktoratet for forvaltning og økonomistyring (DFØ). Anskaffelser.no. Fagsider om offentlige anskaffelser. https://www.anskaffelser.no.
[45] Barney, J. (2002).
[46] Earl, M. J. (1996). *The Risks of Outsourcing IT*. Sloan Management Review, 37(3), 26–32.; Elstad et al. (2022b).
[47] Jae-Nam, L., Huynh, M. Q., Ron Chi-Wai, K., Shih-Ming, P. (2003). *IT Outsourcing Evolution--Past, Present, and Future.* Communications of the ACM, 46(5), 84–89.
[48] Elstad et al. (2022b).
[49] Pedersen, O. B. (2022). *Bør vi samarbeide? – en litteraturstudie om valg av sourcingstrategi* (FFI-rapport 22/01384). Forsvarets forskningsinstitutt.
[50] Se Elstad et al. (2022b) og Pedersen (2022) for flere detaljer.

- Er det lettere å reagere på muligheter og trusler fra omgivelsene dersom en aktivitet utføres med interne ressurser framfor eksterne ressurser?

- Blir IKT-en mer robust, og får den bedre ytelse ved at aktiviteten utføres av interne i stedet for av eksterne ressurser?

- Er det slik at ressursen(e) som er nødvendige for å gjennomføre aktiviteten er kontrollert av et lavt antall konkurrerende organisasjoner?

- Er Forsvaret, gjennom strategier og prosedyrer, i stand til å utnytte den verdifulle, sjeldne, ikke imiterbare kapabiliteten eller ressursen – ved at aktiviteten utføres internt?

3.2 Krigens folkerett

Innrettingen av IKT-virksomheten og valg av sourcingstrategi må være i henhold til gjeldende lov og rett i hele krisespekteret. Den påfølgende korte teksten oppsummerer vurderinger og anbefalinger fra Elstad et al. (2022b), men uten de nyanser som er fremhevet der.

I væpnet konflikt og krig kommer krigens folkerett til anvendelse. Folkeretten er den rett som gjelder mellom stater, og den delen av folkeretten som kalles krigens folkerett eller internasjonal humanitærrett regulerer væpnet konflikt.[51] «Krigens folkerett bygger på prinsippene om distinksjon mellom sivile og stridende, militær nødvendighet, humanitet og proporsjonalitet.»[52] *Distinksjonsprinsippe*t forplikter de krigførende partene kun å angripe lovlige mål, det vil si stridende personer og militære objekter, mens sivile personer og objekter skal beskyttes og respekteres.[53] «Det er tillatt å rette angrep mot lovlige mål selv om dette medfører sivil følgeskade, men det er forbudt å iverksette angrep som må antas å forårsake overdreven sivil følgeskade (proporsjonalitetsprinsippet).»[54]

I henhold til langtidsplanen for forsvarssektoren skal planlegging for sivil støtte i væpnet konflikt være i henhold til krigens folkerett.[55] Sivil støtte omfatter både støtte fra offentlige myndigheter og støtte fra kommersielle sivile aktører gjennom leveranser av varer, tjenester og infrastruktur. Ved inngåelse av strategisk partnerskap eller andre typer samarbeid med sivile virksomheter innen IKT-virksomheten, må Forsvaret derfor vurdere hva som skal til for å ivareta krigens folkerett. Videre må Forsvaret sørge for at de funksjoner sivile aktører forutsettes å utføre i væpnet konflikt, er i henhold til krigens folkerett.

Ved sourcing innen IKT-virksomheten må det gjøres konkrete vurderinger knyttet til krigens folkerett fra sak til sak, da det i liten grad er mulig å trekke generelle konklusjoner. Hva leverandører skal levere til, og utføre for, Forsvaret av IKT-systemer og -tjenester, utvikles

[51] Johansen, S. R. (2019). *«Nød kjenner ingen rett»? Totalforsvar, beredskapsrett og folkerett*; I P. M. Norheim-Martinsen (Red.). *Det nye totalforsvaret* (s. 117–133). Gyldendal, s. 125.
[52] Forsvarsdepartementet. (2020a), s. 80.
[53] Forsvarssjefen (2013). *Manual i krigens folkerett*. Forsvaret, s. 13.
[54] Ibid., s. 14.
[55] Forsvarsdepartementet. (2020a), s. 80.

gjerne gjennom en lengre dialog- og forhandlingsprosess mellom partene. Dette betyr at de folkerettslige vurderingene må inngå i hele prosessen og oppdateres etter hvert som mer detaljer kommer på plass. For å sikre at Forsvaret til enhver tid ivaretar krigens folkerett, betyr det at følgende vurderinger må utføres og dokumenteres som ledd i sourcingprosessen, ved kontraktsinngåelse og i hele leveranseløpet:

- Forsvaret må konkretisere hvilke funksjoner innen IKT-virksomheten som utgjør *direkte deltakelse i fiendtlighetene*. Dette gjelder både funksjoner i cyberdomenet som krigføringsdomene og de funksjonene som innebærer annen direkte støtte til militære operasjoner. Det kan for eksempel være leveranse av kommunikasjonsmidler for å understøtte kommando og kontroll i et stridsområde eller drift av systemer som prosesserer og overfører sensordata som direkte bidrar til kommando- og kontrollfunksjoner ved Forsvarets hovedkvarter. I væpnet konflikt kan slike funksjoner i henhold til nasjonale bestemmelser kun utføres av militært personell.

- Forsvaret må identifisere hvilke funksjoner innen IKT-virksomheten som innebærer *indirekte støtte til krigføringen*, og dermed ikke er å anse som en del av fiendtlighetene. Dette betyr å identifisere hva sivile leverandører kan utføre, uten å utfordre krigens folkerett og nasjonale bestemmelser. Et eksempel er utvikling og leveranse av IKT til bruk i Forsvaret, men der sivil part ikke selv benytter slike systemer. Et annet eksempel på dette kan muligens være generell understøttelse ved leveranser og vedlikehold knyttet til rent administrative IKT-systemer.

- Forsvaret må utføre *risikovurderinger for sivil følgeskade* som ledd i sourcing for å holde denne risikoen så lav som mulig. Dette aspektet kan påvirke innretningen av sourcingmodeller og føre til iverksetting av tiltak.

- Forsvaret må vurdere hvilke *samfunnsmessige konsekvenser* sourcing har for kritiske samfunnsfunksjoner og sivilbefolkningen, slik at det sørges for at måten Forsvaret innretter seg på ikke motvirker en motparts evne eller vilje til å beskytte sivile personer og sivile funksjoner i det norske samfunnet.

3.3 Transaksjonskostnader

Når Forsvaret gjennomfører en prosess eller tjeneste internt forekommer ikke transaksjonskostnader, siden kostnadene ved en intern produksjon er knyttet til produksjonskostnader.[56] Ved inngåelse av strategisk partnerskap vil imidlertid en rekke transaksjonskostnader oppstå, både i forkant og i etterkant av kontraktinngåelse.[57] Transaksjonskostnader vil si «alle kostnader for-

[56] Elstad et al. (2022b).
[57] Pedersen (2022).

bundet med å organisere og gjennomføre en bestemt transaksjon eller handel». Transaksjonskostnader som oppstår i etterkant av en kontraktsinngåelse vil være oppfølging av leverandører og strategisk partner, i tillegg til en rekke koordinerings- og omstillingskostnader.[58]

Det er spesielt tre aspekter som er kritiske ved en transaksjon: (1) usikkerhet, (2) frekvens og hyppighet samt (3) graden av transaksjonsspesifikke investeringer.[59] Usikkerhet vil være knyttet til flere aspekter, blant annet til hvor raskt den teknologiske utviklingen vil gå innenfor den aktuelle tjenesten som skal vurderes utført med interne ressurser, eller om hele eller deler av tjenesten skal leveres som et tjenestekjøp, eller ved samarbeid med ekstern virksomhet. Det er også en økende grad av kompleksitet med tanke på digitale verdikjeder, og hvem som eier, vedlikeholder og opererer de forskjellige delene. Hvor spesifikt en tjeneste er laget for en spesiell anvendelse må også vurderes.

En vurdering som også må gjøres i sammenheng med transaksjonskostnader er om det er behov for strukturelle og prosessuelle endringer i organisasjonen ved en inngåelse av strategisk partnerskap, inkludert en vurdering av hvilke koordinerings- og omstillingskostnader det kan antas at inngår i en eventuell endring. Kompetanse bør også inkluderes i disse vurderingene, spesielt med tanke på kompetanseoverføring til strategisk partner. Dersom det er kompetanseoverføring, hvilken fare vil det ha for tap av den kompetansen man ønsker å beholde internt (ved at kompetansemiljøet i egen organisasjon svekkes).

Forsvaret bør ved inngåelse av et strategisk partnerskap lage en oversikt over de transaksjonskostnader som partnerskapet medfører og oppdatere denne gjennom hele prosessen.

3.4 Risiko for opportunisme

Risiko for opportunisme er en av atferdsmekanismene som inkluderes i vårt forslag til rammeverk. Ved inngåelse av strategisk partnerskap må Forsvaret være klar over muligheten for opportunisme. Opportunisme eksisterer når en av partene i en transaksjon utnytter sårbarhetene til transaksjonspartneren,[60] eksempelvis manglende kompetanse, oversikt, personell med mer. Ved opportunisme handler aktørene ut fra egen interesse framfor å ta hensyn til transaksjonspartnerens interesser. Eksempelvis kan det være at den strategiske partneren vil selge Forsvaret en tjeneste for egen vinning, som Forsvaret ikke har behov for eller som ikke er tilpasset Forsvarets behov.

Når antall kilder til mulig opportunistisk atferd ikke er kjent på forhånd, blir trusselen fra opportunistisk atferd større enn om alle kilder er forhåndskjent. Det vil si at når nivået av usikkerhet

[58] Elstad et al. (2022b).
[59] Williamson, O. E. (1979). *Transaction-cost economics: the governance of contractual relations*. The journal of Law and Economics, 22(2), 233–261.
[60] Barney (2002).

og kompleksitet i en transaksjon er stor, er risikoen for opportunisme også stor.[61] De ulike forhandlingspartene vil ha ulike syn på, og ulike tiltak for å imøtekomme risikoen og dette bør bevisstgjøres i prosessen.

Risikoen for opportunisme vil reduseres når partene vil oppfatte at en opportunistisk atferd er for kostbar.[62] For å unngå opportunistisk atferd fra en av kontraktspartene, er det behov for at det eksisterer en gjensidig avhengighet mellom dem – en maktbalanse. Et tett samarbeid mellom partene kan være et initiativ for å få best mulig kontroll på transaksjonen, og gjennom dette håndtere potensielle muligheter for opportunisme.[63]

Risikoen for opportunisme er reell ved inngåelse av et strategisk partnerskap. Vi anbefaler derfor at Forsvaret er bevisst muligheten for opportunistisk atferd, også etter at det strategiske partnerskapet er inngått. Det er derfor behov for at Forsvaret har tilstrekkelig digital kompetanse til å oppfatte dersom den strategiske partneren viser tendens til opportunistisk atferd.[64] Forsvaret må også inneha kompetanse til å formulere behov, slik at den strategiske partneren evner å forstå bestillingen.[65]

Sporbarhet og gjennomsiktighet i sourcing er sentralt for å synliggjøre premissene mellom partene som inngår i beslutningen, altså Forsvaret og strategisk partner. Ved en strategisk beslutning som sourcing vil et omforent rammeverk for helhetlig dokumentasjon og sporing i prosessen være sentralt, for å bidra til å redusere risiko for misforståelser, konflikt og reforhandling.

