FFI Forsvarets forskningsinstitutt

24/00074

FFI-RAPPORT

Forsvarets moderne og motstandsdyktige digitale grunnmur

– kritiske suksessfaktorer

Ann-Kristin Elstad
Ketil Lund
Åshild Grønstad Solheim
Monica Endregard
Anders Mykkeltveit

Forsvarets moderne og motstandsdyktige digitale grunnmur
– kritiske suksessfaktorer

Ann-Kristin Elstad
Ketil Lund
Åshild Grønstad Solheim
Monica Endregard
Anders Mykkeltveit

Forsvarets forskningsinstitutt (FFI) 6. mars 2024

Emneord
IKT
Beslutningsprosesser
Samhandling
Digital kompetanse
Forsvarlig sikkerhetsnivå

FFI-rapport
24/00074

Prosjektnummer
1643

Elektronisk ISBN
978-82-464-3514-5

Engelsk tittel
A modern and resilient digital backbone for the Norwegian Armed Forces – critical success factors

Godkjennere
Joakim Flathagen, *forskningsleder*
Jan Erik Voldhaug, *forskningssjef*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

En forutsetning for at Forsvaret skal løse oppgavene sine i fred, krise og krig, er tilgang til hensiktsmessig informasjons- og kommunikasjonsteknologi (IKT). Utredninger og studier viser at Forsvaret har utfordringer innen IKT-området. Forsvaret peker på en moderne og motstandsdyktig digital grunnmur som ett av sine IKT-innsatsområder. Så vidt vi vet, er dette første gang det gjøres en helhetlig studie av Forsvarets digitale grunnmur.

Denne studien har en eksplorativ (undersøkende) forskningstilnærming, med følgende forskningsspørsmål: Hva innebærer Forsvarets moderne og motstandsdyktige digitale grunnmur i et helhetlig perspektiv? Sett i et helhetlig perspektiv, hvilke kritiske suksessfaktorer må til for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur? Vi har tatt utgangspunkt i et sosioteknisk rammeverk og tilpasset det til formålet vårt. I rammeverket spiller sosiale og teknologiske elementer sammen og er gjensidig avhengige. Rammeverket vårt består av seks faktorer: (1) organisasjon og mål, (2) teknologi, (3) eiendom, bygg og anlegg, (4) prosesser og prosedyrer, (5) mennesker og (6) kultur.

Basert på analyser av innsamlede data (gruppesamtaler, workshops og sekundærdata) beskriver vi nåsituasjonen for Forsvarets digitale grunnmur innenfor hver av de seks faktorene i rammeverket. Videre beskriver vi Forsvarets moderne og motstandsdyktige digitale grunnmur i form av et sett av forslag, for eksempel en entydig beskrivelse av roller, ansvar og myndighet, interoperabilitet, sikkerhet mot tilsiktede og utilsiktede hendelser, effektive endringsprosesser, helhetskompetanse innen IKT og ledere som bygger kultur.

Vi har identifisert seks kritiske suksessfaktorer for å kunne oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur: Forsvaret må (1) sikre tilgang til nødvendig kompetanse, (2) etablere strukturert fleksibilitet i styringen, (3) bedre evne og vilje til å gjennomføre endringer, (4) muliggjøre en datadrevet virksomhet, (5) utvikle en tilpasningsdyktig digital grunnmur og (6) etablere og vedlikeholde et forsvarlig sikkerhetsnivå.

For hver av de kritiske suksessfaktorene gir vi en rekke anbefalinger. Alle disse kan ikke håndteres på en gang. Vi anbefaler at Forsvaret prioriterer å sikre entydige roller, ansvar og myndighet, siden dette legger grunnlaget for å gjennomføre prosesser og prosedyrer og gir rammer som mennesker og kultur må forholde seg til. Videre anbefaler vi at Forsvaret etablerer og vedlikeholder et forsvarlig sikkerhetsnivå ved å skaffe seg god oversikt, prioritere innsatsområder og allokere ressurser til risiko- og sikkerhetsstyring. Vi anbefaler også at Forsvaret starter å utarbeide omforente målbilder innenfor de ulike teknologiske bestanddelene av den digitale grunnmuren og for helheten. Til slutt anbefaler vi at Forsvaret gjennomfører en systematisk kompetanseanalyse. Denne kompetanseanalysen bør avdekke hvilke kompetansebehov Forsvaret har for å kunne gjennomføre prosessene sine knyttet til IKT, hvilke kompetansebehov Forsvaret kan dekke ved hjelp av egne ressurser og eventuelt hvilke kompetansebehov som kan dekkes av eksterne samarbeidspartnere.

Summary

A prerequisite for the Norwegian Armed Forces to solve their tasks in peace, crisis and war is access to appropriate information and communication technology (ICT). Investigations and studies show that the Armed Forces face challenges within ICT. Hence, the Armed Forces have identified a modern and resilient digital backbone as a priority. To our knowledge, this is the first study of the Armed Forces' digital backbone in a holistic perspective.

Our research approach is exploratory, with the following research questions: (1) What constitutes the Armed Forces' modern and resilient digital backbone in a holistic perspective? (2) What are the critical success factors needed to achieve and maintain a modern and resilient digital backbone for the Armed Forces? Our point of departure is a socio-technical framework that we have adapted for our purposes. Social and technological elements interplay and are mutually dependent. Our framework consists of six factors: (1) organization and goals, (2) technology, (3) real estate and buildings, (4) processes and procedures, (5) people, and (6) culture.

We describe the current situation for the Armed Forces' digital backbone within each of the six factors of the framework. Furthermore, we describe the Armed Forces' modern and resilient digital backbone in the form of a set of proposals based on our data analysis. Such a backbone requires an unambiguous description of roles, responsibilities and authority, interoperability, security against intentional and unintentional incidents, effective change processes, overall competence within ICT and leaders who build culture.

We have identified six critical success factors for achieving and maintaining the Armed Forces' modern and resilient digital backbone: The Armed Forces need to (1) ensure access to necessary competence (2) establish structured flexibility in management, (3) improve ability and willingness to implement changes, (4) enable a data-driven enterprise approach, (5) develop a flexible and adaptable digital backbone, and (6) establish and maintain an appropriate level of security.

For each of the critical success factors, the study presents several recommendations. However, all of them cannot be achieved at once. As a starting point, we recommend that the Armed Forces prioritize ensuring unambiguous roles, responsibilities, and authority, since this lays the foundation for the implementation of processes and procedures and provides a framework that people and culture must relate to. Furthermore, we recommend that the Norwegian Armed Forces establish and maintain an appropriate security level by obtaining an account of its current state, prioritizing areas of effort and allocating resources to risk and security management. We also propose that the Norwegian Armed Forces start preparing unified goals within the various technological components of the digital backbone, as well as for the overall backbone. Finally, we recommend that the Armed Forces prioritize carrying out a systematic competence analysis to uncover the needs that can be covered by internal resources, and identify which competence needs that can be covered by external partners.

Innhold

Forord

I 2021 etablerte forsvarssjefen (FSJ) IKT-avdelingen i Forsvarsstaben (FST J6, nå Teknologi og IKT (T&IKT)). T&IKT støtter FSJ innen strategisk styring av Forsvarets IKT-virksomhet. Forsvarets forskningsinstitutt (FFI) støtter T&IKT med råd og kunnskapsutvikling gjennom FFIs forskningsprosjekt 1643 «IKT for morgendagens forsvar – støtte til FST J6». Hensikten med denne rapporten er å gi T&IKT råd om en moderne og motstandsdyktig digital grunnmur for Forsvaret.

Rapportens helhetlige problemstilling er omfattende og krevende – og utarbeidelsen av rapporten har krevd betydelig innsats fra flere fagmiljøer ved FFI.

Vi ønsker først å rette en stor takk til alle informanter, som har tatt seg tid til å diskutere en omfattende problemstilling med oss. Uten deres bidrag og innsikt i ulike problemstillinger hadde ikke vi fått skrevet denne rapporten.

Vi vil rette en stor takk til seniorforsker Martin Strand ved FFI for sitt tekstlige bidrag om krypto og *zero trust*, som vi har anvendt i rapporten.

Vi ønsker også å rette en takk til referansegruppa ved FFI, som har bidratt med verdifulle innspill, nyttige diskusjoner og faglig kvalitetssikring.

Kjeller, 10. januar 2024

Ann-Kristin Elstad, Ketil Lund, Åshild Grønstad Solheim, Monica Endregard og Anders Mykkeltveit.

1 Innledning

Dagens sikkerhetspolitiske situasjon er krevende. Forsvaret skal bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser (Sikkerhetsloven, 2018). En forutsetning for at Forsvaret skal løse sine oppgaver i fred, krise og krig, er tilgang til tilstrekkelig og hensiktsmessig informasjons- og kommunikasjonsteknologi (IKT). IKT er i dag innebygget i produkter, tjenester, forholdet til ulike interessenter og arbeidsprosesser (Paré et al., 2020). Dersom IKTs potensiale utnyttes, kan det gi nye muligheter og skape verdi for organisasjoner. Samtidig former IKT-endringene organisasjoner og arbeidsprosesser, og skaper nye utfordringer som må håndteres (Cortellazzo et al., 2019). Dette gjelder også for Forsvaret.

Forsvarskommisjonen trekker fram at forsvarssektoren henger etter innen digitalisering[1] og IKT (NOU 2023: 14, s. 61). Riksrevisjonen gjennomførte i 2022 en undersøkelse av Forsvarets informasjonssystemer[2] for kommunikasjon og informasjonsutveksling i operasjoner (Riksrevisjonen, 2022). I denne undersøkelsen kom det blant annet fram at «Mangler i samvirket mellom Forsvarets kommando- og kontrollinformasjonssystemer kan påvirke Forsvarets operative evne» og at «Sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer gir risiko for svekket operativ evne».

FFIs forsvarsanalyse for 2022 viser at «Forsvaret har gap eller kritiske sårbarheter innen kommunikasjon, dersom en motstander aktivt motarbeider dette» (Skjelland et al., 2022, s. 67). Dette funnet følges opp i forsvarsanalysen for 2023 som sier at «Forsvaret har gap eller kritiske sårbarheter innen håndtering av lufttrusler, evne til sikker kommunikasjon dersom en motstander aktivt motarbeider dette, og tilgang på forsyningstjenester under krise/krig» (Skjelland et al., 2023, s. 74).

Forsvarsdepartementet (FD) har et pågående prosjekt som legger opp til endringer i forsvarssektoren i løpet av 2024, kalt «Forsvarssektoren 2024» (F24). IKT er ett av områdene som omfattes av F24. I sitt grunnlagsarbeid avdekket FD flere systemsvakheter (Forsvaret, 2023a).

Visjonen i Forsvarets IKT-strategi er «Økt operativ effekt gjennom robust IKT i kontinuerlig utvikling – IKT for morgendagens forsvar» (Forsvarsstaben, 2021). IKT-strategien definerer tre strategiske mål for IKT: (1) IKT som driver for kommando og kontroll (K2) og samvirke, (2) effektiv styring av IKT for hurtig ivaretakelse av operative behov samt (3) bedre og raskere utnyttelse av teknologi. I tillegg vektlegges digital kompetanse, selv om det ikke er definert som et eget mål.

Forsvaret har utarbeidet Digital reguleringsplan (DRP) (Forsvarsstaben, 2023) som en del av operasjonaliseringen av Forsvarets IKT-strategi. DRP inneholder åtte utvalgte IKT-innsats-

[1] Digitalisering vil si: « *[…] how IT or digital technologies can be used to alter existing business processes*» (Verhoef et al., 2021 s. 891).
[2] Nasjonal sikkerhetsmyndighet (2020a) definerer et informasjonssystem som «IKT-system, data og tjenestene det tilbyr, bruken av dette, samt menneskers interaksjon med IKT-systemet for å støtte opp under virksomhetsprosesser».

områder med tilhørende mål for 2024, 2026 og 2028. Ett av disse IKT-innsatsområdene er «moderne og motstandsdyktig digital grunnmur». Vi anser at den digitale grunnmuren er et fundament for at Forsvaret skal kunne planlegge og gjennomføre operasjoner, både i fredstid og ved sikkerhetspolitisk krise og væpnet konflikt. Samtidig har det ikke vært utført studier av Forsvarets digitale grunnmur som helhet tidligere, og det kan være uklart hvordan Forsvaret skal håndtere denne grunnmuren. Problemstillingen i denne rapporten handler om hva Forsvaret, på strategisk nivå, bør gjøre for å oppnå målet sitt om en moderne og motstandsdyktig digital grunnmur.

1.1 Hva er en digital grunnmur?

Uttrykket «digital grunnmur» har vært benyttet i offentlige dokumenter i Norge de siste årene (se f.eks. Meld. St. 28 (2020−2021); Nasjonal kommunikasjonsmyndighet, 2019; Nasjonal sikkerhetsmyndighet, 2020b, 2021). Det er tilsynelatende ingen omforent forståelse av hva uttrykket faktisk innebærer (se Flathagen et al., 2023). Det er også ulike meninger om nødvendigheten av uttrykket. Eksempelvis ga Digitaliseringsrådet en anbefaling til Direktoratet for e-helse om å bytte navn på sitt tiltak «felles digital grunnmur» fra et uttrykk som beskriver noe fast og varig (grunnmur) til et uttrykk som indikerer mer utvikling – eksempelvis «byggeklosser»[3] (Digitaliseringsrådet, 2018).

Forskjellige organisasjoner vil ha ulike behov og krav knyttet til sin digitale grunnmur, og vil dermed kunne velge ulike løsninger. Generelt innebærer digital grunnmur at en organisasjon har en form for felles digital infrastruktur. En digital infrastruktur kan forstås som «tekniske systemer, datasamlinger og programsystemer som er tilgjengelig for utvikling av tjenester, både for private og offentlige aktører, og som er viktige for at samfunnet skal fungere.» (Bratbergsengen, 2021). Det innebærer at en organisasjon i sin digitale grunnmur har en del grunnleggende IKT-tjenester med tilhørende sikkerhetsregimer. Omfanget av en digital grunnmur kan variere. Generelt kan det derfor sies at de aller fleste organisasjoner benytter en eller annen form for digital grunnmur.

Hvilke løsninger som er nødvendige for en organisasjons digitale grunnmur, er bestemt av en rekke ulike forhold. Noen forhold kan organisasjonen selv påvirke, for eksempel designvalg, omfang, datahåndtering, roller, ansvar, myndighet og sourcingstrategi. Andre forhold ligger utenfor organisasjonens kontroll, som for eksempel lovverk. Generelt er altså en digital grunnmur mer enn teknologi. Det er en rekke andre faktorer som organisasjonen må ta hensyn til, for blant annet å sikre korrekt bruk, forsvarlig sikkerhet, drift og forvaltning av grunnmuren.

Forsvarssektoren er stor og kompleks, og den har noen krav og utfordringer som ikke er så vanlige i andre sektorer. Dette inkluderer håndtering av ulike graderingsnivåer, en rekke ulike våpen- og sensorplattformer med til dels proprietær teknologi, kommunikasjonsteknologier med svært varierende kapasitet samt trusler om fiendtlig aktivitet. Disse spesielle utfordringene gjør

[3] Direktoratet for e-helse benytter likevel begrepet «digital grunnmur» videre.

at det stilles en del særegne krav, både til teknologien og til de øvrige faktorene som er nødvendige for at den digitale grunnmuren skal fungere.

DRP (Forsvarsstaben, 2023) definerer den digitale grunnmuren i form av et sett med IKT-tjenester innenfor IT-plattform[4], infrastruktur[5] og kommunikasjon[6] for hele krisespekteret.[7] En IKT-tjeneste kan beskrives som en funksjon[8] som leveres av programvare (Laskey et al., 2009). For vårt formål er en IKT-tjeneste det samme som en IKT-funksjon (Endregard et al., 2023).

DRPs (Forsvarsstaben, 2023) forståelse av digital grunnmur er ikke unik. Både Nato og det britiske forsvarsdepartementet (UK Ministry of Defence – UK MoD) benytter begrepet *digital backbone* omtrent slik som DRP beskriver digital grunnmur. Felles for disse definisjonene er at teknologisk sett består en digital grunnmur av maskin- og programvare som tilbyr et sett av IKT-tjenester. Vår forståelse av digital grunnmur fra et teknologisk perspektiv er derfor som følger:

> Fra et teknologisk perspektiv består digital grunnmur av maskin- og programvare som tilbyr et sett med IKT-tjenester (jf. IT-plattform, infrastruktur og kommunikasjon i DRP).

Som nevnt er det mange faktorer som har innvirkning på den digitale grunnmuren. Selv om teknologien utgjør «de synlige» bestanddelene av en digital grunnmur, er det nødvendig å se helhetlig på alle faktorer som inngår. Et slikt helhetlig perspektiv på digital grunnmur finnes også i andre sektorer, eksempelvis i anbefalingene fra Digitaliseringsrådet til Direktoratet for e-helse (se Digitaliseringsrådet, 2018) rundt etablering av en felles digital grunnmur. Disse anbefalingene dreier seg mye om hva som må gjøres på ikke-teknologisk side for å lykkes med å innføre en digital grunnmur.

> I denne rapporten omtaler vi digital grunnmur i et helhetlig perspektiv, ved at vi inkluderer teknologiske faktorer sammen med andre nødvendige faktorer[9].

Studien ser på den digitale grunnmuren Forsvaret har i dag, og vi presenterer forslag til en framtidig digital grunnmur som er moderne og motstandsdyktig. Både den nåværende og

[4] IKT-tjenester som skaper et kjøremiljø for applikasjoner (Forsvarsstaben, 2023).
[5] IKT-tjenester for prosessering, lagring, virtualisering og datasenter (Forsvarsstaben, 2023).
[6] IKT-tjenester for overføring av data mellom applikasjoner og/eller IKT-tjenester (Forsvarsstaben, 2023).
[7] I underkapittel 3.4 går vi mer i detalj rundt hva vi mener en digital grunnmur består av, sett fra et teknologisk perspektiv.
[8] Det vil si noe som er av verdi og nytte for brukeren av IKT-tjenesten (Elstad, Lund et al., 2022).
[9] «Organisasjon og mål», «eiendom, bygg og anlegg», «prosesser og prosedyrer», «mennesker» og «kultur». For flere detaljer, se kapittel 3.

framtidige digitale grunnmuren beskrives helhetlig – det vil si at vi ser på teknologiske faktorer sammen med de øvrige faktorene som inngår i grunnmuren.

> Med Forsvarets moderne og motstandsdyktige digitale grunnmur mener vi en framtidig digital grunnmur som inkluderer alle faktorene i vårt rammeverk.

I rapporten vil vi av lesbarhetshensyn forkorte «Forsvarets moderne og motstandsdyktige digitale grunnmur» til bare «digital grunnmur» eller «grunnmur». Det vil alltid framgå av sammenhengen om vi snakker om dagens eller den framtidige digitale grunnmuren.

1.2 Problemstilling og forskningsspørsmål

Forsvaret har et mål om å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur (Forsvarsstaben, 2023). Problemstillingen i denne rapporten er hva Forsvaret, på et strategisk nivå, bør gjøre for å nå dette målet. For å svare på denne problemstillingen må vi, på overordnet nivå, ha oversikt over nåsituasjonen for Forsvarets digitale grunnmur. Videre må vi undersøke hva en «moderne og motstandsdyktig digital grunnmur» innebærer for Forsvaret, altså hva som inngår og hvilke kapabiliteter en slik grunnmur må eller bør ha. Klarhet i disse forholdene legger grunnlaget for å anbefale kritiske suksessfaktorer (KSF-er) som må være til stede for at Forsvaret skal kunne oppnå og opprettholde en slik digital grunnmur.

Oppsummert har denne studien følgende forskningsspørsmål:

1) Hva innebærer Forsvarets moderne og motstandsdyktige digitale grunnmur i et helhetlig perspektiv?
2) Sett i et helhetlig perspektiv, hvilke kritiske suksessfaktorer må til for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur?

1.3 Avgrensninger

Tilgjengelig tid og ressurser tilsier at denne studien ikke kan dekke alle aspekter ved en moderne og motstandsdyktig digital grunnmur for Forsvaret. Studien går heller ikke i dybden på enkelttemaer, men søker å se helhet og sammenheng på tvers av de faktorene som til sammen danner en slik grunnmur.

Vi gjør en avgrensing mot det vi kaller kampnær IKT, da dette temaet vil dekkes i en annen FFI-rapport (Bloebaum et al., under arbeid). Kampnær IKT kan beskrives som IKT som benyttes på taktisk nivå og lavere.

1.4 Bidrag

Denne studien vil gi en bedre forståelse av hva som inngår i en moderne og motstandsdyktig digital grunnmur for Forsvaret, og hvilke kapabiliteter den bør ha. Videre vil studien tydeliggjøre hva Forsvaret bør gjøre for å nå målet om en slik grunnmur. Rapporten presenterer en liste over KSF-er som må til for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur. Hver av KSF-ene inneholder anbefalinger som kan bidra til at Forsvaret når målet om en slik digital grunnmur.

Rapporten tar utgangspunkt i et eksisterende sosioteknisk rammeverk og tilpasser dette til behovet for å oppnå og opprettholde en moderne og motstandsdyktig grunnmur. Rammeverket kan også brukes i andre sammenhenger der forsvarssektoren trenger et helhetlig perspektiv for å kunne videreutvikle et såkalt sosioteknisk system, altså et system bestående av både tekniske og sosiale faktorer.

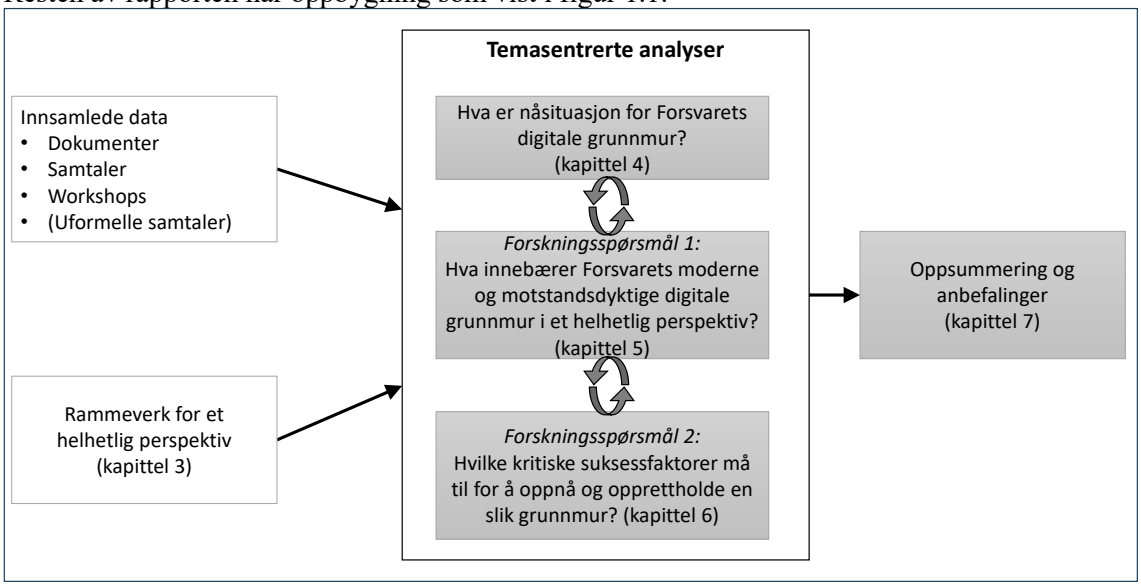
1.5 Leseveiledning

Denne rapporten er først og fremst beregnet på personell i forsvarssektoren som jobber med strategisk styring av IKT-virksomheten[10] og/eller har ansvar for utvikling av IKT-virksomheten i Forsvaret. Dette kapittelet har gitt en kort introduksjon til hva en digital grunnmur er, denne studiens forskningsspørsmål, avgrensninger i studien og studiens bidrag.

Kapittel 2 gir en oversikt over metodiske betraktninger, inkludert forskningstilnærming, datainnsamling, dataanalyse og ivaretakelse av studiens validitet og reliabilitet. Kapittel 2 er myntet på lesere som er spesielt opptatt av framgangsmåten vi har benyttet.

[10] Ifølge Forsvarets IKT-strategi (Forsvarsstaben, 2021) er IKT-virksomheten «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».

Resten av rapporten har oppbygning som vist i figur 1.1.



Figur 1.1 Rapportens oppbygning fra kapittel 3 til kapittel 7.

Kapittel 3 beskriver vårt rammeverk for et helhetlig perspektiv. Her gir vi en kort introduksjon til sosioteknisk systemteori samt en rask gjennomgang av to eksisterende rammeverk. Deretter presenterer vi teori og vårt helhetlige rammeverk som resten av rapporten er bygget rundt.

Kapittel 4 omhandler nåsituasjonen for Forsvarets digitale grunnmur, beskrevet innenfor rammeverket fra kapittel 3. Innholdet i dette kapittelet er i all hovedsak basert på studier av styrende dokumenter, andre offentlige dokumenter, akademisk litteratur i tillegg til litteratur fra konsulentfirmaer. I tillegg har vi hentet enkelte aspekter fra datainnsamlingen (samtaler med personell fra forsvarssektoren).

Kapittel 5 beskriver en framtidig moderne og motstandsdyktig digital grunnmur for Forsvaret. Den beskrives helhetlig gjennom de seks faktorene i rammeverket vårt (1) organisasjon og mål, (2) teknologi, (3) eiendom, bygg og anlegg, (4) prosesser og prosedyrer, (5) mennesker og (6) kultur.

Kapittel 6 beskriver seks KSF-er for å oppnå og opprettholde Forsvarets moderne og motstands-dyktige digitale grunnmur. KSF-er er faktorer ledere må håndtere tilfredsstillende for at organisasjonen skal nå sine mål. Disse seks overordnede KSF-ene blir videre delt opp i ulike temaer, hvor vi kommer med anbefalinger Forsvaret bør gjennomføre for å håndtere disse temaene tilfredsstillende.

Kapittel 4–6 avsluttes alle av et underkapittel som kortfattet oppsummerer funnene i kapittelet. For en rask oversikt kan leseren starte med disse underkapitlene.

I rapportens kapittel 7 presenteres studiens oppsummering og anbefalinger.

2 Metodiske betraktninger

Målet med dette kapittelet er å forklare forskningstilnærming, datainnsamling, dataanalyse og ivaretakelse av studiens validitet og reliabilitet.

2.1 Forskningstilnærming

Studien har en eksplorativ (undersøkende) forskningstilnærming (jf. Ghauri & Grønhaug, 2005; Zikmund, 2003), en forskningstilnærming som er egnet ved uklare problemstillinger. Bidraget til en eksplorativ forskningstilnærming er å skape en større forståelse og innsikt, mer enn en generalisering, i tematikken som studeres (Ghauri & Grønhaug, 2005). Gjennom studien er målet at Forsvaret – og andre relevante aktører – får en større innsikt i og forståelse for hva en moderne og motstandsdyktig digital grunnmur er og hvilke KSF-er som må til for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur. Anbefalingene går ikke i dybden på enkeltelementer innen IKT, men søker overblikk og oversikt.

2.2 Datainnsamling

I en eksplorativ forskningstilnærming kombineres gjerne flere datainnsamlingsteknikker. I denne studien har vi benyttet følgende datainnsamlingsteknikker: gruppesamtale, workshop og uformell samtale.

2.2.1 Utvalg

Gruppesamtaler med personell som jobber med dagens digitale grunnmur i forsvarssektoren kan øke vår forståelse for hvilke kapabiliteter en framtidig moderne og motstandsdyktig digital grunnmur må ha, sett fra deres perspektiv. Våren 2023 ble det derfor gjennomført totalt fire gruppesamtaler med IKT-eksperter fra forskjellige deler av forsvarssektoren. Kompetansen til disse IKT-ekspertene spenner fra strategisk utvikling, digitalisering og styringsmodeller via nettverk, økosystemer, skytjenester og deling av data til taktiske applikasjonstjenesters krav til den digitale grunnmuren. Det var totalt 19 deltakere, både med og uten lederansvar, som deltok i disse gruppesamtalene. Deltakerne var mellom 40 og 65 år.

I tillegg ble det gjennomført to workshops med forskere fra FFI, med totalt ca. 40 deltakere. Alle avdelingene ved FFI var representert under den første workshopen. Kompetansen til forskerne spenner fra utnyttelse av data, taktiske applikasjonstjenesters krav til en digital grunnmur, nettverk og skytjenester. Deltakerne var mellom 25 og 70 år.

2.2.2 Gruppesamtaler med eksperter fra forsvarssektoren innen IKT

Vi gjennomførte fire gruppesamtaler med eksperter fra forskjellige deler av forsvarssektoren i mai og juni 2023. Samtalene hadde en varighet på cirka to timer.

I en gruppesamtale er interaksjonen mellom den som intervjuer og informantene sentral, i tillegg til interaksjonen mellom informantene. Gruppesamtaler krever lite ressurser ved gjennomføring og er ansett som en praktisk datainnsamlingsteknikk for å samle inn data fra flere informanter på kort tid (Ghauri & Grønhaug, 2005). Forskerne som gjennomfører gruppesamtalene, må være bevisste på påvirkningen gruppen selv har på diskusjonen og den informasjonen som blir utvekslet mellom deltakerne. Gruppesamtalen kan påvirkes av gruppestørrelsen og -sammensetningen, personlighetene og rollene til gruppedeltakerne (Ghauri & Grønhaug, 2005). Forskerne må derfor være bevisst på å styre gruppesamtalene, slik at samtalene gir svar på studiens forskningsspørsmål.

Gruppesamtalene hadde en åpen tilnærming. Vi startet med å presentere bakgrunnen for studien og studiens problemstilling. I forberedelsene til gruppesamtalene vektla vi at spørsmålene skulle være strukturerte nok til å svare på problemstillingen. Samtidig skulle spørsmålene være åpne nok til at informantene fikk gode forutsetninger for å komme med tilleggsinformasjon vi ikke hadde tenkt på før samtalene. Følgende spørsmål ble stilt under gruppesamtalene:

- Hva er egentlig Forsvarets digitale grunnmur i dag – sett fra deres perspektiv?
- Hva innebærer en moderne og motstandsdyktig digital grunnmur – og hvilke egenskaper bør Forsvarets digitale grunnmur inneha – sett fra deres perspektiv?
- Sett i et helhetsperspektiv, hvilke kritiske suksessfaktorer må til for å etablere og opprettholde (realisere) en moderne og motstandsdyktig digital grunnmur?

Alle FFI-forskerne i denne studien deltok under gruppesamtalene.[11] Den samme forskeren ledet alle de fire samtalene, for å sikre at de ulike samtalene skulle få en så lik struktur som mulig. Underveis i gruppesamtalene stilte denne forskeren oppfølgingsspørsmålene, dersom informantenes svar var uklare eller dersom informantene benyttet ekspertbegreper som ikke var kjent. Ved behov stilte også de andre forskerne oppfølgingsspørsmål. Alle forskerne noterte underveis i gruppesamtalene.

Personlig intervju ble også vurdert som datainnsamlingsteknikk, men slike intervjuer er mer ressurskrevende enn gruppesamtaler. Disse ressursene hadde vi ikke tilgjengelig i denne studien. Vi vurderte datagrunnlaget fra gruppesamtalene til å være tilfredsstillende, ut ifra tilgjengelig tid og ressurser for vår studie.

Datagrunnlaget fra de fire gruppesamtalene inngår i beskrivelse av nåsituasjon (kapittel 4), en moderne og motstandsdyktig digital grunnmur (kapittel 5) og KSF-er (kapittel 6).

[11] Det var én gruppesamtale hvor én av forskerne ikke var til stede.

2.2.3 Workshops med forskere fra FFI

Første workshop april 2023

Den første workshopen hadde som mål å avdekke deltakernes oppfattelse av hva som var digital grunnmur, hva som ikke var digital grunnmur og hva som var grensetilfeller. I møteinnkallingen antydet vi hvilke spørsmål vi ønsket svar på under workshopen:

- Hva forstår du med begrepet digital grunnmur?
- Hva skal en digital grunnmur inneholde?
- Hva skal en digital grunnmur ikke inneholde?
- Eventuelle tvilstilfeller

Deltakerne ble utstyrt med lapper hvor de noterte ned sine synspunkter. Vi hadde laget ulike soner på veggen, hvor deltakerne plasserte lappene. Etter at alle deltakerne hadde plassert lappene i de ulike sonene, ble innspillene diskutert. På samme måte som under gruppesamtalene med eksperter, var det én forsker som ledet samtalen og stilte oppfølgingsspørsmål ved uklare svar eller ved bruk av ekspertbegreper som ikke var kjent (jf. Geertz, 1983). Ved behov stilte også de andre forskerne oppfølgingsspørsmål. Alle forfatterne av denne rapporten som var til stede under workshopen, noterte innspill og diskusjoner underveis.

Resultater fra første workshop inngår i rapportens kapittel 4.

Andre workshop mai 2023

Den andre workshopen vektla KSF-er. Deltakerne ble delt inn i fem grupper. Gruppene fikk en oppgave om å lage en kort, overordnet beskrivelse av de tre viktigste prioritetene for en digital grunnmur for Forsvaret. Gruppene fikk 20 minutter til disposisjon før resultatet skulle presenteres. Hver gruppe gikk gjennom sine KSF-er, og disse ble deretter diskutert i plenum. Det var én av forfatterne som ledet denne diskusjonen og stilte oppfølgingsspørsmål ved uklare svar eller ved bruk av ekspertbegreper som ikke var kjent (jf. Geertz, 1983). De resterende forfatterne som var til stede, noterte innspillene.