Samtidig vil sporbarhet internt i Forsvaret også være av betydning, siden inngåelse av strategisk partnerskap medfører endringer internt ved at hele eller deler av tjenesten leveres som et tjenestekjøp eller i samarbeid med ekstern virksomhet. Sett i sammenheng med begrenset rasjonalitet, som vi var inne på i kapittel 2.1, kan sporbarhet og gjennomsiktighet i utarbeidelsen av handlingsalternativene bidra til at de ulike interessentene potensielt kan oppnå en forståelse for hvilke kriterier som ligger til grunn for prioriteringer som gjøres. Videre vil en inngåelse av strategisk partnerskap få følger for Forsvarets IKT-styringsmodell. Tjenester som tidligere ble gjennomført internt i organisasjonen vil nå helt eller delvis gjennomføres av en strategisk partner. En slik endring vil få konsekvenser for Forsvaret, ved en endring i roller, ansvar og myndighet i IKT-virksomheten internt i Forsvaret og i grensegangen opp mot strategisk partner.

[61] Ibid.
[62] Barney (2002).
[63] Pedersen (2022).
[64] Vi kommer tilbake til digital kompetanse i kapittel 4.
[65] Elstad et al. (2022b).

3.5 Anbefalinger

I de foregående delkapitlene har vi diskutert momenter knyttet til sourcing og strategisk partnerskap som vi ser er av betydning for Forsvarets arbeid med styring av IKT-virksomheten. Basert på de foregående delkapitlene har vi følgende råd og anbefalinger:

Sourcing og strategisk partnerskap – anbefalinger

- Forsvaret bør ha en systematisk og kontinuerlig prosess for å utvikle og vedlikeholde en sourcing-strategi som tar hensyn til faktorene operativt fortrinn, forsvarlig sikkerhetsnivå, transaksjonskostnader, kompetanse, begrenset rasjonalitet og risiko for opportunisme. Implikasjoner for krigens folkerett bør også være én sentral faktor i strategien og inkluderer konkrete vurderinger for sivile aktørers planlagte bidrag til Forsvarets operative evner i væpnet konflikt.

- Forsvaret bør ved inngåelse av et strategisk partnerskap lage en oversikt over de transaksjonskostnader som partnerskapet medfører og oppdatere denne underveis. Oversikten må tydelig avdekke roller, ansvar og myndighet. FST bør eie denne oversikten, men selve oppfølgingen bør skje delegert i Forsvaret og forsvarssektoren forøvrig.

4 Forsvarssektorens kompetanseutvikling innen IKT-området

Tilgang på tilstrekkelig personell med relevant kompetanse er en nødvendig faktor som bidrar både direkte og indirekte til å sikre IKT-virksomhetens leveranseevne i krisespekteret.[66,67]

4.1 Hva er digital kompetanse?

I følge Lai består kompetansebegrepet av dimensjonene kunnskap, ferdigheter, evner og holdninger.[68] *Digital kunnskap* vil si at en person innehar teoretisk innsikt og forståelse opparbeidet gjennom opplæring og erfaring. De *digitale ferdighetene* handler om selve gjennomføringen – altså det å sette de teoretiske kunnskapene ut i praksis. Grunnleggende bruk av tekstbehandlingsverktøy, presentasjonsverktøy, e-post og så videre er eksempler på elementære digitale ferdigheter. *Digitale evner* handler om det å ha personlige egenskaper og talent til å benytte IKT, og noen mennesker kan ha bedre forutsetninger for dette enn andre. Dette er imidlertid en dimensjon ved digital kompetanse vi ikke berører nærmere i denne rapporten.

Vi velger å inkludere *holdninger* som en del av digital kompetanse. Sentralt i holdninger er en persons tanker og følelser. I ulike atferdsteorier argumenteres det med at holdninger leder til atferdsvalg,[69] og det er nettopp av denne grunnen vi velger å inkludere holdninger som en del av den digitale kompetansen. Hvilket atferdsvalg som tas kan derfor være ledet ut fra en persons holdninger. Dette kan være alt fra et atferdsvalg om å lagre et dokument i en filstruktur til holdninger til strategisk partner innen IKT. Personens ansvars- og lojalitetsfølelse er også en del av holdninger – og kan knyttes til begrenset rasjonalitet og risiko for opportunisme som nevnt tidligere i rapporten (i kapittel 2.1 og 3.4).

4.2 Digital kompetanse – avhengig av rolle

Hvilken digital kompetanse en person bør inneha vil variere avhengig av hvilken rolle vedkommende har i forsvarssektoren. En driftsansvarlig vil ha behov for en type digital kompetanse, mens en person som er innkjøpsansvarlig vil ha behov for en annen. I dette kapittelet deler vi inn den digitale kompetansen i de tre kategoriene sluttbrukerkompetanse, driftskompetanse og strategisk IKT-kompetanse. Ettersom denne rapporten primært gir anbefalinger om IKT på strategisk nivå, legger vi mest vekt på den strategiske IKT-kompetansen i det følgende.

[66] Birkemo, G. A., Kristiansen, P., Farsund, B. (2021). *Risiko ved strategisk samarbeid innen IKT – rammeverk og vurdering*. (FFI-rapport 21/00527). Forsvarets forskningsinstitutt.
[67] Svendsen-utvalget. (2020). *Økt evne til å kombinere menneske og teknologi – Veier mot et høyteknologisk forsvar* (Svendsen-utvalget, 24. juni 2020). www.regjeringen.no.
[68] Lai, L. (2011). *Kompetansemobilisering og egenmotivasjon*. Magma, 3, 50–55; Lai, L. (2013). *Strategisk kompetanseledelse* (3. utgave.). Fagbokforlaget.
[69] Davis, F. D., Bagozzi, R. P., Warshaw, P. R. (1989). *User Acceptance of Computer Technology: A Comparison of Two Theoretical Models.* Management Science, 35(8), 982–1003; Fishbein, M., Ajzen, I. (1975). *Belief, attitude, intention and behavior: an introduction to theory and research*. Addison-Wesley; Ilie, V., Turel, O. (2020).

4.2.1 Sluttbrukerkompetanse

Forsvaret har gjennomgående behov for det som kalles *sluttbrukerkompetanse*. Rollen innehas gjerne av ulike brukere som vanligvis har andre fagfelt enn IKT som spesialisering, men som benytter IKT-verktøy innenfor sitt fagfelt og derfor må kunne anvende disse verktøyene. Den digitale sluttbrukerkompetansen omhandler imidlertid mer enn bare grunnleggende kunnskap. Ferdigheter til å anvende forskjellige IKT-verktøy for å overføre informasjon til flere mottakere og sikre at meningen med informasjonen er effektivt uttrykt, er også en del av den digitale kompetansen.[70] Samarbeid gjennom bruk av IKT til å utvikle sosiale nettverk og samarbeid i team for å utveksle informasjon, forhandle og gjennomføre beslutninger med gjensidig respekt for hverandre for å oppnå et mål, inkluderes også i sluttbrukerkompetanse.[71]

4.2.2 Driftskompetanse

Driftskompetanse er her brukt som en samlebetegnelse og handler overordnet om kompetanse innen områder som utvikling, installasjon, drift og vedlikehold. Rollen innehas av eksperter, gjerne med utdanning innen IKT. Driftskompetanse inkluderer også forståelse av den teknologiske utviklingen – sett i sammenheng med Forsvarets behov. Eksempler på spørsmål en slik type rolle bør kunne besvare er: (1) Hvordan nye teknologiske løsninger, som for eksempel automatisering, kan integreres i eksisterende løsninger eller skape nye muligheter. (2) Hvilke egenskaper og løsninger kreves innen IKT og er det eventuelt nødvendig med noen IKT-endringer? Og (3) hvilke teknologiske konsekvenser får ulike veivalg? Driftskompetanse er nødvendig i Forsvaret, men ikke tilstrekkelig for å kunne svare på denne typen spørsmål.

Denne rollen vil også være en rådgiver for de som skal ta de strategiske veivalgene, men som ikke har den tekniske dybdekompetansen på samme måte som de som er i denne rollen. Det vil si at Forsvaret vil være avhengig av å ha noe slik digital kompetanse for å gi råd om strategiske veivalg, i tillegg til at denne typen digital kompetanse kan bidra til opprettholdelse av daglig drift, vedlikehold og utvikling. Likevel er ikke driftskompetanse alene nok for Forsvaret til å oppnå organisatorisk effektivitet.

4.2.3 Strategisk IKT-kompetanse

Strategisk IKT-kompetanse vil si hvordan Forsvaret, gjennom ledelsen, innretter seg for å oppnå økt organisatorisk effektivitet ved å utnytte IKT. De rollene som skal inneha strategisk IKT-kompetanse er på topp- og mellomledernivå. Det er naturlig at FST J6 innehar strategisk IKT-kompetanse, men samtidig er det også nødvendig at de ulike driftsenhetene i Forsvaret og etatene i forsvarssektoren har denne type kompetanse.[72]

Strategisk IKT-kompetanse handler med andre ord om helhetsforståelse for IKTs rolle i Forsvaret, eksempelvis hvordan og innenfor hvilke rammer ledelsen ønsker å utvikle Forsvaret.

[70] Van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., de Haan, J. (2017). *The relation between 21st-century skills and digital skills: A systematic literature review.* Computers in Human Behavior, 72, 577–588.
[71] Ibid.
[72] Avsnittet er hentet fra Elstad et al. (2022a).

Et eksempel på strategisk IKT-kompetanse er kunnskap og forståelse for hvordan Forsvaret skal tilnærme seg interoperabilitet og automatisering av beslutningsprosesser. Det handler dermed både om prosessene IKT-en er integrert i, og brukerne som skal utnytte potensialet til IKT-en som Forsvaret innehar.