Resultater fra andre workshop inngår i rapportens kapittel 6.

2.2.4 Uformelle samtaler

Det er også gjennomført en rekke uformelle samtaler med personell i forsvarssektoren underveis i studien. Disse uformelle samtalene har gitt forskerne mulighet til å stille spørsmål for å bedre forståelsen knyttet til ulike problemstillinger.

Resultater fra uformelle samtaler inngår i beskrivelse av nåsituasjon (kapittel 4), moderne og motstandsdyktig digital grunnmur (kapittel 5) og KSF-er (kapittel 6).

2.2.5 Sekundærdata

I denne studien inngår styrende dokumenter for forsvarssektoren, andre offentlige dokumenter, akademisk litteratur og litteratur fra konsulentfirmaer. Disse dokumentene har blant annet blitt benyttet for å beskrive nåsituasjonen for Forsvarets digitale grunnmur.

- Langtidsplan for forsvarssektoren (LTP) (Forsvarsdepartementet, 2020a)
- Forsvarssjefens fagmilitære råd 2023 (FMR) (Forsvaret, 2023b)
- IKT-strategi for forsvarssektoren (Forsvarsdepartementet, 2019a)
- Forsvarssektorens klima- og miljøstrategi (Forsvaret et al., 2022)
- Digitaliseringsstrategi for Forsvaret (Forsvarsstaben, 2018)
- Forsvarets IKT-strategi (Forsvarsstaben, 2021)
- Digital reguleringsplan for forsvarssektoren (Forsvarsstaben, 2023)
- Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner (Riksrevisjonen, 2022)
- Svendsen-utvalgets rapport «Økt evne til å kombinere menneske og teknologi Veier mot et høyteknologisk forsvar» (Svendsen-utvalget, 2020)
- Strategi for kunstig intelligens i forsvarssektoren (Forsvarsdepartementet, 2023b)
- Forsvarskommisjonen av 2021 (NOU 2023: 14)
- Totalberedskapskommisjonen av 2021 (NOU 2023: 17)
- Risiko 2023: Økt uforutsigbarhet krever høyere beredskap (Nasjonal kommunikasjons-myndighet, 2023)
- Fokus 2023: Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer (Etter-retningstjenesten, 2023)

Det er også benyttet annen litteratur i rapporten. Se referanseliste for oversikt over de resterende dokumentene som benyttes.

2.3 Dataanalyse

Dataanalyse er prosessen hvor rådata analyseres og tolkes til mer abstrakte funn og kategorier. I en slik dataanalyse identifiserer, kategoriserer og reduserer forskerne rådata (Miles & Huberman, 1994). Formålet med en slik kategorisering er å organisere dataene. Det er derfor et behov for en beskrivelse av denne prosessen for vår studie, slik at andre forskere lettere kan forstå hvordan innsamlede rådata har ledet til spesielle konklusjoner.

En dataanalyse kan være sentrert rundt informanter eller basert på temaer (Miles & Huberman, 1994). I vår studie har vi en temasentrert dataanalyse. Analyseenheter analyseres først hver for seg – for deretter å sammenlignes og analyseres i en helhet.

Analyseenhetene i vår studie er de fire gruppesamtalene med forskjellige deler av forsvarssektoren og de to workshopene med forskere fra FFI.

2.3.1 Forsvarets digitale grunnmur – nåsituasjon

Nåsituasjonen er godt beskrevet i en rekke av dokumentene vi listet i underkapittel 2.2.5. Disse rapportene har vært den primære informasjonskilden for vår beskrivelse. Vi har gått gjennom rapportene, og trukket ut det vi anser som relevant for vår beskrivelse av nåsituasjonen. I tillegg har vi brukt informasjon fra informantene i gruppesamtaler, workshops (der disse har kommet inn på temaet) og uformelle samtaler med aktører i forsvarssektoren.

2.3.2 Forsvarets moderne og motstandsdyktige digitale grunnmur

Datagrunnlaget for utarbeidelsen av forslaget til Forsvarets moderne og motstandsdyktige digitale grunnmur er gruppesamtalene med forsvarssektoren, den første workshopen, de uformelle samtalene og sekundærdata. Tabell 2.1 viser stegene vi har gjennomført i vår dataanalyse for å komme fram til dette forslaget:

STEG	ANALYSEAKTIVITET
1	Under gruppesamtaler og workshops skrev hver enkelt forsker notater. Disse notatene er studiens rådata. Hver forsker delte sine notater med de andre forskerne. Rådataene ble samlet til ett felles dokument for hver av de seks analyseenhetene. Disse seks fellesdokumentene var utgangspunktet for vår analyse.
2	Analysen av hver av analyseenhetene startet med en datareduksjon, dvs. en prosess hvor forskerne velger, forenkler, abstraherer og omformer rådata (Miles & Huberman, 1994). For hver av analyseenhetene analyserte vi notatene og kopierte tekst inn i seks hovedkategorier. Teksten ble ikke endret i denne fasen. Hovedkategoriene i denne studien tilsvarte de seks faktorene i rammeverket (se kapittel 3): (1) organisasjon og mål, (2) teknologi, (3) eiendom, bygg og anlegg, (4) prosesser og prosedyrer, (5) mennesker og (6) kultur.
3	Da teksten fra alle analyseenhetene var kopiert inn i hovedkategorier, leste vi gjennom hovedkategoriene og vurderte om tekst skulle flyttes til andre hovedkategorier. Flytting av rådata mellom hovedkategorier er en del av analyseprosessen, etter hvert som forskerne blir bedre kjent med datamaterialet. Det skjedde også i denne studien.
4	Dataene innenfor hver hovedkategori ble deretter gruppert i underkategorier. For hovedkategorien teknologi (se underkapittel 5.2) grupperte vi dataene i seks underkategorier: (1) IKT-tjenester (funksjonalitet), (2) interoperabilitet, (3) fleksibilitet, (4) utvikling, drift og vedlikehold, (5) forsvarlig sikkerhet (inkl. robusthet og redundans) og (6) klima og miljø. Med unntak av klima og miljø, kjenner vi igjen underkategoriene fra planlegging av materiellanskaffelser innen IKT – som løsningsegenskaper (Forsvarsdepartementet, 2017a), overordnede krav (Forsvarsdepartementet, 2019b) og understøttende kapabiliteter (Forsvarsmateriell & Forsvaret, 2019; Forvarsmateriell & Forsvaret, 2019). Underkategoriene er også brukt i en FFI-studie av muligheter og utfordringer for Forsvaret ved bruk av skytjenester (Lund et al., 2021).

STEG	ANALYSEAKTIVITET
	For de resterende hovedkategoriene i rammeverket eksisterer det ikke tilsvarende inndeling. Her leste forskerne gjennom hver hovedkategori, og plasserte tekst som omhandlet samme tema i ulike underkategorier.
5	I dette steget av analysen sammenlignet vi funn på tvers av analyseenhetene og så funnene i en helhet. Vi laget en tabell med analyseenhetene og hoved- og underkategorier, for å skape helhet (og oversikt). Vi utformet abstrakte navn på hoved- og underkategoriene.
6	Neste steg i analyseprosessen var å skrive et sammendrag av de ulike hoved- og underkategoriene, for en ny datareduksjon. Etter hvert som vår forståelse økte, var det naturlig at vi slo sammen og endret navn på kategoriene. Enkelte uttalelser fra informanter er gjengitt, for å øke sporbarhet, gjennomsiktighet og validitet for studien (se også underkapittel 2.4).

Tabell 2.1 Oversikt over analysestegene vi har gjennomført for å utarbeide vårt forslag til Forsvarets moderne og motstandsdyktige digitale grunnmur. Første kolonne angir stegnummer og andre kolonne angir hvordan vi har gått fram i analysearbeidet.

2.3.3 Kritiske suksessfaktorer for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur

Begrepet kritiske suksessfaktorer (KSF) ble opprinnelig introdusert av Rockart (1979). KSF-ene representerer faktorer en organisasjon må håndtere tilfredsstillende for å nå sine mål (Anthony et al., 1972; Fuglseth, 1989), og varierer fra organisasjon til organisasjon. KSF-ene kan også være generiske, hentet fra litteraturen, eksempelvis «toppledelsesstøtte» og «effektiv kommunikasjon» (Elstad et al., 2009; Snider et al., 2009).

Datagrunnlaget for vår KSF-analyse er gruppesamtalene med forsvarssektoren, den andre workshopen, dokumentene listet i underkapittel 2.2.5 i tillegg til resultatene fra kapittel 5 i denne rapporten. Tabell 2.2 viser stegene vi har gjennomført i vår dataanalyse for å komme fram til KSF-ene.

STEG	ANALYSEAKTIVITET
1	Gruppesamtalene med forsvarssektoren og andre workshop var det empiriske datagrunnlaget for KSF-analysen (dvs. de seks fellesdokumentene, beskrevet i steg 1, tabell 2.1).
2	I første del av KSF-analysen leste vi gjennom fellesdokumentene, analyserte og kopierte tekst inn i hovedkategorier. Disse hovedkategoriene var kandidater til å bli KSF-er. Ved behov ble tekst flyttet mellom hovedkategoriene. Innholdet i hver hovedkategori ble deretter gruppert i underkategorier basert på temaer. Vi utformet abstrakte navn på hoved- og underkategoriene basert på innholdet i hver kategori. De abstrakte navnene på KSF-ene ble inspirert av eksisterende litteratur og tidligere

STEG	ANALYSEAKTIVITET
	forskning ved FFI. Analyseresultatene, dvs. hovedkategoriene, dannet utgangspunktet for den videre KSF-analysen.
3	Neste steg i KSF-analysen var å analysere på tvers av de foreslåtte hovedkategoriene (steg 2 i denne tabellen) og analysen av Forsvarets moderne og motstandsdyktige digitale grunnmur (beskrevet i tabell 2.1). Dette steget inkluderte også en data-reduksjon, siden analysen på tvers avdekket at enkelte av hovedkategoriene ikke var relevante. Analysen avdekket også behov for en KSF som ikke var dekket av hoved-kategoriene. Vi la derfor til én KSF, behov for en tilpasningsdyktig digital grunnmur.
4	Vi skrev deretter et sammendrag for hver foreslåtte KSF. Basert på disse sammen-dragene ble det foretatt en ny datareduksjon hvor KSF-er ble slått sammen, slettet eller endret grunnet bedret forståelse for kategoriene.

Tabell 2.2 Oversikt over analysestegene som er gjennomført for å komme fram til kritiske suksessfaktorer for å oppnå og opprettholde Forsvarets moderne og motstands-dyktige digitale grunnmur. Første kolonne angir stegnummer og andre kolonne angir hvordan vi har gått fram i analysearbeidet.

2.4 Ivaretakelse av studiens validitet og reliabilitet

«Beskrivende validitet» handler om å rapportere fakta så riktig og nøyaktig som mulig og kan forklares som «[…] *the factual accuracy of the account as reported by the researchers*» (Johnson, 1997, s. 284). Så langt det lar seg gjøre, er det ønskelig å være flere forskere til stede under datainnsamlingen. Under datainnsamlingen var derfor alle forskerne som utførte studien til stede. En slik strategi kalles forskertriangulering (Johnson, 1997). Ved at flere forskere er til stede, økes den beskrivende validiteten. Forskerne har både underveis i og i etterkant av data-analysen, benyttet muligheten til å kryssjekke og diskutere funn seg imellom. Nøyaktigheten i det som beskrives, kan øke gjennom slike typer diskusjoner om hva som faktisk skjedde.

«Fortolkende validitet» handler om å utvikle et «vindu» for å forstå tankesettet og perspektivene til informantene (Johnson, 1997) og kan forklares som «[…] *accurately portraying the meaning attached by participants to what is being studied by the researcher*.» (Johnson, 1997, s. 285). Fortolkende validitet søkes i denne studien ivaretatt ved bruk av direkte sitater og bruk av felt-notater fra gruppesamtaler og workshops.

Det ligger en grunnleggende fare for forskerskjevhet, ved at forskeren selektivt observerer og tolker data utfra eget syn og ikke utfra forskningsobjektenes opprinnelige mening og intensjon (Johnson, 1997). I dette ligger en refleksjon rundt hvordan personlig bakgrunn kan påvirke forskningen og hvilke strategier forskeren legger til grunn for å adressere problemet. For eksempel kan en forsker tolke tankesettet til informantene mer likt eller ulikt eget syn enn det som faktisk er tilfellet. Ett av tiltakene som er gjennomført i studien for å motvirke forskerskjevhet, er at forskerne aktivt har reflektert rundt egen objektivitet og egne predisposisjoner (egen forutinntatthet) ved notering og tolkning av data.

Det har også vært etablert en referansegruppe for studien, bestående av forskere og ledere ved FFI. Møter har vært avholdt månedlig for sjekk av innhold og progresjon. Referansegruppa har kommet med nyttige innspill underveis, og dermed bidratt til studiens validitet.

Reliabilitet[12] innen eksplorative forskningsdesign er utfordrende. Dette er også tilfellet for vår forskning. Ved bruk av workshops og samtaler som datainnsamlingsteknikker er det samtalen og deltakerne som styrer datainnsamlingen, og datainnsamlingen blir kontekstavhengig (jf. Ghauri & Grønhaug, 2005). Ved en eksplorativ forskningstilnærming bruker også forskeren seg selv som instrument, både under datainnsamling og fortolkningsprosessen av data. Personer har ulik erfaringsbakgrunn, og vil derfor tolke data ut fra forskjellige preferanser. Det kan derfor være vanskelig for andre forskere å forstå fortolkningsprosessen av andres data (Johannessen et al., 2004). Gjennom dette kapittelet – metodiske betraktninger – har vi styrket studiens reliabilitet. Vi har beskrevet forskningsprosessens framgangsmåte, og en slik beskrivelse gir en sporbarhet og gjennomsiktighet i hvordan studiens dataanalyse er gjennomført.

[12] Reliabilitet vil si studiens pålitelighet.

3 Rammeverk for et helhetlig perspektiv

Dette kapittelet beskriver teori samt vårt rammeverk for et helhetlig perspektiv på den digitale grunnmuren. Rammeverket vil kunne benyttes i en rekke ulike sammenhenger. I denne rapporten bruker vi det for å beskrive Forsvarets digitale grunnmur i dag, og for å beskrive Forsvarets moderne og motstandsdyktige digitale grunnmur.

3.1 Sosioteknisk systemteori

En organisasjon består av en rekke elementer som påvirker, og er gjensidig avhengig av, hverandre. Systemteori er en tilnærming for å beskrive organisasjoner og deres kompleksitet. Overordnet er et system «en helhet sammensatt av deler (elementer) som det finnes visse relasjoner mellom» (Bush et al., 2010, s. 55–56). Et element kan være enkeltpersoner, grupper, eller prosesser og prosedyrer. Mellom elementene eksisterer det en form for relasjon eller forbindelse. Delsystemer dannes av elementene og deres relasjoner. Det eksisterer også relasjoner mellom ulike delsystemer. Elementene i systemet er avhengige av hverandre for å fungere, og egenskapene og oppførselen til disse elementene er bestemt av samspillet med resten av systemet. I et system vil det eksistere mange relasjoner mellom ulike elementer, og ulike delsystemer vil være vevd sammen. Det vil dermed være vanskelig, om ikke umulig, å få fullstendig oversikt over alle sammenhenger i et system (Bush et al., 2010, s. 57).

Det eksisterer en grense mellom elementer som ligger i systemet og elementer som tilhører systemets omgivelser. Det skjer også en utveksling mellom systemet og dets omgivelser (Bush et al., 2010, s. 55–56). Denne problemstillingen kommer vi nærmere inn på i underkapittel 3.9.

Systemet vi studerer er Forsvarets moderne og motstandsdyktige digitale grunnmur.

Vårt rammeverk bygger på sosioteknisk systemteori (se f.eks. Davis et al., 2014; Leavitt, 1965; Lyytinen & Newman, 2008). I et sosioteknisk system ses det i helhet på de sosiale og tekniske systemene, og samspillet mellom disse. De sosiale og tekniske systemene er i et slikt perspektiv gjensidig avhengig av hverandre. Den sosiale delen av systemet omhandler blant annet mennesker i organisasjonen, og det samspillet som foregår mellom disse menneskene i gjennomføring av verdiskapende virksomhetsprosesser for organisasjonen. Det tekniske systemet omhandler teknologiske løsninger og måten disse er koblet og fungerer sammen på.

Det er de abstrakte interaksjonene mellom de to systemene – det sosiale og det tekniske – som vektlegges ved en sosioteknisk tankegang (Sony & Naik, 2020). For eksempel vil ikke det å studere en teknologi i isolasjon gi et helhetlig perspektiv på et system. Det er interaksjonen mellom mennesker, prosesser og teknologier, som får fram samspillet og ser helhet på tvers av enkeltelementer (Sony & Naik, 2020).

3.1.1 Leavitts rammeverk

Et hyppig sitert rammeverk for organisasjonsendring innen sosioteknisk systemteori er utarbeidet av Leavitt (1965). Rammeverket tar utgangspunkt i fire faktorer som til sammen representerer en organisasjon, nemlig «organisasjonsstrukturen», «oppgavene som skal utføres», «menneskene som utfører disse oppgavene» og «teknologien som benyttes».

Digitalisering er et eksempel på organisasjonsendring. Digitaliseringen omhandler teknologifaktoren i form av nye teknologiske løsninger, men også de andre faktorene. Menneskene i organisasjonen må lære seg nye måter å arbeide på. Arbeidsoppgaver blir endret som følge av digitalisering. Hver av faktorene har innvirkning på utfallet, og det eksisterer en gjensidig avhengighet mellom faktorene. Gjennom digitalisering bruker organisasjoner teknologier for å forbedre eksisterende virksomhetsprosesser og koordinering mellom dem (Verhoef et al., 2021).

Det kan imidlertid skje at en av faktorene blir inkompatibel med andre faktorer, og det kan dermed oppstå et gap mellom faktorene i rammeverket. Dersom det eksisterer ulike gap, vil dette kunne redusere det sosiotekniske systemets ytelse og levedyktighet (Lyytinen & Newman, 2008). For sammenhengen mellom oppgaver og teknologi, kan det for eksempel eksistere et gap ved at teknologien ikke er tilstrekkelig i stand til å støtte oppgavene som skal gjøres eller at teknologien ikke er tilstrekkelig robust og redundant. I tillegg kan det være valgt feil eller utilstrekkelig teknologi, som ikke støtter opp om virksomhetsprosessene som skaper verdi for organisasjonen. For sammenhengen mellom mennesker og teknologi, kan for eksempel mennesker mangle kompetanse eller ikke akseptere teknologien. For sammenhengen mellom mennesker og struktur, kan mennesker mangle kompetanse på ulike prosesser og prosedyrer. Eksemplene er basert på Lyytinen og Newman (2008) og tilpasset studiens kontekst. Det kan også være slik at struktur og oppgaver ikke endres, og at teknologiens potensiale dermed ikke blir utnyttet.

3.1.2 Davis et al. sitt rammeverk

Leavitts rammeverk (1965) er veldefinert, teoretisk forankret og kan ved behov utvides med flere faktorer (Lyytinen & Newman, 2008). Davis et al. (2014) er et eksempel på en slik utvidelse, hvor rammeverket til Leavitt er utvidet fra fire til seks faktorer. I tillegg endret Davis et al. (2014) navn på enkelte av faktorene, som vist i tabell 3.1.

I Davis et al. (2014) sitt rammeverk er det også identifisert fire rammefaktorer: interessenter, styrende dokumenter, økonomiske rammebetingelser samt lover og regler. Viktigheten av disse rammefaktorene varierer i hvert system. Disse rammefaktorene er faktorer som organisasjonen selv ikke har kontroll over – men som organisasjonen potensielt kan påvirke og bli påvirket av. Se for eksempel Münch et al. (2022), Roth og Farahmand (2023) og Sony og Naik (2020), som anvender rammeverket til Davis et al. (2014).

LEAVITT (1965)	DAVIS ET AL. (2014)	EKSEMPLER FRA DAVIS ET AL. (2014)
Organisasjonsstruktur	Mål	• Ikke tilfredsstillende prioritering av mål
Oppgaver	Prosesser og prosedyrer	• Manglende koordinering og kommunikasjon • Dårlig kommando og kontroll • Manglende fleksibilitet • Manglende planleggingsprosesser
Mennesker	Mennesker	• Manglende sluttbrukerinvolvering • Manglende kompetanse og opplæring • Manglende tverrfaglige innspill • Manglende forståelse for roller og ansvar
	Kultur	• Rigid lederstil • Dårlig forhold mellom aktører • Ikke tilfredsstillende innstilling (*mindset*) • Tar ikke læring
Teknologi	Teknologi	• Feil på ny teknologi eller programvare • Manglende testing
	Bygninger/ infrastruktur[13]	• Manglende sikring • Ikke tilfredsstillende layout på infrastruktur

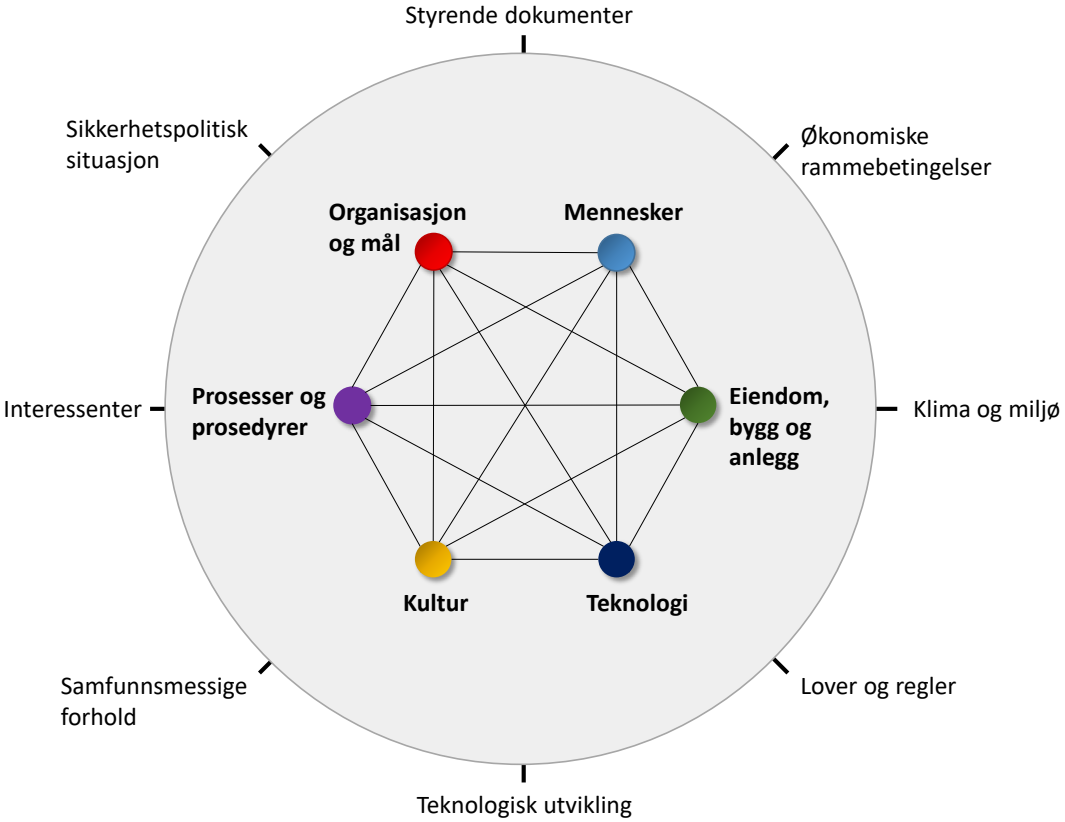
Tabell 3.1 Første og andre kolonne indikerer en sammenlikning av Leavitts (1965) og Davis et al. (2014) sitt rammeverk. Tredje kolonne viser eksempler fra Davis et al. (2014) på ulike uheldige momenter, innenfor hver faktor, som påvirker det sosiotekniske systemet negativt.

3.2 Vårt rammeverk

Vi har valgt å bygge vårt rammeverk på Davis et al. (2014) og tilpasset det til bruk for et helhetlig perspektiv på Forsvarets moderne og motstandsdyktige digitale grunnmur. Vårt rammeverk vises i figur 3.1.

Teknologien i den digitale grunnmuren er ikke en tilstrekkelig betingelse for at grunnmuren skal bli moderne og motstandsdyktig. Forsvaret må også være i stand til å gjøre de riktige tingene, i sine virksomhetsprosesser. Teknologien i den digitale grunnmuren er ikke en verdifull ressurs isolert sett. Det er hvordan faktorene fra vårt rammeverk håndteres i en helhet som bidrar til verdi for Forsvaret.

[13] Infrastruktur her er koblet til bygningsmessig infrastruktur, og ikke til infrastruktur slik den er definert i DRP.



Figur 3.1 Vårt rammeverk for et helhetlig perspektiv, basert på Davis et al. (2014, s. 173). De seks elementene inni sirkelen er faktorer Forsvaret selv kan påvirke, mens de på utsiden er rammefaktorer.

Faktorene vi har valgt å beholde uendret fra Davis et al. (2014) er: «teknologi», «prosesser og prosedyrer», «kultur» og «mennesker». Årsaken til at vi velger å beholde disse, er at dette er faktorer som er gjenkjennbare og relevante for Forsvaret.

Vi har valgt å utvide faktoren «mål» hos Davis et al. (2014) til også å inkludere «organisasjon». Faktoren, «organisasjon og mål», vil dermed omhandle den formelle delen av organisasjonen, inkludert organisasjonskart og IKT-styringsmodell. Vi ønsker å synliggjøre faktorer ved den formelle delen av organisasjonen på linje med «prosesser og prosedyrer», som speiler hvordan ting gjøres i praksis. I tillegg omfatter denne faktoren også de formelle målene Forsvaret har vedtatt.

Vi har valgt å endre navn på faktoren «bygninger/infrastruktur» fra Davis et al. (2014) til «eiendom, bygg og anlegg (EBA)», for å unngå misforståelser knyttet til infrastrukturbegrepet. EBA-faktoren inkluderer de fysiske installasjonene som benyttes av Forsvaret, og eventuelt av sivile leverandører, for å huse den fysiske IKT-infrastrukturen som inngår i den digitale grunnmuren.

Tabell 3.2 viser hva vi legger i de ulike faktorene i rammeverket vårt:

FARGE	FAKTOR	FORKLARING
	Organisasjon og mål	Omhandler den formelle delen av organisasjonen, dvs. organisasjonsstruktur og styringsmodell, inkludert roller, ansvar og myndighet. I tillegg inngår mål fra styrende dokumenter som organisasjonen selv har kontroll over, som f.eks. mål fra strategier og reguleringsplaner.
	Mennesker	Omhandler individene som arbeider i organisasjonen, f.eks. individets kompetanse og aksept for endring.
	Eiendom, bygg og anlegg	Omhandler de fysiske installasjonene Forsvaret og ev. sivile leverandører benytter for å huse den fysiske IKT-infrastrukturen som inngår i den digitale grunnmuren.
	Teknologi	Omhandler maskin- og programvare som tilbyr et sett med IKT-tjenester (IT-plattform, infrastruktur og kommunikasjon), og hvordan disse er koblet og fungerer sammen.
	Kultur	Omhandler momenter knyttet til en felles opplevelse av tilhørighet og fellesskap, f.eks. felles mønstre av meninger og holdninger som gir seg utslag i bestemte handlingsmønstre.
	Prosesser og prosedyrer	Omhandler organisasjonens verdiskapingsprosesser (aktiviteter). Disse gjennomføres av enkeltpersoner, i grupper, på tvers av grupper og/eller ved hjelp av IKT for å nå organisasjonens mål. En prosedyre er en mer detaljert beskrivelse av én eller flere aktiviteter som gjennomføres i en verdiskapingsprosess.

Tabell 3.2 Oversikt over hva som inngår i de ulike faktorene i vårt rammeverk. Første kolonne viser fargen for hver faktor. Andre kolonne angir navnet på faktoren. Tredje kolonne beskriver hva vi legger i hver faktor.

Våre rammefaktorer vises utenfor den grå sirkelen i figur 3.1 og inneholder både Davis (2014) sine fire rammefaktorer og våre egne rammefaktorer som er lagt til for å dekke denne studiens behov. Forsvarets rammefaktorer er annerledes enn mange andre organisasjoners rammefaktorer. Det er derfor behov for å legge til rammefaktorer som sikkerhetspolitisk situasjon og samfunnsmessige forhold i vårt rammeverk. Vi har valgt å støtte oss på Skjelland et al. (2022, 2023) som identifiserer utviklingstrekkene «sikkerhetspolitisk situasjon», «samfunnsmessige forhold», «teknologisk utvikling» og «klima og miljø» som til sammen utgjør Forsvarets viktigste rammefaktorer. Rammefaktorer blir beskrevet i underkapittel 3.9.

Underkapittel 3.3–3.8 beskriver de seks faktorene i rammeverket vårt mer i detalj, og vi knytter dem mot relevant teori. Videre viser vi hvordan de ulike faktorene kan påvirke hverandre. I tillegg setter vi dem inn i en kontekst som er relevant for den digitale grunnmuren.

3.3 Organisasjon og mål

I vårt rammeverk omhandler «organisasjon» den formelle delen av organisasjonen, det vil si organisasjonsstruktur og IKT-styringsmodell. Organisasjonsstruktur forstås som organisasjonens formelle hierarkiske struktur, og om organisasjonen kan oppfattes å være flat eller hierarkisk ut fra antallet nivåer i hierarkiet (se f.eks. Volberda, 1998). En utflating av organisasjonens hierarkiske struktur kan knyttes til økt fleksibilitet, raskere og bedre informasjonsdelings- og beslutningstakningsprosesser (Alberts & Hayes, 2003, 2007; Bjørnstad & Lichacz, 2013).

For å oppnå effektiv samhandling, er det sentralt at det er færrest mulig hindre for denne samhandlingen. «Et hinder er en omstendighet eller ting som hemmer informasjonsdelingen i en eller annen form» (Elstad, Lund, et al., 2022, s. 20). Det kan eksistere hindre både prosessuelt, teknologisk og organisatorisk (Elstad, Lund, et al., 2022). Prosesser forstås som hvordan strukturen er implementert i form av samhandlings-, ledelses- og beslutningstakningsprosesser (jf. DeSanctis & Poole, 1997). Organisatoriske hindre for informasjonsdeling omhandler den formelle delen av organisasjonen, som organisasjonskartet og fordeling av roller, ansvar og myndighet i henhold til dette. I en formell hierarkisk struktur må roller, ansvar og myndighet fordeles på de ulike nivåene i hierakiet, gjennom en IKT-styringsmodell.

> Styringsmodellen definerer et sett aktiviteter, prinsipper, standarder og mål […] utviklet for å sikre effektiv og sikker bruk av teknologi i virksomheten. Styringsmodellen skal sikre ansvarliggjøring av de riktige delene av virksomheten og støtte gode og riktige beslutninger for IKT på tvers av virksomheten. Dette gjøres gjennom å definere hvem som tar avgjørelser, hvordan de blir tatt, og hvorfor de blir tatt gjennom retningslinjer og tilegning av ansvar og myndighet. (Forsvarsdepartementet, 2019a, vedlegg C.1)

Fleksibilitet eller smidighet vil si organisasjonens evne til å tilpasse seg omgivelsenes komplekse og uforutsigbare krav (Hatum & Pettigrew, 2006). Smidige utviklingsmetoder kan ses i sammenheng med fleksibilitet, der mål og effekter ønskes oppnådd innenfor gitte rammer. Fleksibilitet er ikke kun knyttet til organisasjonens evne til fleksibilitet, men også til teknologiens evne til å tilpasse seg varierende og nye behov (jf. Wixom & Todd, 2005). Det vil med andre ord si at både «organisasjon og mål», «prosesser og prosedyrer» – og dermed også «mennesker» og «kultur» – samt «teknologi» må ha evnen til å håndtere fleksibilitet.

Videre inkluderer denne faktoren i rammeverket organisasjonens «mål» – som inngår i styrende dokumenter organisasjonen selv har kontroll over. Sett i kontekst av denne studien omhandler det mål for Forsvaret knyttet til den digitale grunnmuren.