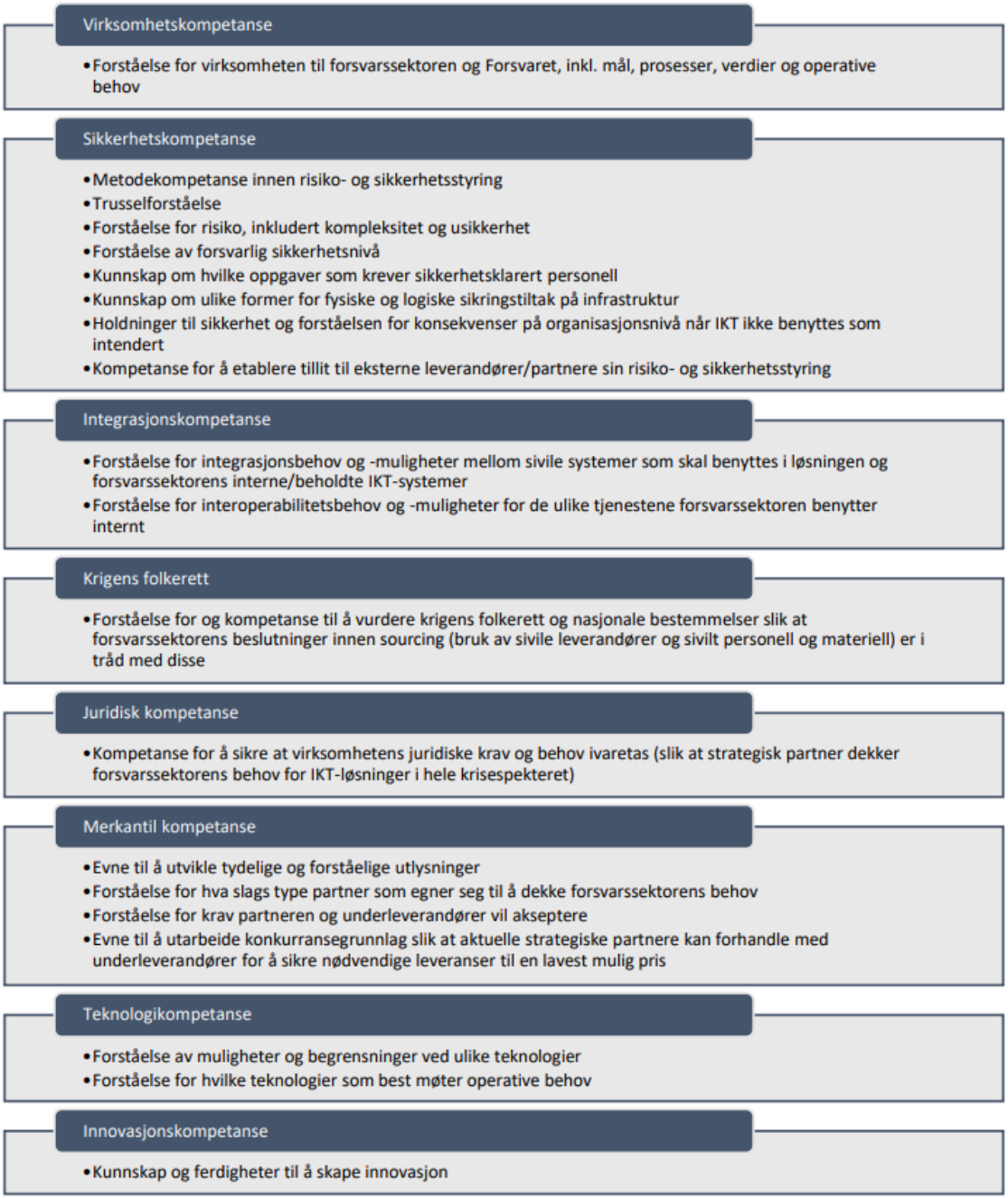
Med ny modell for styring av IKT-porteføljen i Forsvaret vil, etter hva vi forstår, behovseierne, altså de som benytter IKT-en i sine arbeidsprosesser formulere prosessrelaterte, snarere enn tekniske behov – hvilken prosess er det jeg egentlig trenger for å utføre denne oppgaven? Dette vil potensielt kreve en omstilling i tankesett, og kanskje også i *hvem* som formulerer behovene.

En sentral del av den strategiske IKT-kompetansen er å forstå hvilken teknologi som dekker hvilke behov og som utfører hvilke oppgaver, inkludert fordeler og ulemper ved de forskjellige teknologiene. Det betyr at når et operativt behov, som er formulert av en behovseier, skal omformes til konkrete tiltak må behovseier, leveranseorganisasjon og personell med strategisk IKT-kompetanse i fellesskap finne ut hva som er den beste måten å møte behovet på.

Sikkerhet og forståelsen av hva som er forsvarlig sikkerhetsnivå inngår også i den strategiske IKT-kompetansen. Dette inkluderer å sørge for at organisasjonen er bevisst hvilke konsekvenser ikke-intendert bruk av IKT kan få på organisasjonsnivå, eksempelvis uautorisert tilgang til informasjon. Vi kommer nærmere tilbake til forsvarlig sikkerhetsnivå i kapittel 5.

Figur 4.1 viser en oversikt over ulike deler av strategisk IKT-kompetanse Forsvaret har behov for.[73] Det er ikke slik at én person skal inneha alle disse formene for strategisk IKT-kompetanse, men det er en nødvendighet at et tverrfaglig team, eksempelvis FST J6, til sammen innehar denne kompetansen. «God tverrfaglig kompetanse i IKT-virksomheten er den viktigste faktoren som vil kunne bidra til mer presise risikovurderinger og dermed mindre usikre og bedre beslutningsgrunnlag.»[74]

[73] Merk at ikke alle kompetansetypene som vises i figuren er omtalt i denne rapporten. For flere detaljer rundt strategisk IKT-kompetanse henviser vi til Elstad et al (2022b) og Birkemo et al. (2021).
[74] Birkemo et al. (2021).



Figur 4.1 Strategisk IKT-kompetanse (jf. Elstad et al. (2022b).)

Som vi har sett i dette kapitlet er det behov for flere typer IKT-kompetanse i Forsvaret. Hvilken kompetanse det er størst behov for i fremtiden, vil kunne endre seg basert på de handlingsalternativ Forsvaret velger for sourcing og strategisk partnerskap. Det kan for eksempel være behov for en annen form for strategisk IKT-kompetanse, med for eksempel mer vekt på juridisk og merkantil kompetanse, dersom Forsvaret øker avhengigheten til strategiske partnere. Som vi var inne på i kapittel 2 må Forsvarets ivaretakelse av krigens folkerett være en faktor ved valg av sourcing. Slike vurderinger kan også ha betydning for hvilken kompetanse Forsvaret må ha

selv. Det å beholde og videreutvikle den kritiske IKT-kompetansen i Forsvaret er vesentlig for at IKT-virksomhetens leveranseevne og Forsvarets operative evne opprettholdes i hele krise-spekteret. Det bør derfor utvikles en strategi for å rekruttere og beholde kritisk IKT-personell som er i tråd med de beslutningene som tas i knyttet til sourcing og strategisk partnerskap. Betydningen at riktig IKT-kompetanse bør også tydeliggjøres i de ulike IKT-strategier og IKT-planer som anvendes i forsvarssektoren.

4.3 Anbefalinger

Basert på de foregående delkapitlene har vi følgende råd og anbefalinger:

Forsvarssektorens kompetanseutvikling innen IKT-området – anbefalinger

- Det bør utvikles en strategi for å rekruttere og beholde kritisk IKT-personell i Forsvaret. Digital kompetanse bør også være et sentralt tema i øvrige IKT-strategier og IKT-planer i forsvarssektoren.
- Ved inngåelse av strategisk partnerskap bør Forsvaret utarbeide en strategi som tydeliggjør hva slags IKT-kompetanse sektoren må ha selv. Den bør inkludere hvordan forsvarlig sikkerhetsnivå og folkerett skal ivaretas.
- Forsvaret bør videreutvikle sin sluttbrukerkompetanse, driftskompetanse og kompetanse innen strategisk IKT. Planer bør inneholde konkrete tiltak. Det må inkluderes mål om økt kunnskap om teknologiske muligheter samt holdninger og bevissthet knyttet til IKT.

5 Forsvarlig sikkerhetsnivå

Forsvarets primære oppgave er å ivareta nasjonale sikkerhetsinteresser, det vil si norsk suverenitet, territorielle integritet og demokratiske styreform. Forsvarets IKT-strategi sier at «IKT er uunnværlig for at Forsvaret skal kunne gjennomføre sine operasjoner på en effektiv og sikker måte.»[75] Sikkerhetsloven[76] setter krav til at Forsvaret skal ivareta et *forsvarlig sikkerhetsnivå* for sin virksomhet i krig, krise og fred, herunder IKT-virksomheten. Det forebyggende sikkerhetsarbeidet skal sørge for at Forsvarets IKT-systemer er beskyttet mot inntrengning og skade slik at IKT-systemenes tilgjengelighet, integritet og konfidensialitet er ivaretatt. Som presisert i Forsvarets IKT-strategi, skal forsvarlig sikkerhetsnivå baseres på vurdering av risiko for Forsvarets operative evne og verdier.[77] Videre skal sikkerhetstiltak balansere risiko, effekt og kostnad.[78]

FST J6 har etablert et styringsområde for *sikkerhet,* der IKT sikkerhetsstyring er en integrert del av den strategiske styringen av forsvarssektorens IKT.[79] FFI støtter FST J6 sitt arbeid på sikkerhetsområdet, blant annet ved å utvikle et forslag til rammeverk for risikobaserte vurderinger for Forsvarets bruk av IKT.[80] Forsvarlig sikkerhetsnivå inngår også som en sentral faktor som må vurderes ved sourcing innen IKT-virksomheten.[81] De råd som fremkommer i dette kapitlet bygger på disse to forskningsrapportene.

5.1 Sikkerhetslovens bestemmelser

Sikkerhetsloven, som trådte i kraft 1. januar 2019, legger til grunn en funksjons- og risikobasert systematikk for det forebyggende sikkerhetsarbeidet. Sikkerhetsloven og virksomhetsikkerhetsforskriften[82] setter krav til virksomhetenes evne til sikkerhetsstyring. Virksomhetens leder har ansvaret, og det forebyggende sikkerhetsarbeidet skal være en del av virksomhetens styringssystem (sikkerhetsloven § 4-1). Virksomheten skal regelmessig gjennomføre og dokumentere vurdering av risiko og iverksette de sikkerhetstiltakene som er nødvendige for å gi et forsvarlig sikkerhetsnivå (sikkerhetsloven §§ 4-2, 4-3 og 4-4).

[75] Forsvarsstaben (2021), s. 4.
[76] Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven).
[77] Forsvarsstaben (2021), s. 8.
[78] Ibid, s. 9.
[79] Forsvarsstaben (2022b). *IKT-styringsmodell for forsvarssektoren*.
[80] Endregard, M., Nystuen, K. O., Farsund, B. H., Elstad, A. K. (2023). *Forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT – en innledende studie*. (FFI-rapport 23/00600). Forsvarets forskningsinstitutt. *Under arbeid.*
[81] Elstad et al. (2022b).
[82] Forskrift 20. desember 2018 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften).

I forarbeidene til sikkerhetsloven påpeker Forsvarsdepartementet (FD) at forsvarlig sikkerhetsnivå er «en rettslig standard som kun skal trekke opp de ytre rammene virksomhetene må forholde seg til, og gi virksomhetene mulighet til å se det totale omfanget av sikkerhetstiltak i sammenheng, også tiltak som ikke følger av sikkerhetsloven».[83]

I henhold til virksomhetsikkerhetsforskriften skal det etableres et styringssystem for sikkerhet og et styringsdokument for det forebyggende sikkerhetsarbeidet (kapittel 2 i forskriften). Videre skal det fastsettes sikkerhetsmål, det vil si hvordan kravene til et forsvarlig sikkerhetsnivå skal oppfylles og kriterier for å evaluere om kravene er oppfylt. Kapittel 3, § 12 i virksomhetsikkerhetsforskriften, setter krav til vurdering av risiko. Gjennom en verdivurdering skal virksomheten vurdere hvilken betydning skjermingsverdige verdier (informasjon, informasjonssystemer, objekter og infrastruktur) har for grunnleggende nasjonale funksjoner (GNF) eller nasjonale sikkerhetsinteresser. Følgende elementer skal inngå i vurderingen: trusler og sannsynlighet, sårbarheter, konsekvenser for skjermingsverdige verdier og avhengigheter til andre virksomheter.

5.2 Verdihierarki som utgangspunkt for risikobaserte vurderinger

FFI har som nevnt utviklet et forslag til systematikk og rammeverk for å utføre risikobaserte vurderinger og etablere et forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT. God sikkerhet forutsetter både tilstrekkelig innsikt i virksomhetens kjerneverdier, det vil si de verdier som utvikles og forvaltes som resultat av virksomhetens kjerneaktiviteter, og hvordan disse understøtter GNF eller nasjonale sikkerhetsinteresser.

Rammeverket har en hierarkisk struktur som søker å lage en sammenheng mellom overordnede målsettinger for nasjonal sikkerhet og militære operasjoner, til IKT-virksomheten som skal sørge for militær operativ evne. En strukturert tilnærming der prosessen og resultater dokumenteres bidrar til sporbarhet og til at den informasjon som er innhentet og de vurderinger som er gjort, ivaretas for ettertiden. Dette vil kunne lette arbeidet når nye vurderinger skal utføres samt sørge for at lovkrav om dokumentasjon oppfylles.

Forsvarets overordnede formål er å bidra til å ivareta statssikkerheten og nasjonale sikkerhetsinteresser, det vil si Norges suverenitet, territorielle integritet og demokratiske styreform. Politiske myndigheters oppdrag til Forsvaret er spesifisert i ni oppgaver.[84] I henhold til sikkerhetsloven skal hvert sektordepartement identifisere sine GNF-er, det vil si tjenester, produksjon og andre former for virksomhet som er av en slik betydning at helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

[83] Forsvarsdepartementet (2017). *Prop. 153 L (2016–2017). Lov om nasjonal sikkerhet (sikkerhetsloven)*. s. 81.
[84] Forsvarsdepartementet (2020a).

FD har utpekt fem GNF-er:[85]

- GNF 1: Situasjonsforståelse – Evnen til etterretning, situasjonsforståelse og rettidig varsling.
- GNF 2: Innsats – Evnen til å håndtere episoder og sikkerhetspolitiske kriser og om nødvendig forsvare norsk eller alliertes territorium.
- GNF 3: Kommando og kontroll – Evnen til kommando og kontroll over norske og allierte styrker.
- GNF 4: Beskyttelse – Evnen til beskyttelse av norske og allierte styrker, kritiske samfunnsfunksjoner, samt kritiske funksjoner for Forsvaret.
- GNF 5: Forsvarsdepartementets virksomhet, handlefrihet og beslutningsdyktighet.

FD har operasjonalisert disse GNF-ene i 24 underfunksjoner (21 militære evner og 3 evner for FD) som dermed beskriver forsvarssektorens kjernevirksomhet.[86]

FFI har etablert et verdihierarki som skaper sammenheng mellom de nasjonale sikkerhetsinteressene, Forsvarets oppgaver, GNF-er og underfunksjonene (se Figur 5.1). Verdihierarkiet er et hensiktsmessig utgangspunkt for å vurdere hvordan ulike deler av IKT-virksomheten inngår i, og er nødvendig for, underfunksjonene (militære evner). Med dette som utgangspunkt kan viktigheten, kritikaliteten og fordelen som IKT gir, vurderes for forsvarssektoren for å oppnå sektorens mål og ivareta nasjonale sikkerhetsinteresser.

En slik vurdering forutsetter kunnskap i hele spennet fra operativ virksomhet til teknologi. Som nevnt i kapittel 1 anvendes IKT innenfor både rene administrative kontorsystemer, i operativ sammenheng, integrert i kampsystemer samt integrert i bygg og anlegg i form av industrielle IKT-systemer. All virksomhet og alle prosesser i forsvarsektoren skal imidlertid støtte opp om de operative militære evnene. Vurderingen av risiko må derfor knyttes til Forsvarets behov og bruk av IKT i sin virksomhet, både i væpnet konflikt, krise og fred.

For å vurdere risiko er det den funksjonaliteten IKT utgjør for Forsvaret i ulike situasjoner som er viktig. Det vil si hvilke operative evner IKT bidrar til, både direkte og indirekte. Behovet for IKT, og hvor kritisk dette behovet er, bestemmes av operativ kontekst. Det er viktig å presisere at sikkerhet innebærer både konfidensialitet, integritet og tilgjengelighet. Risikobildet må kontinuerlig oppdateres i lys av endringer innen verdier, sårbarheter og trusler.

[85] Forsvarsdepartementet (2022a). *For budsjettåret 2023. (Prop. 1 S (2022-2023),* s. 122.
[86] Underfunksjonene er Unntatt offentlighet, og inkluderes derfor ikke i denne rapporten.

Figur 5.1 Verdihierarki for Forsvarets virksomhet (evner/underfuksjoner) som understøtter grunnleggende nasjonale funksjoner (GNF), Forsvarets oppgaver og nasjonal sikkerhet (Endregard et al., 2023).

Verdihierarkiet bør være utgangspunktet for en systematikk og et grunnlag for å vurdere risiko og sikkerhet knyttet til Forsvarets IKT-baserte funksjoner basert på hvordan disse funksjonene understøtter de operative evnene / underfunksjonene.[87] Forsvaret bør derfor konkretisere de IKT-baserte funksjonene, -systemene og -tjenestene som understøtter Forsvarets militære evner.

[87] Funksjonsbegrepet er sentralt i sikkerhetsloven. Vi velger å benytte begrepet IKT-baserte funksjoner som et samlebegrep for både IKT-tjenester, informasjonssystemer og IKT-infrastruktur. En IKT-basert funksjon inkluderer menneskelige, teknologiske og organisatoriske ressurser (se Endregard et al (2023), s. 18).

Dette innebærer at Forsvaret må forstå og synliggjøre hvordan IKT-baserte funksjoner griper inn i og er integrert i de militære evnene.

Med utgangspunkt i de identifiserte IKT-baserte funksjonene kan det så utføres verdi- og risikovurderinger for de IKT-systemer, -infrastruktur og informasjon som disse funksjonene er avhengig av. Formålet er å identifisere de operative konsekvensene og skadefølgene det kan få dersom skjermingsverdige verdier, det vil si informasjon, informasjonssystemer, infrastruktur og objekter, blir utsatt for ulike former for sikkerhetstruende virksomhet. Konsekvenser kan være at IKT-baserte funksjoner faller bort eller blir vesentlig redusert, eller at informasjon ikke lenger er tilgjengelig eller ikke er til å stole på.

Slike risikovurderinger og eventuelle andre viktige hensyn, eksempelvis kost/nytte-vurderinger, setter Forsvaret i stand til å definere sikkerhetskrav for de IKT-baserte funksjonene, -tjenestene og -systemene, og til å implementere nødvendige sikkerhetstiltak for å ivareta et forsvarlig sikkerhetsnivå. Forsvarlig sikkerhetsnivå oppnås når risikoen med tilhørende usikkerheter vurderes til å være på et akseptabelt nivå.

Forsvarlig sikkerhetsnivå er en dynamisk størrelse som raskt vil endres i takt med endringer i virksomhetens innhold og struktur (endringer i IKT-systemer og deres bruk, nye fremskaffelser, endringer i organisasjon og personell, sourcing og så videre). Det er derfor viktig at verdi- og risikovurderingene knyttet til Forsvarets bruk av IKT som grunnlag for sikkerhetskrav kontinuerlig oppdateres og vedlikeholdes i lys av de endringene som skjer teknologisk og organisatorisk.

5.3 Anbefalinger

Forsvarets kjerneoppgave er å ivareta nasjonal sikkerhet i væpnet konflikt, krise og fred. Forsvarssjefen, som etatsleder, er ansvarlig for at Forsvarets IKT-virksomhet har et forsvarlig sikkerhetsnivå slik at nasjonale sikkerhetsinteresser ivaretas. Det forbyggende sikkerhetsarbeidet for IKT-virksomheten skal sørge for at IKT-funksjonene som Forsvaret er helt avhengig av, er sikre, robuste og tilgjengelige. I henhold til sikkerhetsloven og tilhørende forskrifter skal Forsvaret til enhver tid ivareta og dokumentere et forsvarlig sikkerhetsnivå for sin virksomhet, inkludert IKT-virksomheten, basert på risikobaserte vurderinger. Dette er ikke trivielt. Forsvaret har et helhetlig ansvar for å sørge for et forsvarlig sikkerhetsnivå, uavhengig av sourcing. Forsvaret og forsvarssjefen, som etatens leder, må derfor også inneha nødvendig kompetanse for løpende å kunne gjøre vurderinger av forsvarlig sikkerhetsnivå.

Basert på de foregående delkapitlene har vi følgende råd og anbefalinger:

Forsvarlig sikkerhet – anbefalinger

- Forsvaret bør utvikle et metodisk kunnskapsgrunnlag for å gjennomføre helhetlige verdi- og risikovurderinger i henhold til systematikken i sikkerhetsloven. Systematikken bør baseres på Forsvarets GNF-er og militære evner. Forsvaret bør identifisere hvordan IKT inngår i Forsvarets militære evner og understøtter nasjonale sikkerhetsinteresser.

- Forsvaret bør utføre verdi- og risikovurderinger for de identifiserte IKT-baserte funksjonene, dette for å identifisere de operative konsekvensene og skadefølgene det kan få dersom de skjermingsverdige verdiene som inngår i funksjonene blir utsatt for ulike former for sikkerhetstruende virksomhet. Verdi- og risikovurderingene bør kontinuerlig oppdateres og vedlikeholdes.

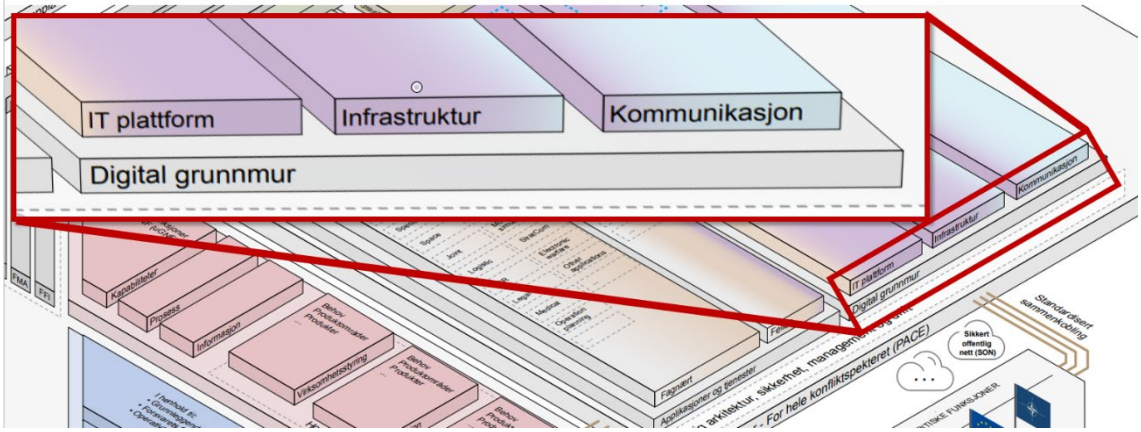
- Basert på risikovurderinger og eventuelle andre sentrale hensyn som kost/nytte bør Forsvaret definere sikkerhetskrav for de IKT-baserte funksjonene, -tjenestene og -systemene og implementere nødvendige sikkerhetstiltak for å ivareta et forsvarlig sikkerhetsnivå.