«Mål» er tett knyttet til de andre faktorene. I en rasjonell idealmodell vil beslutningstaker (menneskefaktoren) alltid sette de riktige målene og alltid velge det beslutningsalternativet som er mest egnet for å nå målene (se f.eks. Bush et al., 2010; Fardal & Elstad, 2020; March, 1994). Det vil si at ved en rasjonell idealmodell vil Forsvaret alltid sette de riktige målene og velge de riktige beslutningsalternativene for den digitale grunnmuren. For at Forsvaret skal være i stand

til dette, må all informasjon være tilgjengelig om alle mulige løsninger og konsekvenser av disse (se f.eks. Bush et al., 2010; Fardal & Elstad, 2020; March, 1994). En rasjonell idealmodell er ikke oppnåelig. Ulike momenter vil påvirke beslutninger:

- tid, kognitive begrensninger og mangelfull informasjon (Simon, 1957, 1964)
- opportunisme og uklare mål (Allison, 1971; Cyert & March, 1963; Cyert & March, 1992)
- følelser, usikkerhet, erfaring og gruppedynamikk (Das & Teng, 1999; Stacey, 2007)

Listen viser flere momenter fra menneskefaktoren som påvirker faktoren «organisasjon og mål», for eksempel følelser og usikkerhet. I tillegg viser listen momenter fra kulturfaktoren, som gruppedynamikk. Faktoren «organisasjon og mål» er også knyttet til faktoren «prosesser og prosedyrer», med tanke på gjennomføring av beslutningsprosesser i praksis. I organisasjoner med uklare roller og ansvarsområder, kan problemer bli liggende og flyte, og ingen av aktørene tar ansvar for beslutningene. Uløste problemer beslaglegger ressurser – knyttet til faktorene «mennesker» og «prosesser og prosedyrer» – og «endeløse» diskusjoner foregår. Problemene møter ikke en akseptabel løsning, og beslutninger blir betraktet som en tilfeldig prosess (Bush et al., 2010; Fardal & Elstad, 2020).

3.4 Teknologi

«Teknologi» inngår som en faktor i vårt rammeverk. Som vi beskrev i kapittel 1 er en digital grunnmur fra et teknologisk perspektiv en samling av maskinvare og programvare som tilbyr et sett av IKT-tjenester. I dette kapittelet viser vi først til hvordan DRP beskriver den digitale grunnmuren i sitt grunnlagskart. Deretter viser vi hvordan grunnmuren kan beskrives gjennom Natos C3-taksonomi (Nato, 2021), som DRP sitt grunnlagskart tar utgangspunkt i.

3.4.1 Digital grunnmur i henhold til DRP

DRP (Forsvarsstaben, 2023) består i hovedsak av tre deler – (1) DRP-grunnlagskart for forsvarssektorens IKT, (2) åtte IKT-innsatsområder[14] med mål for årene 2024, 2026 og 2028 og (3) ti prinsipper for regulering av IKT-utvikling, -drift og -forvaltning. DRP-grunnlagskartet benytter et organisasjonsperspektiv, mens resten av DRP i hovedsak må sies å ha et teknologi-perspektiv. Denne første versjonen av DRP (fra 2023) inneholder ikke detaljerte veikart, men inkluderer en prioritering av de åtte IKT-innsatsområdene over ulike tidsperioder, og denne prioriteringen utgjør en form for overordnet veikart.

DRP-grunnlagskartet er basert på begreper og fargekoding fra Natos C3-taksonomi (Nato, 2021). Vi finner begrepet digital grunnmur i dette kartet, i tillegg til applikasjoner[15] og tjenest-

[14] De åtte innsatsområdene er: (1) helhetlig kommando og kontroll (K2), samvirke med allierte og totalforsvaret, (3) IKT-integrerte kamplattformer, sensorer, effektorer og beslutningstagere, (4) dele og utnytte informasjon og data, (5) tidsriktige og relevante applikasjoner og tjenester, (6) moderne og motstandsdyktig digital grunnmur, (7) konsolidering og utfasing og (8) forsvarlig sikkerhetsnivå.

[15] En applikasjon er et dataprogram som kjøres for å løse oppgaver for eller gi informasjon til en bruker (Store norske leksikon (2005–2007)).

er[16]. DRP sin digitale grunnmur består av IT-plattform (primært operativsystem og en del felles IKT-tjenester), infrastruktur (f.eks. lagring og prosessering) og kommunikasjon (f.eks. fibernett og radiokommunikasjonssystemer). I tillegg er krypto gjennomgående, det vil si at krypto-tjenester finnes både i digital grunnmur og i applikasjoner og tjenester. EBA og utstyr finnes også både i digital grunnmur og i applikasjoner og tjenester.

Helhetlig arkitektur, sikkerhet, management og drift vises også på grunnlagskartet. Begrepet *management* kan omtrentlig forstås som styring og kontroll av IKT-systemer[17]. Innen infrastrukturtjenester og IT-plattform benyttes i dag ofte begrepet orkestrering som innebærer å håndtere sammensetningen av og livssyklusen til programvaren som inngår. Dette inkluderer installasjon av programvaren og å sikre at den til enhver tid kjører. Videre håndteres skalering opp og ned etter belastning, det vil si at antallet instanser av programvaren varieres etter antallet brukere. Til slutt sørges det også for lastbalansering, som innebærer å flytte kjørende programvare mellom maskiner for å sikre at maskinene har noenlunde lik belastning. Et av de mest kjente orkestreringsrammeverkene er Kubernetes (for flere detaljer se Kubernetes, u.d.). En pågående trend er at kommunikasjonstjenester bygges opp med skyteknologi, og også her benyttes begrepet orkestrering (Mykkeltveit & Fongen, 2020). IKT-tjenester for styring og kontroll av digital grunnmur er en del av den digitale grunnmuren, mens applikasjonstjenestene normalt vil ha egne IKT-tjenester for styring og kontroll.

Vi benytter begrepet «styring og kontroll» for *management* og orkestrering av den digitale grunnmuren.

3.4.2 Natos C3-taksonomi

DRPs grunnlagskart tar utgangspunkt i Natos C3-taksonomi. I figur 3.2 viser vi de delene av taksonomien som helt eller delvis omfattes av digital grunnmur. Vi har lagt på en illustrasjon av digital grunnmur i henhold til DRP (IT-plattform, infrastruktur og kommunikasjon). Dette gjør det mulig å gi en grov oversikt over hvilke typer IKT-tjenester som vil være inkludert i henholdsvis IT-plattform, infrastrukturtjenester og kommunikasjonstjenester, og dermed i en digital grunnmur.

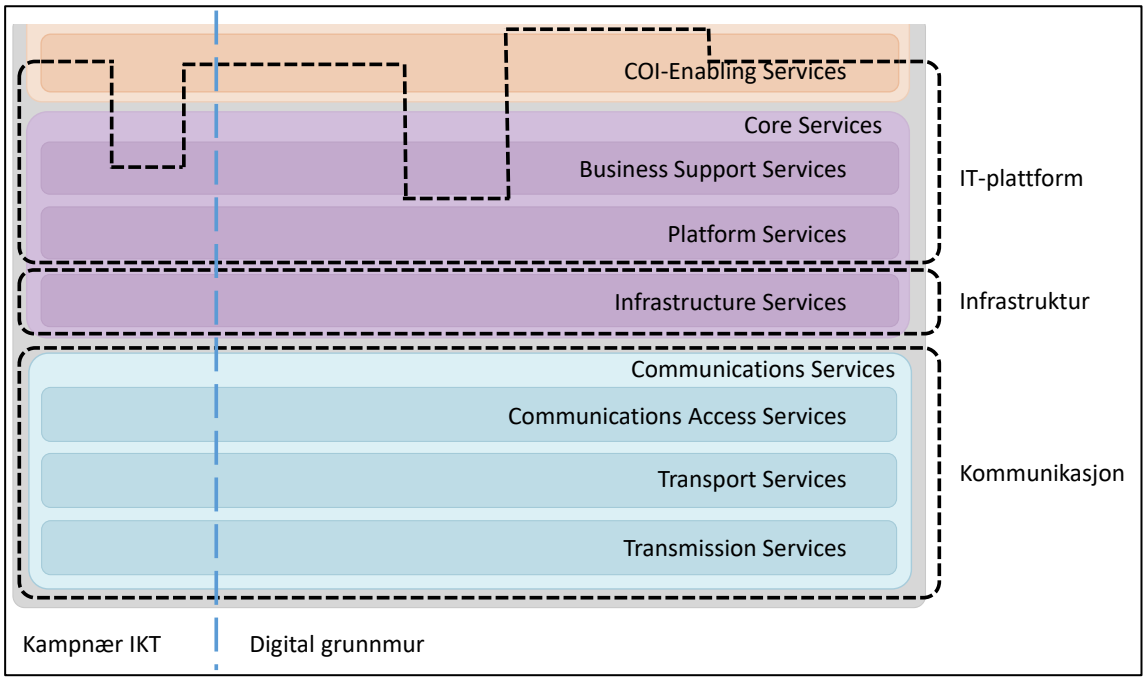
Som figur 3.2 viser er kommunikasjonstjenester (*Communications Services*) og infrastrukturtjenester (*Infrastructure Services*) i sin helhet inkludert i digital grunnmur. For IT-plattform er det derimot bare *Platform services* som i sin helhet inngår i IT-plattformlaget av digital grunnmur. For *Business Support Services* og *Community of Interest* (COI)-*Enabling Services* angir

[16] En IKT-tjeneste kan beskrives som en funksjon som leveres av programvare (Laskey et al., 2009). Mens en applikasjon er rettet spesifikt mot brukere er ikke dette nødvendigvis tilfelle for en IKT-tjeneste – den kan også levere funksjonen til annen programvare.
[17] Et IKT-system er den teknologiske delen av et informasjonssystem (definert i Nasjonal sikkerhetsmyndighet, 2020a), og innbefatter dermed både den digitale grunnmuren og applikasjonene og IKT-tjenestene som kjører på den.

avgrensningen at slike tjenester kan være en del av grunnmuren, eller de kan være applikasjonstjenester.

> Vi benytter begrepet applikasjonstjeneste om applikasjoner og programvare som kjører på, og bruker IKT-tjenestene fra, den digitale grunnmuren.

Nøyaktig hvilke IKT-tjenester innenfor *Business Support* og *COI-Enabling Services* som tilhører den digitale grunnmuren, vil variere med behov og etter hva som er hensiktsmessig.



Figur 3.2 IKT-tjenester som er inkludert i digital grunnmur (basert på Nato, 2021).

I tillegg til denne horisontale avgrensningen gjør vi også en vertikal avgrensning i denne studien, illustrert med blå stiplet linje i figur 3.2. Denne linjen illustrerer avgrensningen mot kampnær IKT[18], som nevnt i underkapittel 1.3.

3.5 Eiendom, bygg og anlegg

EBA inngår som en faktor i et helhetlig perspektiv på digital grunnmur. Med EBA sikter vi til de fysiske installasjonene som benyttes av Forsvaret og eventuelt av sivile leverandører for å huse utstyr knyttet til IT-plattformer, infrastrukturtjenester og kommunikasjonstjenester som inngår i digital grunnmur.

[18] For flere detaljer, se Bloebaum et al. (under arbeid).

I vårt rammeverk inkluderer EBA bygningsmessig infrastruktur, tilkobling til annen infrastruktur, som strøm- og vannforsyning, samt fysisk sikring av disse dersom det er påkrevd. Noen av nettverkene som leverer kommunikasjonstjenester, eksempelvis 4G eller 5G mobiltjenester og satellittkommunikasjon, tilhører sivile leverandører. I tillegg leverer sivile aktører skytjenester med tilhørende datasentre. Dermed er deler av sivil EBA relevant for den digitale grunnmuren.

3.6 Prosesser og prosedyrer

Faktoren «prosesser og prosedyrer» i vårt rammeverk omhandler organisasjonens verdiskapingsprosesser. Slike verdiskapingsprosesser består av ulike former for aktiviteter, som gjennomføres for å nå organisasjonens mål. I vår studie er det verdiskapingsprosesser knyttet til den digitale grunnmuren som er relevant. Aktivitetene i disse prosessene kan gjennomføres av enkeltpersoner, grupper, på tvers av grupper eller ved hjelp av IKT. En prosedyre er en detaljert beskrivelse av én eller flere aktiviteter som gjennomføres i en verdiskapingsprosess. Standard eller stående operasjonsprosedyre (SOP) er et eksempel på en prosedyrebeskrivelse i Forsvaret. Interne prosesser ved et hovedkvarter reguleres gjerne i de stående operasjonsprosedyrene, og inkluderer framgangsmåte og steg som skal gjennomføres i aktiviteten (Forsvaret, 2019, s. 194).

3.6.1 Virksomhetsprosesser

En representasjon av overordnede virksomhetsprosesser som skaper verdi, blir beskrevet som en organisasjons verdikjede. Verdiskapingsprosesser kan beskrives gjennom primæraktiviteter, som er de aktivitetene i en organisasjon som skaper direkte verdi (Barney, 2002). I Forsvaret kalles disse primæraktivitetene for Forsvarets kjernevirksomhet. Primæraktivitetene er strategisk viktige aktiviteter, eller aktiviteter nært tilknyttet til disse, som med mangelfull utføring vil få store konsekvenser for organisasjonen. Et eksempel på primæraktivitet for Forsvaret er å hevde norsk suverenitet, som inngår som én av Forsvarets ni oppgaver (Forsvarsdepartementet, 2020a).

Støtteaktivitetene er de aktivitetene som er nødvendige forutsetninger for at primæraktivitetene kan skape verdi (Barney, 2002), for eksempel ulike former for anskaffelser. Støtteaktivitetene i Forsvaret omtales gjerne som tilretteleggende virksomhet.[19]

Den digitale grunnmuren benyttes i hele spennet av virksomhetsprosesser som Forsvaret gjennomfører, fra tilretteleggende virksomhet til utførelse av Forsvarets kjernevirksomhet. Det kan være vanskelig å skille ut den digitale grunnmuren fra selve gjennomføringen av en aktivitet, slik at den «blir en nødvendig betingelse for at Forsvaret kan være i stand til å utføre aktiviteter som en del av kjernevirksomheten» (Elstad, Endregard, et al., 2022, s. 11).

Forsvarssektoren har de senere årene gitt mer oppmerksomhet til porteføljestyring (Presterud et al., 2022). Porteføljestyring handler om å «definere, balansere og styre sin samlede portefølje av

[19] Avsnittet er gjengitt fra Elstad, Endregard & Mykkeltveit (2022).

prosjekter og programmer på en slik måte at strategiske mål nås og ressursene utnyttes best mulig.» (Bukkestein et al., 2021, s. 19). Porteføljestyring er derfor en virksomhetsprosess for Forsvaret og for oppnåelsen og opprettholdelsen av Forsvarets moderne og motstandsdyktige digitale grunnmur. Forsvarsstaben var i 2023 i gang med å implementere en ny IKT-porteføljemodell, som deler Forsvarets IKT inn i tre hovedområder: operasjoner, virksomhetsstyring og digital grunnmur (Forsvarsstaben, 2023). Hovedområdene speiler til en viss grad inndelingen i kjernevirksomhet og tilretteleggende virksomhet, hvor operasjoner inngår som en del av kjernevirksomheten, og virksomhetsstyring og digital grunnmur tilrettelegger for gjennomføringen av Forsvarets kjernevirksomhet.

3.6.2 Endringsledelse

I kapittel 4 kommer vi inn på flere utfordringer for dagens digitale grunnmur. For å løse disse utfordringene kreves det en eller annen form for endringsprosesser. Skal Forsvaret kunne oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur vil IKT-virksomheten måtte gjennomgå endringer, potensielt både strukturelt og prosessuelt. Lewin (1952) er én av grunnleggerne for en prosessmodell som kan benyttes for slike typer organisasjonsendringer. Modellen er enkel av natur, men kan likevel være nyttig som en påminnelse av hvilke overordnede faser en organisasjonsendring innebærer. Modellen består av tre faser som vist i figur 3.3.

Figur 3.3 Prosessmodell for organisasjonsendring. Kilde: Lewin (1952).

Den første fasen, opptining, handler om å etablere en forståelse blant de ansatte for endringen. I denne fasen handler det om at lederne gjør de ansatte klare for endringen og etablerer en forståelse for hvilke virksomhetsprosesser som skal forandres og hvorfor. Sett i kontekst av denne studien, er Forsvaret i denne fasen nå. For Forsvarsstaben handler det om å gjøre de ansatte i IKT-virksomheten klare for organisasjonsendringene som må til for å oppnå en moderne og motstandsdyktig digital grunnmur.

Organisasjonen utarbeider i den første fasen mål for endringene, som lederne kommuniserer til de ansatte – inkludert intensjonen for endringene. For de virksomhetsprosessene som gjennomgår en endring, bør organisasjonen utarbeide en beskrivelse av hvordan intendert gjennomføring av disse virksomhetsprosessene er tenkt. Intendert gjennomføring av virksomhetsprosessene er en standard eller norm for hvordan de ansatte skal gjennomføre prosesser som er berørt av endringen (Elstad, Lund, et al., 2022; Lillestøl, 1994). En slik beskrivelse må være helhetlig (basert på mål), og omhandle intensjonen (bakgrunn) og den forventede gjennomføring av virksomhetsprosessene som er påvirket av endringen.