- Forsvaret bør gjennomføre helhetlige risikobaserte vurderinger som ledd i sourcing for å vurdere forsvarlig sikkerhetsnivå for ulike sourcingalternativer og eventuelt gjøre justeringer i alternativene. Vurderingene bør inkludere hvilke sikkerhetstiltak som må til, med tilhørende konsekvenser og kostnader.

6 Digital grunnmur

Begrepet digital grunnmur har etter hvert blitt svært utbredt og benyttes både av ulike direktorater[88,89], Nasjonal kommunikasjonsmyndighet (NKOM), Nasjonal sikkerhetsmyndighet (NSM) og i forsvarssektoren. Det ser imidlertid ikke ut til å finnes en omforent definisjon av hva begrepet innebærer. Stortingsmelding 28, «Vår felles digitale grunnmur – Mobil-, bredbånds- og internettjenester»[90], gir ingen tydelig beskrivelse av hva grunnmuren faktisk skal bestå av, men gir en indirekte definisjon gjennom målet om at «Den digitale grunnmuren skal gi alle brukere tilgang til sikre og robuste nett og tjenester.»

Forsvaret ga i 2023 ut en digital reguleringsplan (DRP) [91] der det uttrykkes mål for Forsvarets digitale grunnmur på kort og lang sikt. I DRP omfatter den digitale grunnmuren *IT-plattform*, *infrastruktur* og *kommunikasjon* (Figur 6.1). IT-plattform inneholder programvare som sørger for et kjøremiljø for applikasjoner og tjenester, og består blant annet av operativsystem, programvare for drift og overvåking samt en del kjernetjenester. Infrastruktur består hovedsakelig av maskinvare for IT-plattformlaget og sørger for blant annet prosessering og lagring. Kommunikasjon sørger for overføring av data mellom applikasjoner og tjenester over ulike bærere.



Figur 6.1 I Forsvarets digitale reguleringsplan (DRP) omfatter den digitale grunnmuren IT-plattform, infrastruktur og kommunikasjon (figur fra Forsvarsstaben (2023)).

I dette kapitlet vil vi først diskutere hvordan begrepet digital grunnmur er definert. Deretter vil vi diskutere hvilken nytte en slik grunnmur kan ha for Forsvaret, før vi beskriver noen utvalgte kommunikasjonsteknologier som vil kunne inngå i grunnmuren. Disse teknologiene mener vi

[88] Direktoratet for e-helse. (2018). *Felles digital grunnmur*. https://www.digdir.no/digitaliseringsradet/direktoratet-e-helse-felles-digital-grunnmur/1803.
[89] Direktoratet for samfunnssikkerhet og beredskap (2021) *Felles satsingsområder for nød- og beredskapskommunikasjon mot 2030. Strategi for Nasjonal styringsmodell for nød- og beredskapskommunikasjon.*
[90] Kommunal- og distriktsdepartementet. (2020). *Vår felles digitale grunnmur – Mobil-, bredbånds- og internettjenester (Meld. St. 28 (2020–2021)).*
[91] Forsvarsstaben (2023).

Forsvaret bør vie ekstra oppmerksomhet i tiden fremover, da de kan gi store gevinster for Forsvaret.

6.1 Hva er en digital grunnmur?

Som nevnt innledningsvis finnes det ikke en omforent forståelse av hva som ligger i begrepet *digital grunnmur*. NSM gir følgende beskrivelse:[92]

> «Ønsket om samvirke mellom samfunnskritiske funksjoner tilsier at IT-plattformene deres bør ha en felles arkitektur i bunn som sikrer gjenbruk og interoperabilitet på tvers av funksjonene. Og arkitekturen til en slik felles digital grunnmur bør være basert på åpne standarder og løsninger som ikke låser IT-plattformene og tjenestene til spesifikke produkter og leverandører, inkludert skytjenesteleverandører, og hemmer videre utvikling av plattformene.»

NKOM definerer på sin side den digitale grunnmuren som «nett og tjenester som er avgjørende for at Norge skal være et moderne, trygt og solid samfunn.» og sier videre at «[…] den digitale grunnmuren muliggjør digitalisering i de ulike sektorene». [93]

Der Stortingsmelding 28 og NKOM primært ser ut til å vektlegge tilgang til kommunikasjonsnett og -tjenester i sin definisjon, er NSMs beskrivelse mer spesifikk gjennom å beskrive behov for felles IT-plattformarkitektur basert på åpne standarder og løsninger. Skal en digital grunnmur kunne muliggjøre utveksling av informasjon mellom ulike applikasjoner og tjenester, er NSMs definisjon antakelig best egnet som utgangspunkt for dette. Applikasjoner og tjenester som skal kjøre på en felles grunnmur er nødt til å forholde seg til et sett av spesifikasjoner satt av IT-plattformen for å sikre interoperabilitet[94], altså at applikasjonene og tjenestene kan kjøre på grunnmuren og utveksle data med den. På denne måten forenkles utveksling av data mellom ulike applikasjoner og tjenester, og mulighetene for deling av informasjon øker tilsvarende.

I den grad Forsvaret kan sies å ha en digital grunnmur i dag, utgjøres den primært av FISBasis-plattformene[95] sammen med Forsvarets kommunikasjonsinfrastruktur (FKI)[96]. I sum er dette et sett av kommunikasjonsløsninger samt en del IT-plattformer som til sammen kan sies å utgjøre en slags digital grunnmur, dog relativt diversifisert og lite sammenhengende.

Det finnes i dag i liten grad omforente veikart eller målbilder for hvordan en gjennomgående digital grunnmur for Forsvaret bør se ut. I DRP finner man imidlertid starten på det som på sikt kan bli en slik spesifikasjon. En moderne og motstandsdyktig digital grunnmur er ett av åtte

[92] NSM. (2021). *Statens muligheter for IT-modernisering og digital transformasjon*. https://nsm.no/aktuelt/statens-muligheter-for-it-modernisering-og-digital-transformasjon-1.
[93] NKOM. (2019). *EkomROS 2019: Den digitale grunnmuren», Risikovurdering av ekomsektoren.*
[94] For mer informasjon om begrepet interoperabilitet henviser vi til Elstad et al. (2022a).
[95] FISBasis B/U, H/NS samt TYR. Det finnes også en rekke mindre plattformer som gjerne er spesialisert for spesifikke anvendelser.
[96] Her mener vi FKI i en vid definisjon, dvs. alle typer infrastruktur og kommunikasjonsteknologi i Forsvaret.

innsatsområder i DRP, og det beskrives kort-, mellomlange og langsiktige overordnede mål for den digitale grunnmuren, samt en del regulerende prinsipper.

Det vil åpenbart være en gjensidig avhengighet mellom den digitale grunnmuren og applikasjonene og tjenestene som kjører på den; grunnmuren må støtte behovene til applikasjonene og tjenestene, samtidig som applikasjoner og tjenester må følge de reguleringer og føringer som grunnmuren gir, blant annet for å sikre interoperabilitet. Dette betyr at en gjennomgående digital grunnmur må tas frem parallelt med utvikling av nye applikasjoner og tjenester. Selve spesifikasjonen av den digitale grunnmuren må likevel på plass først, slik at det deretter kan beskrives hvilke standarder, formater, protokoller, osv. det forventes at applikasjoner og tjenester skal benytte og rette seg etter.

6.2 Hvorfor trenger Forsvaret en digital grunnmur og hva kan den bidra til?

I Riksrevisjonens undersøkelse av Forsvarets informasjonssystem[97] trekkes manglende mulighet til samhandling på grunn av kommando og kontroll (K2)-systemer med ulik teknologi frem som et problem. I tillegg beskrives manglende sikkerhet i disse systemene som et annet problem. En digital grunnmur vil være et virkemiddel for å redusere begge disse problemene. En felles grunnmur som spesifiserer krav til applikasjonene vil, som nevnt, gjøre det enklere å oppnå interoperabilitet mellom applikasjoner og tjenester som kjører på grunnmuren. En digital grunnmur basert på en omforent spesifikasjon kan med andre ord bidra både til forbedret interoperabilitet og gjøre det enklere å ta i bruk nye teknologier.

Videre kan grunnmuren potensielt bidra til et mer helhetlig sikkerhetsregime ved å samle større deler av sikkerhetsfunksjonaliteten i grunnmuren og pålegge alle applikasjoner og tjenester å bruke denne funksjonaliteten fremfor å implementere egne løsninger. Ved å samle sikkerhetsfunksjonaliteten på ett sted blir det også enklere å sørge for sentralisert styring av IKT-sikkerheten i Forsvaret. Den strategiske IKT-ledelsen vil ha bedre forutsetning for å styre en enhetlig grunnmur enn en rekke diversifiserte systemer. Dessuten vil en enhetlig grunnmur gjøre det enklere å ta i bruk nye verktøy for styring og kontroll, oppnå god konfigurasjonsstyring, og etablere systemer for prioritering og sikkerhetsovervåking.[98]

DRP sier at det skal utarbeides målbilder og veikart for henholdsvis IT-plattform, infrastruktur og kommunikasjon. Som en del av arbeidet med å utvikle dette anbefaler vi at det legges vekt på å avklare ambisjoner og forventninger til den digitale grunnmuren. Et eksempel kan være å konkretisere hvilke funksjoner som bør være i grunnmuren og hvilke som kan overlates til applikasjonene og tjenestene som kjører på grunnmuren. Det vil være vesentlig å avklare hvilke krav det er fornuftig og mulig å stille til applikasjonene, for eksempel grensesnitt, protokoller og sikkerhetsfunksjoner. Slike krav må fastslås, slik at de som skal utvikle eller anskaffe applikasjoner og tjenester vet hva slags kjøremiljø de vil måtte forholde seg til.

[97] Riksrevisjonen (2022).
[98] Mykkeltveit, A., Fongen, A. (2020). *Moderne løsninger for management av sammensatte kommunikasjonsinfrastrukturer*. (FFI-rapport 20/01320). Forsvarets forskningsinstitutt.

Videre er det viktig å påse at de føringene som gis om den digitale grunnmuren i DRP faktisk etterleves, særlig i forbindelse med fremskaffelser og utviklingstiltak knyttet til selve grunnmuren, men også for applikasjoner og tjenester som skal benytte den. Vi anbefaler derfor at Forsvaret sørger for at det i styringsmodellen for IKT utpekes en myndighet som kan sørge for at de IKT-tiltak som iverksettes er i henhold til grunnmurens spesifikasjoner. Føringer som er nødvendige for å realisere den digitale grunnmuren bør forankres i organisasjonen gjennom brukerinvolvering slik at det etableres en forståelse for nødvendigheten av de føringene som er vedtatt. Dette forholdet har vi beskrevet tidligere i delkapittel 2.2.

6.3 Kommunikasjonsteknologier som bør inngå i grunnmuren

Som nevnt består den digitale grunnmuren ifølge DRP av både IT-plattformer, infrastruktur og kommunikasjon (figur 6.1). Forsvaret har et bredt spekter av løsninger innenfor alle disse områdene, og har også pågående fremskaffelsesprosjekter som har til hensikt å fornye og erstatte flere av disse løsningene. Det faller utenfor denne rapportens formål å omtale disse løsningene i detalj, men vi vil i det følgende beskrive noen kommunikasjonsteknologier som en fremtidig grunnmur vil måtte ta hensyn til og som vi mener Forsvaret bør ha spesiell oppmerksomhet på i tiden fremover da de vil kunne gi forbedret kommunikasjonskapasitet og tilgjengelighet og dermed operative gevinster.

De teknologiene vi legger vekt på er *kommersiell mobilteknologi* samt kommersiell og militær *satellittkommunikasjon*. Vi vil videre i dette kapitlet diskutere hvilket mulighetsrom som ligger i å anvende disse teknologiene samt gi noen anbefalinger om hvordan Forsvaret kan realisere dette.

6.3.1 Kommersiell mobilteknologi

Kommersiell mobilteknologi har utviklet seg gjennom flere teknologigenerasjoner. Femte generasjons mobilteknologi (5G) er nå i ferd med å tas i bruk i de kommersielle mobilnettene, og gir vesentlig høyere overføringskapasiteter, høyere pålitelighet, støtte for flere tilkoblede enheter og tilfredsstiller flere brukerbehov enn hva som er mulig med 4G. Den nye radioteknologien i 5G kan benytte flere frekvensområder enn tidligere, blant annet med egenskaper som gjør dem mindre utsatt ved elektronisk krigføring.[99] Den kommersielle mobilteknologien forventes å utvikle seg vesentlig de neste årene og vil kunne utgjøre en viktig bestanddel i Forsvarets digitale grunnmur.

Kommersiell mobilteknologi er allerede tatt i bruk i Forsvaret i et omfang som ikke er uvesentlig. Mange av Forsvarets taktiske kommunikasjonsnoder har 4G-modem som benyttes fordi 4G har forholdsvis høy overføringskapasitet, er enkelt tilgjengelig og gir en god tjeneste. I tillegg benyttes mobiltelefon sannsynligvis av flere avdelinger til å løse ulike oppgaver uten at dette er forankret i noe sambandskonsept.

[99] Birutis, A., Mykkeltveit, A., Ulversøy, T., Borlaug, Ø. D., Kårstad, J., (2022). *A study of 5G New Radio and its vulnerability to jamming*. (FFI-rapport22/00906). Forsvarets forskningsinstitutt.

Mime-programmet skal fornye Forsvarets kampnære IKT og baserer seg på et hybridkonsept[100] hvor «det benyttes både tradisjonell militær teknologi og militært tilpasset kommersiell teknologi». Balansen i dette hybridkonseptet er imidlertid uklar i den forstand at det foreløpig ikke er bestemt om noen militære kommunikasjonssystemer skal erstattes med mobilteknologi eller om mobilteknologi utelukkende skal være et supplement. Det er heller ikke avgjort om det er noen avdelinger som skal ta i bruk kommersiell mobilteknologi som primær kommunikasjonsløsning og når dette eventuelt skal skje.

Konkrete beslutninger om hvordan hybridkonseptet skal realiseres krever vurderinger rundt flere brukeres behov, tekniske muligheter og begrensninger, trusler og sårbarheter samt økonomiske betraktinger. I program Mime jobbes det med hybridkonseptet primært ut i fra en «*bottom-up*»-tilnærming i samarbeid med utvalgte brukere. Det er etablert ulike team som hovedsakelig gjennomfører vurderinger rundt en bestemt teknologi.[101] De konkrete beslutningene må imidlertid gjøres på strategisk nivå som må utarbeide retningslinjer for hvor i organisasjonen og i hvilke situasjoner teknologien kan anvendes på en sikker måte, jamfør beskrivelse av intendert bruk (kapittel 2.2.1).

Vi anbefaler at Forsvaret tar i bruk 5G, også i operativ bruk, og utarbeider føringer for bruk av teknologien, for eksempel i form av en egen strategi for 5G.[102] Det finnes også andre kommersielle trådløse teknologier, slik som Wi-Fi, som til dels kan benyttes til samme formål som 5G. Strategien bør tilsikte å begrense antall varianter av slike teknologier for å sørge for en helhetlig og forsvarlig ivaretagelse av sikkerheten.

Strategien bør beskrive innenfor hvilke rammer det kan anses trygt å anvende 5G-løsninger, og bør inneholde tiltak om hvordan teknologien skal tas i bruk. Tiltakene bør følge prinsippet om strukturert fleksibilitet, som nevnt i kapittel 2, slik at det blir en balanse mellom de enkelte avdelingenes mulighet til å prøve ut ny teknologi og de mulighetene det gir, samtidig som det settes rammer for gjennomføringen og implementasjonen av teknologien.

6.3.2 Kommersiell satellittkommunikasjon

Omfattende kommersialisering av romteknologi sammen med teknologisk utvikling har nå gjort det mulig å lage satellitter langt billigere enn tidligere. Dette gjelder særlig for mindre satellitter i lav jordbane, hvor satellittene utsettes for mindre kosmisk stråling enn i høyere baner og dermed kan bygges ved hjelp av billigere komponenter. Videre har større konkurranse blant operatørene av raketter gjort at også oppskyting av satellitter har blitt billigere. Til sammen har disse

[100] Hybridkonseptet er definert som alternativ 3a i Konseptuell Løsning for prosjekt 8043 Taktisk Ledelsessystem for landdomenet som ble vedtatt av Stortinget i 2018. Forsvarsdepartementet (2021b). *For budsjettåret 2021. (Prop. 1 S (2020-2021))*.
[101] I Mime finnes det blant annet team for hver av teknologiene Combat Net Radio (CNR), 5G, Taktisk mobil bredbåndslink og satellittkommunikasjon.
[102] Voldhaug, J. E., Hansen, B. J., Lund, K., Mykkeltveit, A., Rytir, M., Bentstuen, O. I. (2021). *Hvordan kan ny IKT gjøre Forsvaret bedre?* (FFI-rapport 21/01819). Forsvarets forskningsinstitutt.

faktorene ført til at flere nye kommersielle systemer for satellittkommunikasjon nå er på vei til å bli realisert.[103]

Denne utviklingen vil kunne føre til en betydelige økning av tilgjengelig overføringskapasitet på steder uten godt utbygd bakkebasert infrastruktur. Dersom denne type løsninger utnyttes av Forsvaret, kan den potensielt gi høyhastighetskommunikasjon til alle Forsvarets kjøretøy og enheter, i prinsippet uavhengig av hvor de befinner seg. Enheter trenger da ikke å stoppe for å etablere kommunikasjon, men kan i stedet plassere og bevege seg ut fra rent operative vurderinger.

Selv om den teknologiske utviklingen har gått hurtig har det så langt vært begrenset med kommersielle systemer som har kunnet realisere disse mulighetene for det norske forsvaret. Dette skyldes blant annet at markedspotensialet for å tilby satellittjenester i nordområdene har vært begrenset. Iridium har i mange år vært det eneste satellittbaserte systemet som har tilbudt kommunikasjonstjenester i polare strøk.[104] De siste årene har også leverandøren OneWeb begynt å tilby globalt dekkende kommunikasjonstjenester, inkludert polområdene, med betydelig høyere kapasitet enn det Iridium kan tilby.[105] Starlink-systemet som tilbys av SpaceX, begynte i løpet av 2022 å tilby sin tjeneste så langt nord som Svalbard. I tillegg til disse leverandørene planlegger Telesat å starte opp Lightspeed-systemet[106] som skal tilby sammenlignbare tjenester som OneWeb og Starlink.

De ulike kommersielle systemene som nevnes her har ulike tekniske egenskaper og dermed forskjellige sårbarheter, med de har til felles at de kan tilby relativt rimelig overføringskapasitet for flere av Forsvarets avdelinger. Sammen med utviklingen innen små og mobile satellitt-terminaler vil dette trolig åpne for en rekke nye anvendelsesområder for satellittkommunikasjon for Forsvaret i tiden fremover. De kommersielle systemene bør utnyttes som supplement til de militære systemene som anvendes i dag og de som er under planlegging. Aktuelle bruksområder er, i tillegg til mobilt bruk for Forsvarets operative avdelinger, å benytte kommersiell satellittkommunikasjon som reserveløsning for stasjonær infrastruktur på faste lokasjoner, eller for å overføre velferdstrafikk slik at kapasitet kan frigjøres fra militære og mer kostbare systemer.

Betydningen av kommersielle satellittkommunikasjonssystemer er demonstrert gjennom 2022 i Ukraina-konflikten, der Starlink i flere tilfeller har vist seg å kunne tilby en verdifull kommunikasjonstjeneste for de ukrainske styrkene.[107] Utstrakt bruk av slike systemer gjør imidlertid at de kan bli et mål dersom signalene kan detekteres av fiendtlige styrker.[108]

[103] Ibid.
[104] Mjelde, T. M., Berg, T. J., Arneson, V Sander, J. (2015). *Iridium Pilot kommunikasjonstester mellom FFI, KV Svalbard og Haakonsvern – oppsett og resultater.* (FFI-rapport 2015/02209). Forsvarets forskningsinstitutt.
[105] Landmark, L., Mjelde, T. M., Rytir, M., Rygg, E., Sander, J. (2022). OneWeb test results. (FFI-eksternnotat 22/01872). Forsvarets forskningsinstitutt.
[106] https://www.telesat.com/leo-satellites/.
[107] Davis, M. (2022). *The implications of Commercial Space. From Enabling Military Capability to Introducing New Dynamics into Competition.* The air power journal. Ch 4. Nov 2022.
[108] Ibid.

På bakgrunn av disse betraktningene mener vi at Forsvaret bør gjennomføre en analyse av hvordan nye kommersielle satellittkommunikasjonstjenester kan dekke Forsvarets brukerbehov og hvilke sårbarheter de enkelte systemene har. Analysen bør resultere i en plan som beskriver intensjon og tiltenkt bruk, og som åpner for at avdelinger kan prøve ut den nye teknologien.

Forsvaret bør dessuten utrede fremskaffelse av et stort antall terminaler for sivil satellittkommunikasjon til bruk på kjøretøy og farkoster. Forsvaret bør vurdere terminaler til bruk med både eksisterende geostasjonære satellittsystemer og som kan benyttes for eksisterende og kommende kommersielle systemer i andre baner.

6.3.3 Utnyttelse av planlagte militære satellittløsninger

Som vi har vært inne på i kapittel 5 må Forsvaret gjennomføre verdi- og risikovurderinger for å identifisere de operative konsekvensene og skadefølgene dersom IKT-baserte verdier blir utsatt for sikkerhetstruende virksomhet. Sivile kommunikasjonssystemer har gjerne noen sårbarheter som igjen medfører en risiko. Det vil i mange tilfeller være behov for egne spesialdesignede systemer for Forsvaret som både har mer robuste tekniske egenskaper enn sivile systemer og som vil kunne muliggjøre større kontroll over leverandørkjeden.