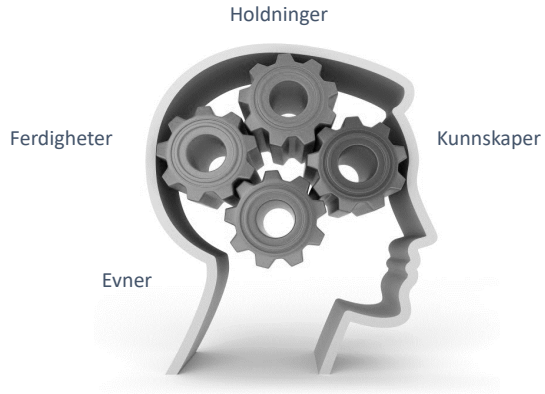
Den andre fasen handler om selve overgangen til en ny tilstand, det vil si oppnåelsen av en moderne og motstandsdyktig digital grunnmur. I denne andre fasen vil Forsvaret gjennomføre flere tiltak for å oppnå en slik grunnmur. Forslag til innhold i Forsvarets moderne og motstandsdyktige digitale grunnmur beskriver vi i denne rapportens kapittel 5.

Den tredje fasen handler om å opprettholde endringen, ved at prosesser og prosedyrer gjennomføres som intendert. For eksempel handler det om at menneskene, kulturen, prosessene og prosedyrene støtter opp om en opprettholdelse av Forsvarets moderne og motstandsdyktige digitale grunnmur. Kritiske suksessfaktorer for å oppnå og opprettholde denne grunnmuren presenterer vi i kapittel 6 i denne rapporten.

3.7 Mennesker

Med faktoren «mennesker» i vårt rammeverk mener vi individene som arbeider i organisasjonen. I vår kontekst vil det i all hovedsak si personell innenfor IKT-virksomheten. I denne faktoren er det et individperspektiv, mens kulturfaktoren (underkapittel 3.8) har et gruppeperspektiv.

For vår studie er individets kompetanse relevant. I denne rapporten ser vi på kompetanse bestående av kunnskaper, ferdigheter, evner og holdninger (Lai, 2011, 2013), som vist i figur 3.4.



Figur 3.4 Kompetanse består av en persons kunnskaper, ferdigheter, evner og holdninger. Kilde: Elstad, Lund, et al., 2022.

Det at en person innehar en form for kunnskap vil si at vedkommende har teoretisk innsikt som er opparbeidet gjennom utdanning og erfaring (Lai, 2011; Elstad, Endregard, et al., 2022; Elstad, Lund, et al., 2022). En person kan for eksempel ha kunnskap om skyteknologi samt muligheter og konsekvenser for automatisering av drift og vedlikehold. Denne kunnskapen

> […] kobles sammen i strukturer hvor de enkelte delene er integrert med hverandre. Denne kunnskapen består både av fakta som vi har lært, og regler, prinsipper og strategier som benyttes i læringsprosessen. Når vi går inn i en læringssituasjon vil vi alltid ta med oss tidligere kunnskap. […] Når vi møter en ny situasjon, vil vi hente frem et men-

> talt kart som setter oss i stand til å forstå eller tolke den nye situasjonen. (Bush et al., 2010, s. 298)

Ferdigheter handler om selve gjennomføringen av atferden (Elstad, Endregard, et al., 2022; Elstad, Lund, et al., 2022), for eksempel gjennomføringen av drifts- og vedlikeholdsoppgaver av den digitale grunnmuren. Ferdigheter har en sterk kobling til kunnskap ved at en person kan lese seg til hvordan en atferd skal utføres, før de teoretiske momentene utøves gjennom en atferd.

Evner handler om personlige egenskaper og talent (Elstad, Endregard, et al., 2022; Elstad, Lund, et al., 2022), hvor noen personer har bedre forutsetninger for å gjennomføre prosesser og prosedyrer enn andre. Vi vil imidlertid ikke gå nærmere inn på evner i denne rapporten, men nevner det som en del av kompetansebegrepet en bør være klar over at eksisterer.

Holdninger er også en del av en persons kompetanse (Lai, 2011,2013). Atferdsteorier argumenterer med at holdninger leder til atferdsvalg (Davis et al., 1989; Fishbein & Ajzen, 1975; Ilie & Turel, 2020). Det vil si at en persons tanker og følelser inngår i kompetanse, eksempelvis gjennom innstilling og vilje til å benytte teknologi, for eksempel nye måter å gjennomføre drift og vedlikehold på. I tillegg kan en persons ansvars- og lojalitetsfølelse for teknologibruken inngå som en del av holdningsdimensjonen. Videre er forventninger til utfall relevant når personer bestemmer seg for å dele kunnskap eller ikke (Paroutis & Al Saleh, 2009).

En person som ikke aksepterer en endring, vil oppleve en eller annen form for motstand mot endringen. Motstand mot endring kan ses gjennom to faser: (1) den kognitive og følelsesmessige fasen, som resulterer i en beslutning om motstand, og (2) fasen med gjennomføring av selve motstandsatferden, hvor for eksempel brukeren unngår å anvende IKT-en (jf. Ferneley, & Sobreperez, 2006). Det at den kognitive og følelsesmessige fasen kan resultere i en motstandsaktivitet, er i henhold til atferdsteorier. For den første motstandsfasen er det avdekket flere årsaker til at brukeren fatter en beslutning om motstand, som lav motivasjon for endring, politisk og kulturell *deadlock* og kynisme (Ali et al., 2016).

Tidligere forskning ved FFI har indikert at hva slags type digital kompetanse en person skal inneha, er avhengig av rollen vedkommende har i organisasjonen (Elstad, Lund, et al., 2022; Elstad, Endregard, et al., 2022). En grov inndeling av digital kompetanse skiller mellom sluttbrukerkompetanse, spesialistkompetanse (for eksempel drift, utvikling og vedlikehold) samt strategisk IKT-kompetanse (Elstad, Lund, et al., 2022; Elstad, Endregard, et al., 2022).

3.8 Kultur

Kultur er et begrep vi benytter i det daglige, og det eksisterer ulike tolkninger av hva en kultur er. I denne rapporten kommer vi ikke til å diskutere kulturbegrepet i seg selv eller ulike tilnærminger til kultur, det vil bli for omfattende innenfor denne studiens tid og ressurser. I det følgende vil vi komme kort inn på hva vi legger i kultur, samt tillit og læringsfellesskap som en del av kulturen.

Som vi kommer tilbake til i kapittel 4 er det avdekket utfordringer innen kultur for nåsituasjonen til den digitale grunnmuren. Kultur inngår derfor som en del av vårt helhetlige rammeverk. Vår forståelse av kultur tar utgangspunkt i en av de mest benyttede definisjonene:

> *The culture of a group can now be defined as a pattern of shared basic assumptions learned by a group as it solved its problems for external adaption and internal integration, which has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems*. (Schein, 2004, s. 18)

Som sitatet viser, omfatter kulturen en rekke grunnleggende antakelser og ulike former for virkelighetsoppfatninger. I vårt rammeverk ser vi derfor på kultur som de felles mønstrene av meninger og holdninger, som resulterer i bestemte måter å tenke, føle og handle på (jf. f.eks. Jacobsen & Thorsvik, 2007, s. 114). Tillit, tilhørighet og fellesskap inngår i en organisasjonskultur.

Underkapittel 3.7 handlet om individuell kompetanse, det vil si hver enkelt persons kompetanse, og hvordan individene tar med seg tidligere kunnskap inn i læringssituasjonen. I dette underkapittelet ser vi læring fra et annet perspektiv – nemlig gruppenivå. På gruppenivå kan læringsfellesskap benyttes for forståelse av læring i organisasjoner (se f.eks. Ardichvili et al., 2003; Wenger, 1998; Wenger & Snyder, 2000), gjennom et sett med felles mønstre av meninger og holdninger, som resulterer i bestemte måter IKT-virksomheten velger å lære på.[20]

Læringsfellesskap kan inngå i en organisasjonskultur, hvor medlemmene har noe felles kunnskap, en følelse av en gruppeidentitet og noen overlappende verdier, i tillegg til å gjennomføre en bestemt aktivitet sammen. Læringsfellesskap er derfor relevant i forbindelse med å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur, med tanke på at dette vil kreve endringsprosesser og behov for ny kompetanse. Felles kunnskap og overlappende verdier gir bedre forutsetninger for å dele taus kunnskap om den digitale grunnmuren. Årsaken til dette er at medlemmene har innsikt i implisitte antakelser og verdier som ligger i hverandres kunnskap om grunnmuren. Felles kunnskap, gruppeidentitet og overlappende verdier legger også til rette for utvikling og vedlikehold av tillitsbaserte forhold, som igjen skaper et godt grunnlag for kunnskapsdeling (Hislop, 2013) for den digitale grunnmuren.

Tillit er allment akseptert som en kritisk faktor for at organisasjoner skal fungere, i det å muliggjøre kunnskapsdeling og gjennomføring av endringsprosesser (se f.eks. Alberts & Hayes, 2005; Atkinson & Moffat, 2005; MacKenzie, 2008). Tillit mellom personell i IKT-virksomheten er derfor en nødvendig faktor for å oppnå samarbeid om den digitale grunnmuren. Det finnes ulike former for tillit. Tillit til integritet baserer seg på troverdigheten til fellesskapets omdømme og konsistensen til medlemmenes tidligere atferd (Usoro et al., 2007). Velviljebasert tillit er tillit til at andre har troverdige intensjoner, og ikke vil misbruke informasjon og ta æren for innsatsen (Paroutis & Al Saleh, 2009). Tillit til velvilje kan bidra til å overvinne frykten for å tape ansikt ved at medlemmene er trygge på at man ikke vil bli kritisert eller gjort til latter når

[20] Underkapittelet om læringsfellesskap er inspirert av Elstad et al. (2016).

man offentlig deler kunnskap (Usoro et al., 2007). Frykt for å tape ansikt ble av Ardichvili et al. (2003) identifisert som en av barrierene for kunnskapsdeling, hvor de påpeker at personer nøler med å dele kunnskap av frykt for å bli kritisert eller for å villede de andre medlemmene.

Læringsfellesskap er dynamiske; de utvikler seg etter hvert som nye medlemmer tas opp, andre medlemmer forlater gruppen, og gruppens kunnskap tilpasses endringer i omverdenen (Mørk et al., 2012). Organisasjoner har også ulike subkulturer, som «både kan ha ulik orientering, overlappe hverandre og stå i konflikt med og motarbeide hverandre» (Jacobsen & Thorsvik, 2007, s. 117). En gruppekultur vil også bli lært bort til nye medlemmer «som den riktige måten å oppfatte på, tenke på og føle på […] det er ikke uvanlig at man i organisasjoner både kan finne et mangfold av kulturer, og kulturer som er preget av tvetydighet og konflikt» (Jacobsen & Thorsvik, 2007, s. 121).

Et eksempel fra Diesen (2022) kan illustrere nødvendigheten av kulturfaktoren i vårt rammeverk. Han hevder at institusjonell militær konservatisme oppstår dersom teknologien truer fagmiljøers operative betydning, ressurstilgang eller interesser for øvrig. Dette kan utløse sterke krefter som motsetter seg endring, og Diesen påpeker at den kulturelle betingelsen er vanskeligst å oppfylle. Med andre ord er kulturen, gjennom felles mønstre av meninger og holdninger, en betingelse for å oppnå en moderne og motstandsdyktig digital grunnmur.

3.9 Rammefaktorer

Som vi var inne på i underkapittel 3.1, eksisterer det en grense mellom elementer som ligger i systemet og elementer som tilhører systemets omgivelser. Rammefaktorer tilhører systemets omgivelser og er dermed faktorer Forsvaret selv ikke kan kontrollere – såkalte ikke-kontrollerbare faktorer. Samtidig skjer det også en utveksling mellom systemet og dets omgivelser, og det er nødvendig å ha oversikt over rammefaktorer og deres utveksling med systemet. Formålet med dette kapittelet er ikke å gå i detalj, men å gjøre oppmerksom på noen eksempler som vi anser er relevante for den digitale grunnmuren. I det følgende presenterer vi de åtte ikke-kontrollerbare faktorene i vårt rammeverk.

3.9.1 Lover og regler

Forsvarssektoren må etterleve en rekke lover, regler, forskrifter og internasjonale konvensjoner. For det første gjelder norsk lov, det vil si Grunnloven og alle øvrige lover vedtatt av Stortinget. Grunnloven skal trygge demokratiet, rettsstaten og menneskerettighetene (§ 2). Grunnloven er den høyeste rettskilden i norsk rett, og dersom det oppstår motstrid mellom en lov eller en forskrift og Grunnloven, har Grunnloven forrang.

Av lover med relevans for framtidig innretning av digital grunnmur, framhever vi sikkerhetsloven med forskrifter, arbeidsmiljøloven, personvernlovgivningen og krigens folkerett.

Sikkerhetsloven (2018) har som formål å beskytte nasjonale sikkerhetsinteresser og opprettholde grunnleggende nasjonale funksjoner (GNF) og gjelder for alle statlige, fylkeskommunale

og kommunale organer. Sikkerhetsloven gjelder også for leverandører av varer og tjenester i forbindelse med sikkerhetsgraderte anskaffelser. I tillegg kan departementene fatte vedtak slik at sikkerhetsloven også helt eller delvis gjelder andre virksomheter. Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetsikkerhetsforskriften, 2018) gjelder alle virksomheter som er underlagt sikkerhetsloven. Med virkning fra 1. juli 2023 ble bestemmelsene om eierskapskontroll strammet inn gjennom endringer i sikkerhetsloven (Endringslov til sikkerhetsloven, 2023).

Arbeidsmiljøloven (2005) gir rammer for rettigheter og plikter for arbeidsgivere og arbeidstakere og er den grunnleggende loven for arbeidslivet i Norge. Loven inneholder blant annet regler om arbeidsmiljø, stillingsvern, arbeidstid, permisjon, ansettelse og avslutning av arbeidsforhold.

Norge har sluttet seg til en rekke internasjonale konvensjoner og rettsregler som er gjort til norsk lov gjennom vedtak av Stortinget. Norge ratifiserte Den europeiske menneskerettighetskonvensjonen (EMK) i 1952, og EMK trådte i kraft 3. september 1953. EMK ble tatt inn i norsk rett i 1999 gjennom lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven). Personvern er nært knyttet til enkeltindividers muligheter for privatliv, selvbestemmelse og selvutfoldelse. Retten til privatliv følger blant annet av EMK artikkel 8. EUs personvernforordning (General Data Protection Regulation (GDPR)) skal bidra til å beskytte personopplysninger. Ny lov om behandling av personopplysninger ble vedtatt 15. juni 2018 og trådte i kraft 20. juli 2018 (Personopplysningsloven, 2018). Den nye loven gjennomfører GDPR i Norge og gjør personvernforordningen til norsk lov. Forskrift om behandling av personopplysninger (2018) utdyper lovparagrafene i personopplysningsloven.

Folkerett, eller internasjonal rett, er rettsregler som gjelder mellom stater og mellom stater og organisasjoner slik som FN. Menneskerettigheter er en del av folkeretten. En gren av folkeretten kalles internasjonal humanitærrett. Dette er rettsregler som gjelder for opptreden under krig og væpnet konflikt, der formålet er å hindre unødvendige lidelser. Internasjonal humanitærrett er det samme som krigens folkerett (Cooper, 2023). Krigens folkerett er forankret i Haag-konvensjonene med regler om midler og metoder for krigføringen og i Genève-konvensjonene som søker å beskytte individer som ikke deltar i krigføringen, det vil si sivile og krigsfanger. Forsvaret ga i 2013 ut «Manual i krigens folkerett» på oppdrag fra FD. Manualen inneholder de nasjonale reglene og tolkningen av krigens folkerett (Forsvarssjefen, 2013). En revidert versjon er under utarbeidelse.

3.9.2 Styrende dokumenter

I det følgende nevnes to eksempler på politisk styrende dokumenter som Forsvaret må ta hensyn til for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur.

Langtidsplan for forsvarssektoren

Den gjeldende LTP-en fra 2020[21] legger føringer for utviklingen av forsvarssektoren. LTP-en trekker fram en del temaer som er relatert til, og har konsekvenser for, den digitale grunnmuren. LTP peker på at digitaliseringen treffer forsvarssektoren med full tyngde, og at sektoren må «settes i bedre stand til hurtigere gjennomføring av teknologiske generasjonsskifter» (LTP, s. 41). Slike teknologiske generasjonsskifter er aktuelle for den digitale grunnmuren. Et eksempel kan være skyteknologi, som blant annet fører til endringer i hvordan nettverk utformes og driftes.

LTP påpeker at digitalisering må skje samtidig som sikkerhetsaspektet ivaretas. Innenfor temaet forebyggende sikkerhet trekker LTP fram at grunnsikringen i forsvarssektorens informasjonssystemer må sørge for et forsvarlig sikkerhetsnivå og akseptabel risiko. Samarbeidet og ansvarsfordelingen mellom etater om håndtering av trusler i det digitale rom, står sentralt (LTP, s. 75), og «Forsvarssektorens evne til å forebygge, avdekke og håndtere trusler i det digitale rom skal styrkes for å beskytte Forsvarets egen virksomhet» (LTP, s. 74).