Arctic Satellite Broadband Mission (ASBM) er et eksempel på et system som er utviklet for Norges spesielle behov i nordområdene. Dette systemet vil i slutten av 2023 settes i drift av Space Norway. Systemet vil bestå av to satellitter i høyelliptisk jordbane (HEO). Dette vil bli et norsk statseid system for bredbåndskommunikasjon i Arktis som har en investeringsramme på 3,8 milliarder kroner og med en antatt levetid på 15 år.[109]

Forsvaret anskaffer egne nyttelaster for kommunikasjon på disse satellittene, og satellittene vil også ha nyttelaster for Inmarsats kommersielle nettverk, samt en amerikansk militær nyttelast.

FFI har gjennomført beregninger som viser at ASBM gir bedre dekning i Norge enn geostasjonære satellitter, spesielt i Nord-Norge.[110] Kapabiliteten som ASBM utgjør, vil derfor kunne ha stor betydning for Forsvarets evne til å operere i nordområdene dersom den utnyttes godt. For at dette systemet skal kunne utnyttes fullt ut av Forsvaret er det imidlertid en forutsetning at det anskaffes terminaler som kan kommunisere over satellittene og som kan integreres med Forsvarets kampplattformer. Det er igangsatt fremskaffelser av terminaler for maritime fartøy. ASBM vil imidlertid også kunne ha anvendelser innen landdomenet, både for de kampplattformene og enhetene som i dag benytter geostasjonære satellittsystemer og for andre enheter som per i dag ikke bruker satellittkommunikasjon. Per i dag er det ikke igangsatt fremskaffelsesaktiviteter som vil kunne realisere bruk av ASBM i landdomenet.

Det finnes leverandører som både kan utvikle og tilpasse eksisterende terminaler for å kunne benyttes med ASBM, men denne type terminaler er per i dag ikke hyllevare. Som vi beskrev i

[109] Space Norway (2020). *Årsrapport 2020.*
[110] Skeie, B. (2022). *ASBM-klaring over hele Norge*. (FFI-eksternnotat 22/00580). Forsvarets forskningsinstitutt.

kapittel 1 er det erfaringsmessig meget tidkrevende å gjennomføre IKT-investeringer i forsvarssektoren. Det er dermed en betydelig risiko for at det vil kunne ta flere år før landdomenet får utnyttet de mulighetene ASBM gir med hensyn på dekning og bredbåndskapasitet.

Ettersom levetiden til ASBM er anslått å være 15 år er det avgjørende at systemet tas i bruk så raskt som mulig slik at kapasiteten blir utnyttet best mulig gjennom levetiden. Staten Norge vil få redusert utbytte av den betydelige investeringen systemet utgjør så lenge det ikke er anskaffet nok terminaler, og Forsvaret vil heller ikke få realisert den operative gevinsten som dette systemet kan gi.

På bakgrunn av dette mener vi at Forsvaret på kort sikt bør sørge for at det sikres god utnyttelse av ASBM, også i landdomenet, og anskaffe terminaler som kan tilpasses operativ bruk på aktuelle plattformer. På noe lengre sikt bør Forsvaret også identifisere løsningsalternativer for neste generasjon satellittsystem når levetiden for ASBM løper ut. Gitt de mulighetene som satellittkommunikasjon gir, bør det utredes om Forsvaret bør fremskaffe en egen satellittkonstellasjon, for å dekke behov som ikke kan dekkes av kommersielle eller allierte løsninger, eller om det bør etableres en fremtidig løsning sammen med andre aktører.

6.4 Anbefalinger

Basert på de foregående delkapitlene har vi følgende råd og anbefalinger:

Digital grunnmur – anbefalinger

- Forsvaret bør ytterligere avklare ambisjoner og forventninger til den digitale grunnmuren, og videreutvikle prinsipper, krav og føringer i henhold til dette, slik at de som skal utvikle eller anskaffe applikasjoner og tjenester vet hva de vil måtte forholde seg til.
- Forsvaret bør inkludere i styringsmodellen for IKT en myndighet som kan sørge for at de IKT-tiltak som iverksettes er i henhold til grunnmurens spesifikasjoner.
- Forsvaret bør utarbeide strategier som beskriver tiltenkt og sikker bruk av sivile kommunikasjonsteknologier som 5G og kommersielle satellittkommunikasjonssystemer.
- Forsvaret bør fremskaffe terminaler som sikrer god utnyttelse av planlagte satellittløsninger og utrede en egen satellittkonstellasjon for å dekke fremtidige behov.

7 Oppsummering

I denne rapporten har vi presentert temaer som er viktige i forbindelse med Forsvarets IKT. Det har ikke vært til hensikt å behandle IKT-området i sin fulle bredde i denne rapporten, men det er valgt ut noen områder hvor vi mener at Forsvaret bør gjøre grep på kort sikt for å oppnå bedre effekt av IKT. De fem hovedtemaene vi har behandlet i denne rapporten er:

1. Kvalitet i beslutningsprosessene
2. Sourcing og strategisk partnerskap
3. Forsvarssektorens kompetanseutvikling innen IKT-området
4. Forsvarlig sikkerhetsnivå
5. Digital grunnmur

Innenfor hvert hovedtema har vi gitt anbefalinger som vi mener kan være relevante både for Forsvarsstabens IKT-avdeling (FST J6) og for øvrige beslutningstakere som jobber med investering og strategisk styring av IKT-virksomheten.

Hovedtema 1 «Kvalitet i beslutningsprosessene». Her anbefaler vi:

- Beslutninger knyttet til utviklingen av IKT-området bør være sporbare og gjennomsiktige for å ivareta kvaliteten i beslutningsprosessen.
- Intendert IKT-bruk på et overordnet nivå bør inkluderes i eksisterende prosessbeskrivelser, som for eksempel SOP-er og TOR-er. En SOP bør inneholde hvor, hvordan informasjons-produktene skal organiseres, samt intensjonen bak denne organiseringen.
- Det bør i størst mulig grad styres etter prinsipper om strukturert fleksibilitet, ved å etablere en balanse mellom autonomi og rammer i gjennomføringen.

Hovedtema 2 «Sourcing og strategisk partnerskap». Her anbefaler vi:

- Forsvaret bør ha en systematisk og kontinuerlig prosess for å utvikle og vedlikeholde en sourcing-strategi som tar hensyn til faktorene operativt fortrinn, forsvarlig sikkerhetsnivå, transaksjonskostnader, kompetanse, begrenset rasjonalitet og risiko for opportunisme. Implikasjoner for krigens folkerett bør også være én sentral faktor i strategien.
- Forsvaret bør ved inngåelse av et strategisk partnerskap lage en oversikt over de transaksjonskostnader som partnerskapet medfører og oppdatere denne underveis. Over-sikten må tydelig avdekke roller, ansvar og myndighet.

Hovedtema 3 «Forsvarssektorens kompetanseutvikling innen IKT-området». Her anbefaler vi:

- Det bør utvikles en strategi for å rekruttere og beholde kritisk IKT-personell i Forsvaret. Digital kompetanse bør også være en sentralt tema i øvrige IKT-strategier og IKT-planer i forsvarssektoren.

- Ved inngåelse av strategisk partnerskap bør Forsvaret utarbeide en strategi som tydeliggjør hva slags IKT-kompetanse sektoren må ha selv. Den bør inkludere hvordan forsvarlig sikkerhetsnivå og folkerett skal ivaretas.
- Forsvaret bør videreutvikle sin sluttbrukerkompetanse, driftskompetanse og kompetanse innen strategisk IKT. Planer bør inneholde konkrete tiltak. Det må inkluderes mål om økt kunnskap om teknologiske muligheter samt holdninger og bevissthet knyttet til IKT.

Hovedtema 4 «Forsvarlig sikkerhetsnivå». Her anbefaler vi:

- Forsvaret bør utvikle et metodisk kunnskapsgrunnlag for å gjennomføre helhetlige verdi- og risikovurderinger i henhold til systematikken i sikkerhetsloven. Systematikken bør baseres på Forsvarets GNF-er og militære evner.
- Forsvaret bør utføre verdi- og risikovurderinger for IKT-baserte funksjoner. Verdi- og risikovurderingene bør kontinuerlig oppdateres og vedlikeholdes.
- Forsvaret bør definere sikkerhetskrav for de IKT-baserte funksjonene, -tjenestene og -systemene og implementere nødvendige sikkerhetstiltak for å ivareta et forsvarlig sikkerhetsnivå.
- Forsvaret bør gjennomføre helhetlige risikobaserte vurderinger som ledd i sourcing for å vurdere forsvarlig sikkerhetsnivå for ulike sourcingalternativer.

Hovedtema «Digital grunnmur». Her anbefaler vi:

- Forsvaret bør ytterligere avklare ambisjoner og forventninger til den digitale grunnmuren, og videreutvikle prinsipper, krav og føringer i henhold til dette, slik at de som skal utvikle eller anskaffe applikasjoner og tjenester vet hva de vil måtte forholde seg til.
- Forsvaret bør inkludere i styringsmodellen for IKT en myndighet som kan sørge for at de IKT-tiltak som iverksettes er i henhold til grunnmurens spesifikasjoner.
- Forsvaret bør utarbeide strategier som beskriver tiltenkt og sikker bruk av sivile kommunikasjonsteknologier som 5G og kommersielle satellittkommunikasjonssystemer.
- Forsvaret bør fremskaffe terminaler som sikrer god utnyttelse av planlagte satellittløsninger og utrede en egen satellittkonstellasjon for å dekke fremtidige behov.

Moderne IKT er en viktig del av fornyingen av Forsvaret og er helt nødvendig for å understøtte operativ evne og for effektiv gjennomføring av virksomheten i forsvarssektoren. For å få effekt av IKT må det være en systematisk kobling mellom teknologien, organisasjonens mål og strategier samt den bevisste målrettede anvendelsen. FFI arbeider videre med råd innen teknologiske muligheter, og anvendelser, samt virkemidler som gir en mer effektiv bruk av IKT. FFI vil i 2023 spesielt vektlegge å studere hvordan forsvarssektoren kan gjøre vurderinger som gir et forsvarlig sikkerhetsnivå og studere hvordan Forsvarets fremtidige digitale grunnmur bør være.

Referanser

Arnfinnson, B., Elman, E., Eriksen. H.S. (2020). *Hvor mye bruker forsvarssektoren på IKT?* (FFI-rapport 20/00806). (BEGRENSET). Forsvarets forskningsinstitutt.

Barney, J. (2002). *Gaining and sustaining competitive advantage*. Prentice Hall.

Berg, H., Waage, K. (2020). *Effektive materiellanskaffelser i Forsvaret – øker andelen hyllevarekjøp.* (FFI-rapport 20/03147). Forsvarets forskningsinstitutt.

Berg, H., Holgeid, K., Jørgensen, M., Volden, G. H. (2021). *Hvordan lykkes med digitalisering? En undersøkelse av nyttestyring i IT-prosjekter i offentlig sektor.* Concept-rapport nummer 64.

Birkemo, G. A., Kristiansen, P., Farsund, B. (2021). *Risiko ved strategisk samarbeid innen IKT – rammeverk og vurdering*. (FFI-rapport 21/00527). Forsvarets forskningsinstitutt.

Birutis, A., Mykkeltveit, A., Ulversøy, T., Borlaug, Ø. D, Kårstad, J., (2022). *A study of 5G New Radio and its vulnerability to jamming*. (FFI-rapport 22/00906). Forsvarets forsknings-institutt.