LTP (s. 132) presiserer at

> [Forsvarssektoren må] styrke sin evne til å ta i bruk og utnytte teknologi raskt og effektivt. Virksomhetene i sektoren skal samhandle bedre med det sivile markedet og ta i bruk nye moderne plattformer og metoder for å etablere og videreutvikle IKT-løsningene.

Videre viser LTP til IKT-strategi for forsvarssektoren (2019a) og presiserer at

> Forsvarssektoren skal ha en fremtidsrettet og nytenkende IKT-virksomhet som er koordinert og delegert, med evne til å utnytte nye plattformer. […] Ansvar skal være delegert til etatene innenfor rammen av en tydelig og helhetlig styringsmodell, i tråd med de politiske rammer og føringer som er gitt. (LTP, s. 32)

Melding til Stortinget om prioriterte endringer, status og tiltak i forsvarssektoren i lys av langtidsplanen

Etter den forverrede sikkerhetspolitiske situasjonen som følge av Russlands angrepskrig mot Ukraina, sendte regjeringen en melding til Stortinget som omhandler prioriterte endringer, status og tiltak i forsvarssektoren i lys av langtidsplanen (Meld. St. 10 (2021–2022)). Meldingen rapporterer om at «IKT-området i sektoren er preget av utvikling og omfattende satsinger», samtidig som «[…] risikoen for forsinkelser i IKT-investeringene fremdeles er høy» og kan få negativ effekt på operativ evne (Meld. St. 10 (2021–2022), s. 28).

> Videreutvikling av strategisk samarbeid med NATO, allierte, næringslivet, og andre statlige aktører vil være nødvendig for å lykkes med å hente ut effekter av ny teknologi

[21] LTP er som tidligere nevnt en forkortelse for «Langtidsplan for forsvarssektoren» (Forsvarsdepartementet, 2020a).

> og digitalisering for å sikre en bærekraftig tilførsel og utnyttelse av kompetanse, samt kontinuerlig videreutvikling av robuste kompetansemiljøer i sektoren. (Meld. St. 10 (2021–2022), s. 28)

Som sitatet viser, sier meldingen at det er nødvendig med eksternt samarbeid, for at Forsvaret skal kunne hente ut effekter av ny teknologi, som for eksempel en moderne og motstandsdyktig digital grunnmur. Regjeringen varsler (Meld. St. 10 (2021–2022), s. 45) at den vil øke innsatsen på digital sikkerhet i forsvarssektoren for å styrke motstandskraften mot sammensatte trusler. Dette skal gjøres både gjennom å styrke Etterretningstjenestens evne til å «[…] følge, attribuere, varsle og aktivt motvirke digitale trusler før hendelser inntreffer», samt «[…] styrking av Cyberforsvaret med både verktøy for sikkerhetsmessig overvåking og videreutvikling av evnen til IKT-responsmiljøet (MilCERT).» Begge disse foreslåtte tiltakene vil inngå som en del av Forsvarets moderne og motstandsdyktige digitale grunnmur.

3.9.3 Økonomiske rammebetingelser

FDs siste budsjettproposisjon (Prop. 1 S (2023–2024)) bruker ikke begrepet digital grunnmur, men gir føringer og økonomiske rammer for IKT-virksomheten og dermed også for digital grunnmur. Budsjettproposisjonen følger opp både gjeldende LTP, IKT-strategi for forsvarssektoren (Forsvarsdepartementet, 2019) og Riksrevisjonens rapport (Riksrevisjonen, 2022). Sistnevnte påpekte økende risiko for begrensninger i Forsvarets samvirke med Nato og allierte, på grunn av utfordringer med interoperabilitet innen IKT-området. Dette er planlagt utbedret på sikt gjennom virksomhetsprogrammene Militær anvendelse av skytjenester (MAST) og Mime.

Hvert år får forsvarssektoren tildelt investerings- og driftsmidler til IKT. Disse midlene utgjør de økonomiske rammebetingelsene for IKT-virksomheten i Forsvaret. Den faktiske bruken av disse midlene blir dels bestemt av FD, dels av Forsvaret og dels av Forsvarsmateriell (FMA) IKT-kapasiteter. De økonomiske rammebetingelsene, altså finansering av Forsvaret, styres av politiske beslutninger. Det vil alltid være usikkerhet knyttet til framtidige økonomiske rammebetingelser. Grunnet samfunnsmessige forhold og den nåværende sikkerhetspolitiske situasjonen er det mye oppmerksomhet rundt investeringer til Forsvaret, men dette kan endre seg.

FFI har gjort en rekke undersøkelser knyttet til investeringsprosesser og materiellanskaffelser i Forsvaret, for flere detaljer se for eksempel Presterud et al. (2022), Presterud et al. (2018) og Berg og Waage (2020).

3.9.4 Klima og miljø

Bærekraftig utvikling kan beskrives som «En utvikling som imøtekommer dagens behov uten å ødelegge mulighetene for at kommende generasjoner skal få dekket sine behov» (FN-sambandet, 2023a). Bærekraftig utvikling har tre dimensjoner – klima og miljø, økonomi og sosiale forhold – og «det er sammenhengen mellom disse tre dimensjonene som avgjør om noe er bære-

kraftig» (FN-sambandet, 2023a). FN har definert 17 bærekraftsmål[22], som er «verdens felles arbeidsplan for å utrydde fattigdom, bekjempe ulikhet og stoppe klimaendringene innen 2030.» (FN-sambandet, 2023b). Stortinget har vedtatt Norges handlingsplan for å nå bærekraftsmålene innen 2030 (Meld. St. 40 (2020–2021)). LTP (s. 123) sier at «Forsvarssektoren skal bidra til Norges innsats for å nå FNs bærekraftsmål.»

Forsvarskommisjonen (NOU 2023: 14) peker på flere utfordringer knyttet til klima og miljø, som for eksempel at klimaendringer er en trusselmultiplikator (se også Beadle et al., 2019), ekstremvær og innvirkning på operativ evne, raskere klimaendringer i Arktis samt klimatilpasninger og politiske konsekvenser.

Forsvarsektoren har gitt ut en egen klima- og miljøstrategi (Forsvaret et al., 2022) som dekker den første av de tre bærekraftsdimensjonene, altså klima og miljø. Strategien dekker 11 av FNs 17 bærekraftsmål[23]. Forsvarsektorens klima- og miljøstrategi (Forsvaret et al., 2022, s. 4) sier at forsvarssektoren skal redusere negative miljøpåvirkninger og bidra til et bærekraftig samfunn – både nasjonalt og internasjonalt – samt være forberedt på og tilpasset til klimaendringene. I underkapittel 5.2.6 kommer vi nærmere inn på hva Forsvaret bør gjøre for å ivareta klima og miljø med tanke på den digitale grunnmuren.

I forsvarssjefens fagmilitære råd 2023 (FMR) (Forsvaret, 2023b) trekkes også FNs bærekraftsmål fram, sammen med forsvarssektorens klima- og miljøstrategi. I FMR legges det vekt på at Forsvaret, som kontraktør og innkjøper, har et ansvar for å sørge for en bærekraftig utvikling, gjennom bevissthet rundt bærekraft i forbindelse med anskaffelser, drift og avhending av materiell. Dette er relevant også for den digitale grunnmuren, både ved valg av eventuelle strategiske partnere og leverandører samt i forbindelse med utvikling, drift og avhending av eget materiell.

For flere detaljer om konsekvenser av klimaendringer og klimatilpasninger for Forsvaret mot 2040, se Granlund et al. (2022). Det er gjennomført en mulighetsstudie av klimavennlig teknologi for Forsvaret, for flere detaljer se Arnfinnsson og Tønsberg (2023). For flere detaljer om hvordan Forsvaret kan kutte utslipp av klimagasser, se Arnfinnsson og Kirkhorn (2021).

3.9.5 Teknologisk utvikling

Den teknologiske utviklingen er en faktor som påvirker Forsvaret generelt. Vi tror utviklingen innen flere framvoksende teknologier vil kunne påvirke den digitale grunnmuren. Noen teknologiske trender som vil påvirke Forsvaret, er analysert i Andås (2020) og Bentstuen (2022). Blant de teknologiske trendene som nevnes i disse to studiene, tror vi blant annet bruk av kunstig intelligens (KI), økt bruk av sensorer og avanserte analyser av store datamengder («stor-

[22] FNs 17 bærekraftsmål: (1) utrydde fattigdom, (2) utrydde sult, (3) god helse og livskvalitet, (4) god utdanning, (5) likestilling mellom kjønnene, (6) rent vann og gode sanitærforhold, (7) ren energi til alle, (8) anstendig arbeid og økonomisk vekst, (9) industri, innovasjon og infrastruktur, (10) mindre ulikhet, (11) bærekraftige byer og lokalsamfunn, (12) ansvarlig forbruk og produksjon, (13) stoppe klimaendringene, (14) livet i havet, (15) livet på land, (16) fred, rettferdighet og velfungerende institusjoner og (17) samarbeid for å nå målene.
[23] Følgende mål er dekket: 3, 4, 6, 7, 9, 11, 12, 13, 14, 15 og 17.

data»), vil få påvirkning på hva det forventes at den digitale grunnmuren leverer av IKT-tjenester. Et eksempel på dette er overgangen fra å drifte egne IKT-systemer til å benytte seg av skytjenester. Når skytjenester blir den foretrukne måten å bygge opp IKT-systemer på ellers i samfunnet, kan det føre til at de moderne produktene baserer seg på skyteknologi, mens andre produkter fases ut. I tilfellet med skytjenester er det ikke gitt at Forsvaret på en enkel måte kan nyttiggjøre seg den teknologiske utviklingen, da det blant annet er uklarheter rundt hvordan skytjenester kan benyttes for å lagre og behandle gradert informasjon (Lund et al., 2021).

3.9.6 Interessenter

Interessenter tilfører organisasjonen ressurser, som arbeidskraft, penger og lojalitet, og har interesser i hvordan organisasjonens ressurser brukes. Eksempler på interessenter er kunder, ledere, leverandører og partnere (Barney, 2002). Alle interessenter har i en eller annen form en relasjon med organisasjonen (Jones & Hill, 2013). For eksempel gir leverandører organisasjonen varer og forventer inntekter og pålitelige kjøpere. Regjeringen gir regler og forskrifter som skal følges, og forventer at Forsvaret vil følge disse reglene. Forsvaret har også andre interessenter, som Nato, befolkningen, media og de andre aktørene i totalforsvaret.

Interessenter kan ha konkurrerende behov. Et eksempel kan være innenfor sourcing[24], hvor en organisasjon har interessenter internt gjennom de ansatte og eksternt gjennom potensielle strategiske partnere. Et annet eksempel kan være åpenhet til befolkningen sett opp mot behovet for sikkerhetsgradert informasjon. På grunn av slike motstridende interesser kan en organisasjon ikke tilfredsstille alle sine interessenter samtidig. Cameron (1978) konkluderte med at én interessentgruppe må betjenes på bekostning av en annen. Lederne må ta valg mellom de ulike motstridende kravene fra interessentene (Friedman & Miles, 2002; Jones & Hill, 2013), og vi har derfor med interessenter som en rammefaktor.

3.9.7 Samfunnsmessige forhold

Det er en rekke samfunnsmessige forhold som Forsvaret ikke selv kan kontrollere, men må forholde seg til. «Forsvarskonseptet beskriver sammenhengen mellom de sikkerhets- og forsvarspolitiske målene og Forsvarets oppgaver med tilhørende ambisjon.» (LTP, s. 25).

Forsvarskonseptet består av nasjonal forsvarsevne, det kollektive forsvaret i Nato og bilaterale forsterkningsplaner med nære allierte, understøttet av et moderne og forberedt totalforsvar (LTP, s. 25). Forsvarskonseptet bygger på sivilt-militært samarbeid i tråd med totalforsvarskonseptet. Totalforsvarskonseptet innebærer gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn i forbindelse med forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespekteret (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2018). Forsvaret er derfor avhengig av å samhandle med både offentlige, private og frivillige totalforsvarsaktører. Det skjer også en rask og omfattende globalisering av digitale verdikjeder med store multinasjonale selskaper i spissen for teknologiutviklingen. Dette

[24] Sourcing er den strategiske beslutningen som skjer i forkant av kjøp av for eksempel tjenester. Se for eksempel Elstad, Endregard og Mykkeltveit (2022) for flere detaljer.

påvirker mulige samarbeidskonstellasjoner samt hvordan Forsvaret kan nyttiggjøre seg av teknologi.

Beredskap og krisehåndtering bygger på at alle samfunnets ressurser skal kunne benyttes ved behov. Ressursene er begrenset og skal i minst mulig grad dupliseres. Det betyr at Forsvaret er avhengig av sivil støtte i sin operative virksomhet i hele krisespekteret, og at Forsvaret yter bistand til politiet og andre sivile beredskapsaktører. I tillegg ivaretar Forsvaret en rekke samfunnsoppgaver i det daglige for, og i samarbeid med, sivile myndigheter, eksempelvis grensevakt og toll- og fiskerioppsyn.

Forsvaret har inngått en rekke kommersielle avtaler om leveranser av materiell og tjenester, inkludert ekom-tjenester til den digitale grunnmuren. I praksis betyr dette at Forsvaret er avhengig av å samhandle med et bredt spekter av aktører. Det krever muligheter for samhandling og utveksling av informasjon mellom informasjonssystemer på samme graderingsnivå, men også mellom graderingsnivåer og med ugraderte informasjonssystemer. Sivilt-militært samarbeid og sivile totalforsvarsaktørers behov for samhandling med Forsvaret, er derfor viktige rammefaktorer for utviklingen av den digitale grunnmuren.

FDs IKT-organisasjon leverer graderte IKT-tjenester til statlige og private virksomheter, og disse IKT-tjenestene utvikles videre (Forsvarsdepartementet, 2023a, s. 64). Dette gjelder blant annet Nasjonalt BEGRENSET nett (NBN) og Nasjonalt HEMMELIG nett (NHN).

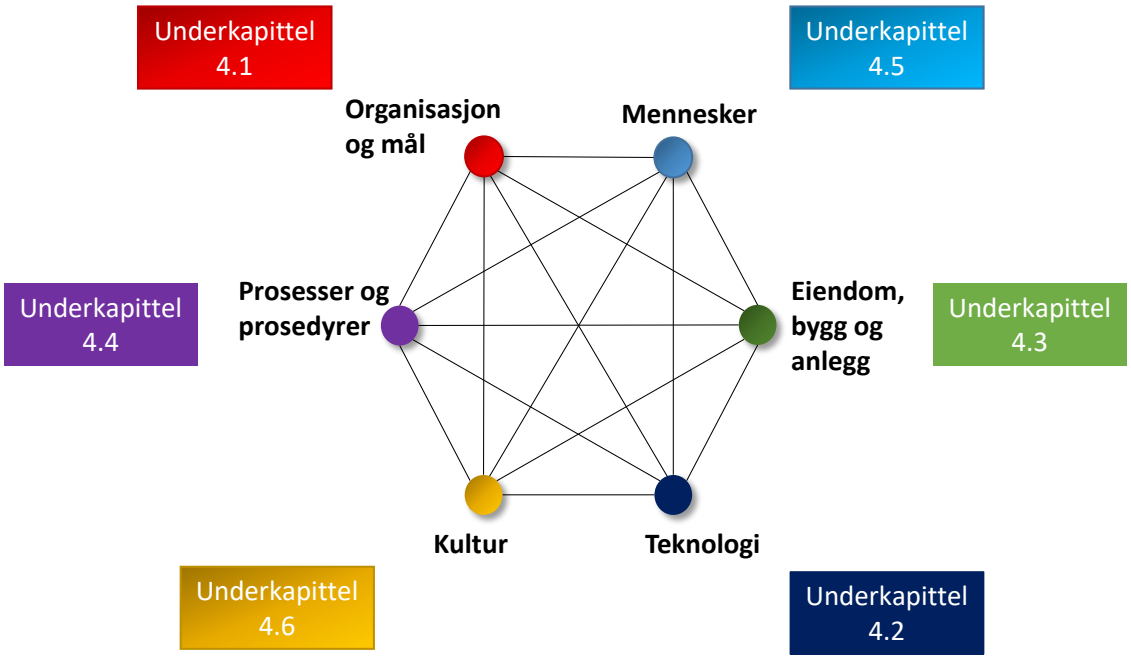
Den stadig økende globaliseringen innen teknologiutvikling og selskapsstrukturer, er en utvikling verken Forsvaret eller Norge selv kan styre. Verdikjedene for produksjon av maskinvare og programvare er komplekse og uoversiktlige. Store multinasjonale selskaper, som Facebook, Google, Amazon, Microsoft og Apple, er premissgivere og drivere for en stor del av teknologi- og IKT-tjenesteutviklingen framover. Det er mulig å se for seg at de multinasjonale teknologigigantene vil ta over som de eneste kompetente tilbydere av moderne digitale tjenester på sikt.