Davis, F. D., Bagozzi, R. P., Warshaw, P. R. (1989). *User Acceptance of Computer Technology: A Comparison of Two Theoretical Models.* Management Science, 35(8), 982–1003.

Davis, F. D. (1989). *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. MIS Quarterly, 13(3), 318–340.

Davis, M. (2022). *The implications of Commercial Space. From Enabling Military Capability to Introducing New Dynamics into Competition.* The air power journal. Ch 4. Nov 2022.

DeLone, W. H., McLean, E. R. (2003). *The DeLone and McLean Model of Information Systems Success: A Ten-Year Update*. Journal of Management Information Systems, 19(4), 9–30.

Diesen, S. (2022). *Teknologiutviklingens påvirkning på militære styrker og bruken av militærmakt*. (FFI-rapport 22/01682). Forsvarets forskningsinstitutt.

Direktoratet for e-helse (2018). *Felles digital grunnmur*. https://www.digdir.no/digitaliseringsradet/direktoratet-e-helse-felles-digital-grunnmur/1803.

Direktoratet for samfunnssikkerhet og beredskap (2021) *Felles satsingsområder for nød- og beredskaps-kommunikasjon mot 2030. Strategi for Nasjonal styringsmodell for nød- og beredskapskommunikasjon.*

Earl, M. J. (1996). *The Risks of Outsourcing IT*. Sloan Management Review, 37(3), 26–32.

Elstad, A. K., Lund, K., Kristiansen, S., Bloebaum, T. H. (2022a). *Informasjonsdeling i Forsvarets beslutningsprosesser – kritiske suksessfaktorer* (FFI-rapport 22/00146). Forsvarets forskningsinstitutt.

Elstad, A. K., Endregard, M., Mykkeltveit, A. (2022b). *Sourcing for forsvarssektorens IKT-virksomhet – skisse til rammeverk*. (FFI-rapport 22/02237). Forsvarets forskningsinstitutt.

Endregard, M., Nystuen, K. O., Farsund, B.H., Elstad, A. K. (2023). *Forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT – en innledende studie*. (FFI-rapport 23/00600). Forsvarets forskningsinstitutt.

Ferneley, E. H., Sobreperez, P. (2006). *Resist, comply or workaround? An examination of different facets of user engagement with information systems*. European Journal of Information Systems, 15(4), 345–356.

Finne, H. (2019) *Styring og gjennomføring av store statlige IKT-prosjekter. Ekspertenes erfaringer og vurderinger*. Concept rapport nummer 56.

Fishbein, M., Ajzen, I. (1975). *Belief, attitude, intention and behavior: an introduction to theory and research*. Addison-Wesley.

Forskrift 20. desember 2018 om virksomheters arbeid med forebyggende sikkerhet (virksomhet-sikkerhetsforskriften).

Forsvarsdepartementet (2017). *Prop. 153 L (2016–2017). Lov om nasjonal sikkerhet (sikker-hetsloven).*

Forsvarsdepartementet (2019). *IKT-strategi for forsvarssektoren – Hoveddokument* (Godkjent av Forsvarsministeren 27. mars 2019.).

Forsvarsdepartementet (2020a). *Prop. 14 S (2020–2021). Evne til forsvar – vilje til beredskap. Langtidsplan for forsvarssektoren*.

Forsvarsdepartementet (2020b). *Tildelingsbrev for Forsvaret 2021*.

Forsvarsdepartementet (2021a). *Tildelingsbrev for Forsvaret 2022*.

Forsvarsdepartementet (2021b). *For budsjettåret 2021*. (Prop. 1 S (2020–2021)).

Forsvarsdepartementet (2022a). *For budsjettåret 2023*. (Prop. 1 S (2022–2023)).

Forsvarsdepartementet (2022b): *Framtidige anskaffelser til forsvarssektoren 2022–2029*. Kap. 4.5 Cyberdomenet.

Forsvarssjefen (2013). *Manual i krigens folkerett*.

Forsvarsstaben (2018). *Digitaliseringsstrategi for Forsvaret*.

Forsvarsstaben (2021). *Forsvarets IKT-strategi. Økt operativ effekt gjennom robust IKT i kontinuerlig utvikling - IKT for morgendagens forsvar*.

Forsvarsstaben (2022a). *Stående ordre for Forsvarsstaben*, sjef forsvarsstaben, september 2022

Forsvarsstaben (2022b). *IKT-styringsmodell for forsvarssektoren*.

Forsvarsstaben (2023). *Digital reguleringsplan*. (BEGRENSET).

Ilie, V., Turel, O. (2020). *Manipulating user resistance to large-scale information systems through influence tactics*. Information & Management, 57(3).

Jae-Nam, L., Huynh, M. Q., Ron Chi-Wai, K., Shih-Ming, P. (2003). *IT Outsourcing Evolution--Past, Present, and Future.* Communications of the ACM, 46(5), 84–89.

Johansen, S. R. (2019). *Nød kjenner ingen rett»? Totalforsvar, beredskapsrett og folkerett*. I P. M. Norheim-Martinsen (Red.), Det nye totalforsvaret (s. 117–133). Gyldendal.

Kommunal og distriktsdepartementet (2020). *Vår felles digitale grunnmur – Mobil-, bredbånds- og internettjenester (Meld. St. 28 (2020–2021)).*

Lai, L. (2011). *Kompetansemobilisering og egenmotivasjon*. Magma, 3, 50–55.

Lai, L. (2013). *Strategisk kompetanseledelse* (3. utgave.). Fagbokforlaget.

Landmark, L., Mjelde, T. M., Rytir, M., Rygg, E., Sander, J. (2022). *OneWeb test results.* (FFI-eksternnotat 22/01872). Forsvarets forskningsinstitutt.

Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven).

March, J. (1994). *Primer on Decision Making: How Decisions Happen*. Simon and Schuster.

Mjelde, T. M., Berg, T. J., Arneson, V., Sander, J. (2015). *Iridium Pilot kommunikasjonstester mellom FFI, KV Svalbard og Haakonsvern – oppsett og resultater.* (FFI-rapport 2015/02209). Forsvarets forskningsinstitutt.

Mykkeltveit, A., Fongen, A. (2020). *Moderne løsninger for management av sammensatte kommunikasjonsinfrastrukturer*. (FFI-rapport 20/01320). Forsvarets forskningsinstitutt.

NKOM. (2019). *EkomROS 2019: Den digitale grunnmuren», Risikovurdering av ekomsektoren.*

NSM. (2021). *Statens muligheter for IT-modernisering og digital transformasjon*. https://nsm.no/aktuelt/statens-muligheter-for-it-modernisering-og-digital-transformasjon-1.

Paré, G., Guillemette, M. G., Raymond, L. (2020). *IT centrality, IT management model, and contribution of the IT function to organizational performance: A study in Canadian hospitals.* Information & Management, 57(3), 103198.

Pedersen, O. B. (2022). *Bør vi samarbeide? – en litteraturstudie om valg av sourcingstrategi* (FFI-rapport 22/01384). Forsvarets forskningsinstitutt.

Presterud, A. O., Øhrn, M., Waage, K., Berg, H. (2018). *Effektive materiellanskaffelser i Forsvaret – kartlegging av tidsbruk, forsinkelser og gjennomføringskostnader* (FFI-rapport 18/00231). Forsvarets forskningsinstitutt.

Presterud, A.O., Lien, B., Voldhaug, J.E. (2022). *Porteføljestyring i forsvarssektoren – Status i leveranseoppfølgingen*. (FFI-rapport 22/01167). Forsvarets forskningsinstitutt.

Riksrevisjonen (2022). *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner.* (Ugradert versjon av Dokument 3:3 (2022−2023)).

Skeie, B. (2022). *ASBM-klaring over hele Norge*. (FFI-eksternnotat 22/00580). Forsvarets forskningsinstitutt

Skjelland, E., Berg-Knutsen, E., Arnfinnsson, B., Diesen, S., Glærum, S., Guttelvik, M. S., Kvalvik, S., Mørkved, T., Olsen, K. E., Sellevåg, S. R., Sendstad, C., Strand, K. R., Voldhaug, J. E. (2022). *Forsvarsanalysen 2022.* (FFI-rapport 22/00659). Forsvarets forskningsinstitutt.

Space Norway. (2020). *Årsrapport 2020.*

Svendsen-utvalget. (2020). *Økt evne til å kombinere menneske og teknologi - Veier mot et høyteknologisk forsvar* (Svendsen-utvalget, 24. juni 2020). www.regjeringen.no

Van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., de Haan, J. (2017). *The relation between 21st-century skills and digital skills: A systematic literature review.* Computers in Human Behavior, 72, 577–588.

Venkatesh, V., Morris, M. G., Davis, G. B., Davis, F. D. (2003). *User acceptance of information technology: toward a unified view.* MIS Quarterly, 27(3), 425–478.

Williamson, O. E. (1979). *Transaction-cost economics: the governance of contractual relations*. The journal of Law and Economics, 22(2), 233–261.

Voldhaug, J. E., Hansen, B. J., Lund, K., Mykkeltveit, A., Rytir, M., Bentstuen, O. I. (2021). *Hvordan kan ny IKT gjøre Forsvaret bedre?* (FFI-rapport 21/01819). Forsvarets forsknings-institutt.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan, med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs formål

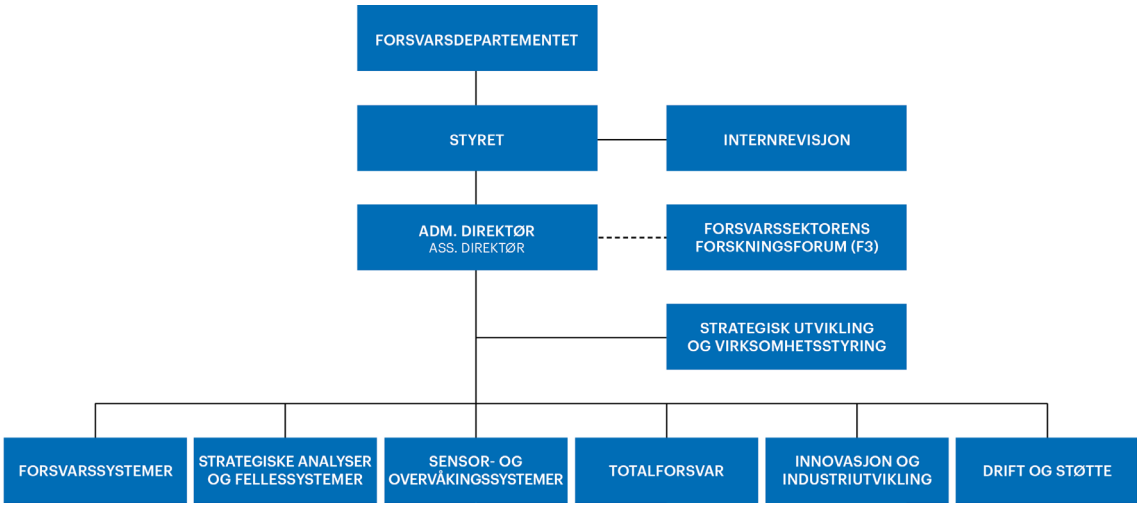
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

FFIs visjon

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs verdier

Skapende, drivende, vidsynt og ansvarlig.



Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en