3.9.8 Sikkerhetspolitisk situasjon

Hva som skjer i verden rundt oss, påvirker forsvarsplanleggingen, og «Angrepet på Ukraina representerer starten på en ny tid i Europa, og en varig endring av våre sikkerhetspolitiske omgivelser.» (Meld. St. 10 (2021–2022), s. 11). Regjeringen vektlegger at det blir stadig viktigere å investere i nasjonalt forsvar og sikkerhet for å ivareta sentrale norske interesser og sikkerhet. Det synes å være politisk enighet om at det haster med å utbedre mangler i nasjonalt forsvar og sikkerhet. Det at Finland har blitt medlem av Nato, og at Sverige kanskje blir det snart, kan påvirke planforutsetninger og mulighetene på IKT-området, og være et grunnlag for tettere nordisk samarbeid.

4 Forsvarets digitale grunnmur – nåsituasjon

Målet med dette kapittelet er overordnet å beskrive nåsituasjonen for Forsvarets digitale grunnmur for hver av de seks faktorene i vårt rammeverk, med vekt på identifiserte utfordringer. Figur 4.1 viser kapittelinndelingen for nåsituasjonen for de ulike faktorene i vårt rammeverk.



Figur 4.1 Kapittelinndeling for nåsituasjonen for de seks faktorene i vårt rammeverk.

4.1 Organisasjon og mål

Faktoren «organisasjon og mål» i vårt rammeverk omhandler de formelle delene av organisasjonen, det vil si organisasjonsstruktur og mål fra styrende dokumenter som organisasjonen selv har kontroll over. I det følgende går vi nærmere inn på IKT-styringsmodell og de styrende dokumentene som Forsvaret selv kan påvirke.

4.1.1 IKT-styringsmodell

Forsvarets IKT-strategi peker på utfordringer ved eksisterende IKT-virksomhet, som silotilnærming og begrensninger knyttet til samvirke og interoperabilitet. Videre står det at: «Forsvarssektorens evne til å finansiere og drive styring og prioritering ved gjennomføring av IKT-prosjekter har store utfordringer, og prosessen fra et behov oppstår til det understøttes med IKT som gir operativ effekt kan effektiviseres».

Riksrevisjonen (2022) avdekket i sin rapport flere utfordringer ved dagens IKT-styringsmodell, det vil si hvordan IKT-området er organisert og fordelingen av roller, ansvar og myndighet for aktørene i IKT-virksomheten. Riksrevisjonen (2022) konkluderte med at overlappende og uklare ansvarsforhold mellom etatene i forsvarssektoren har påvirket gjennomføringsevnen på IKT-området.

Ansvar, myndighet og funksjon for å utøve og videreutvikle den strategiske IKT-styringen i sektoren er lagt til forsvarssjefen (Forsvarsdepartementet, 2020b, s. 19). Gjeldende LTP fra 2020 gir en oversikt over forventede oppdrag innenfor IKT-området. Denne oppdragsbeskrivelsen kan anses som en del av den formelle organisasjonen, men er ikke en IKT-styringsmodell i seg selv. Tabell 4.1 gir en oversikt over de tre primære aktørene for utvikling, drift og vedlikehold av den digitale grunnmuren, og hva disse er forventet å gjøre:

AKTØR	OPPDRAGSBESKRIVELSE
Cyber-forsvaret	Cyberforsvaret er Forsvarets avdeling for informasjons- og kommunikasjons-teknologi (IKT) og har som hovedoppdrag å stille krav til, etablere, drifte og beskytte Forsvarets IKT til bruk i operasjoner og daglig virksomhet. Avdelingen utfører defensive tiltak i Forsvarets egen IKT som en del av integrerte felles-operasjoner. Cyberforsvaret er innrettet mot leveranser av IKT til forsvars-sektoren og mot oppdrag innenfor sitt ansvarsområde som kun kan løses av Forsvaret (LTP, s. 108).
FMA	Forsvarsmateriell (FMA) skal på vegne av Forsvarsdepartementet ivareta ans-varet for å framskaffe, forvalte og avhende materiell for Forsvaret og andre etater i forsvarssektoren på en ressurseffektiv måte. FMAs hovedoppgave er å sørge for at Forsvaret og andre etater får tilgang til kostnadseffektivt og sikkert materiell i tråd med vedtatte langtidsplaner, slik at Forsvarets operative evne ivaretas. FMA skal forvalte materiellet effektivt gjennom hele dets levetid, og er tillagt fagmyndighet for materiell i forsvarssektoren. FMA skal gi faglige råd innenfor materiellanskaffelser og forvaltning i forsvarssektoren, og gi faglige råd til Forsvarsdepartementet og etatssjefene i sektoren for å videreutvikle materiellet til å gi mest mulig operativ evne innenfor ressursrammene (LTP, s. 120).
Forsvars-bygg	Forsvarsbygg skal, på vegne av Forsvarsdepartementet, utøve eierrollen for for-svarssektorens eiendommer, bygg og anlegg (EBA) på en nøktern og effektiv måte. Forsvarsbyggs hovedoppgaver er å forvalte de statlige eiendommene for-svarssektoren disponerer, gjennomføre investeringer i EBA og avhende EBA som sektoren ikke lenger har behov for. Forsvarsbygg skal være forsvarssektor-ens fremste faglige rådgiver innenfor tjenestefeltet EBA og gi faglige råd for en effektiv anvendelse av ressursene til Forsvarsdepartementet og øvrige etater i forsvarssektoren. Forsvarsbygg skal bidra til understøttelse av forsvarsevnen gjennom kostnadseffektive og funksjonelle EBA-tjenester og rådgivning, både innenfor investeringer, drift og vedlikehold og avhending. Forsvarsbyggs forvaltningsansvar av sektorens EBA skal gi etatene i sektoren tilgang på funksjonell og kostnadseffektiv EBA (LTP, s. 119).

Tabell 4.1 Overordnet oppdragsbeskrivelse for Cyberforsvaret, Forsvarsmateriell og Forsvarsbygg. Kilde: LTP (2020).

Denne oppdragsbeskrivelsen gir en oversikt over hvilke virksomhetsprosesser det er forventet at Cyberforsvaret, FMA og Forsvarsbygg skal utføre. Eksempelvis skal Cyberforsvaret utføre prosesser knyttet til «å stille krav til, etablere, drifte og beskytte Forsvarets IKT til bruk i operasjoner og daglig drift», mens FMA skal på vegne av FD ha ansvaret for å framskaffe, forvalte og avhende materiell for forsvarssektoren på en ressurseffektiv måte.

I Prop. 1 S (2023–2024) (s. 44) påpekes det at ny styringsmodell for forsvarssektoren «skal tydeliggjøre roller og ansvar» – og «rydde opp i roller og ansvarsdelingen mellom etatene» – «slik at Forsvaret kan bli i stand til å håndtere ansvaret for strategisk IKT-styring». Videre skal

styrkingen av Cyberforsvaret fortsette «for å modernisere Forsvarets IKT-infrastruktur og styrke evnen til å beskytte Forsvarets IKT» (Prop. 1 S (2023–2024), s. 91). IKT-responsmiljøet (MilCERT) skal styrke «evnen til å forebygge, avdekke og håndtere uønskede digitale hendelser rettet mot Forsvarets IKT i fred, krise og krig» (Prop. 1 S (2023–2024), s. 91).

4.1.2 Forsvarets IKT-strategi

Forsvarets IKT-strategi (Forsvarsstaben, 2021) skal «bidra til å realisere målene som er beskrevet i IKT-strategien for forsvarssektoren (2019) og Digitaliseringsstrategien for Forsvaret (2018)». Forsvarets IKT-strategi «legger føringer for utviklingen av IKT-området som Forsvarets ledelse skal styre etter, og primærmålgruppen for strategien er hele Forsvaret». Ifølge Forsvarets IKT-strategi er visjonen for IKT i Forsvaret «Økt operativ effekt gjennom robust IKT i kontinuerlig utvikling – IKT for morgendagens forsvar».

Forsvarets IKT-strategi har tre strategiske mål for IKT i Forsvaret: (1) IKT som driver for K2 og samvirke, (2) effektiv styring av IKT for hurtig ivaretakelse av operative behov, og (3) bedre og raskere utnyttelse av teknologi. Et delmål (1.3) sier at «IKT-utvikling skal være behovsdrevet, koordinert og delegert, innenfor rammene av Forsvarets digitale reguleringsplan». Forsvarets IKT-strategi omhandler også mål og prinsipper for innretting av IKT-porteføljestyring[25]:

> For å tilrettelegge for tettere kobling mot behovseiere og korte ned tiden det tar fra et behov er identifisert og prioritert til løsning er tatt frem og tatt i bruk, vil styringen av IKT-porteføljen organiseres i delporteføljer som eies av de som eier behovene. En behovseier er den sjef som er ansvarlig for den funksjonen eller det området som rommer det aktuelle behovet. Dette handler i stor grad om å ansvarlig- og myndiggjøre behovseiere for å sikre at de behovene som gir størst effekt løses raskt og effektivt.

4.1.3 Digital reguleringsplan (DRP)

DRP (Forsvarsstaben, 2023) definerer åtte IKT-innsatsområder. Hvert IKT-innsatsområde har ett sett med mål for 2024, 2026 og 2028, med tilhørende målkort, som til sammen danner et målbilde. Figur 4.2 viser målkortet for IKT-innsatsområdet «moderne og motstandsdyktig digital grunnmur».

[25] Begrepsbruken i Forsvarets IKT-strategi er ikke harmonisert med begrepene som benyttes i IKT-porteføljestyring (Forsvarsstaben, under utarbeidelse) og DRP. Hovedområder omtales i IKT-strategien som delporteføljer.

(U) Målkort moderne og motstandsdyktig digital grunnmur (DG):

IKT-innsatsområdet skal muliggjøre rask IKT-utvikling og hurtig ivaretakelse av operative behov gjennom en skalerbar, fleksibel, motstandsdyktig og moderne digital grunnmur

Mål 2024	Mål 2026	Mål 2028
• Målbilder og veikart etablert, tidskritisk modernisering pågår • Støtte for smidighet og høy endringstakt • Tidlig tilretteleggelse for felles innovasjon	• Modernisering av plattform og infrastruktur • Forsvarbar og robust kommunikasjon • Tilrettelagt for innovasjon • Sektorfelles digital grunnmur på prioriterte områder	• Modernisert grunnmur • Modernisert kommunikasjon • Etablert støtte og kapasitet for stordata og analyse • Gjennomgående sektorfelles digital grunnmur

(U) Figur 1 Målkort moderne og motstandsdyktig digital grunnmur (DG).

Figur 4.2 Målkort hentet fra DRP (Forsvarsstaben, 2023) for IKT-innsatsområdet moderne og motstandsdyktig digital grunnmur.

Målene i figur 4.2 viser at dette IKT-innsatsområdet legger føringer for hvordan den digitale grunnmuren må utformes, og at den digitale grunnmuren også spiller en rolle i å oppfylle målene i de øvrige IKT-innsatsområdene.

IKT-innsatsområdet «tidsriktige og relevante applikasjoner og tjenester» i DRP omhandler også mål som er relevante for digital grunnmur, vist i figur 4.3. Målene i figur 4.3 viser at IKT-innsatsområdet tidsriktige og relevante applikasjoner og tjenester skal ivareta forsvarssektorens behov for modernisering av applikasjons- og tjenesteporteføljen. Ett av målene for 2028 omhandler direkte digital grunnmur, og sier at applikasjons- og tjenesteporteføljen skal benytte modernisert digital grunnmur.

(U) Målkort tidsriktige og relevante applikasjoner og tjenester (TAT):

IKT-innsatsområdet skal ivareta forsvarssektorens behov for modernisering av applikasjons- og tjenesteporteføljen, samt sikre effektiv støtte, kapasitet og skalerbarhet til strukturutvikling, operasjoner og virksomhetsstyring

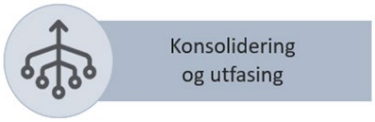
Mål 2024	Mål 2026	Mål 2028
• Felles målbilder og veikart etablert og iverksatt • Tidskritisk modernisering • Kontinuerlig leveranser innenfor prioriterte områder	• Kontinuerlig modernisering	• Moderniserte applikasjoner og tjenester • Applikasjons- og tjenesteportefølje benytter modernisert digital grunnmur

(U) Figur 1 Målkort tidsriktige og relevante applikasjoner og tjenester (TAT).

Figur 4.3 Målkort hentet fra DRP (Forsvarsstaben, 2023) for IKT-innsatsområdet tidsriktige og relevante applikasjoner og tjenester.

Et annet IKT-innsatsområde fra DRP vi trekker fram er «konsolidering og utfasing», hvor figur 4.4 viser målkortet.

(U) Målkort Konsolidering og utfasing (KU):



IKT-innsatsområdet skal sørge for at antallet informasjons-systemer reduseres til et nødvendig minimum, og at applikasjoner og tjenester i størst mulig grad harmoniseres, standardiseres og reduseres

Mål 2024	Mål 2028
• Konsolidering av informasjonssystemer pågår • Konsolidering av applikasjoner og brukernært utstyr pågår	• Informasjonssystemer konsolidert i sektor • Bærekraftig applikasjons- og tjenesteportefølje • Fellestjenester harmonisert i sektor

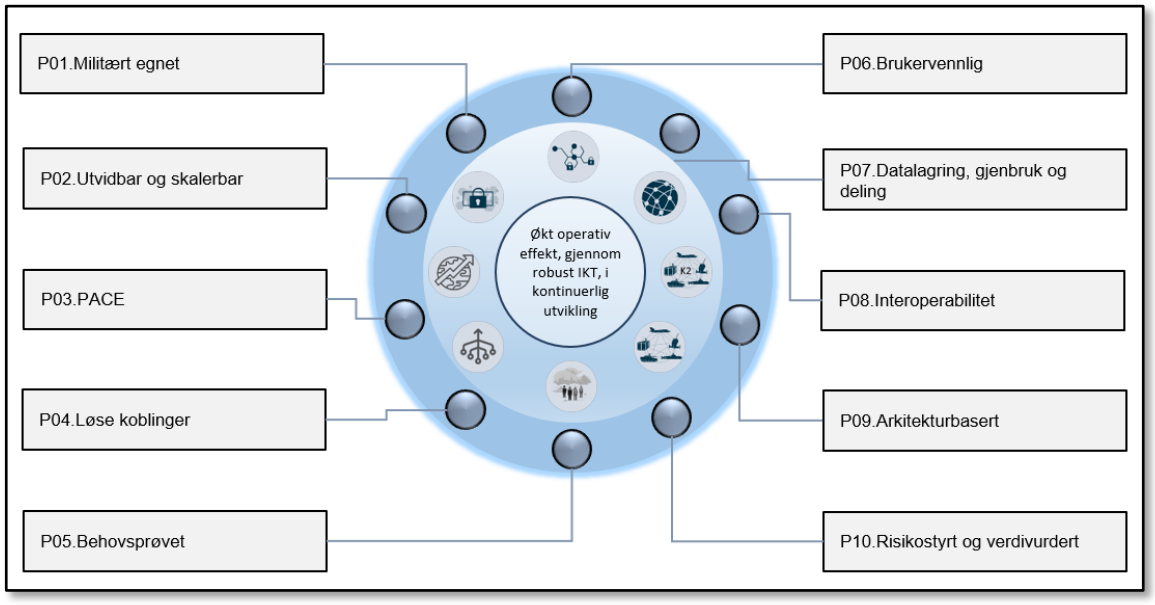
(U) Figur 1 Målkort Konsolidering og utfasing (KU).

Figur 4.4 Målkort hentet fra DRP (Forsvarsstaben, 2023) for IKT-innsatsområdet konsolidering og utfasing.

Figur 4.4 viser at konsolidering og utfasing skal redusere antall informasjonssystemer til et nødvendig minimum. I tillegg angir DRP et mål om en «bærekraftig applikasjons- og tjenesteportefølje» i 2028, samt at «fellestjenester er harmonisert i sektor».

Videre inneholder DRP (Forsvarsstaben, 2023) ti prinsipper for regulering av IKT-utvikling, -drift og -forvaltning, vist i figur 4.5. I midten av figuren finner vi igjen visjonen fra Forsvarets IKT-strategi (Forsvarsstaben, 2021), og IKT-innsatsområdene er representert med små symboler.

> [Prinsippene i DRP] skal bidra til å oppnå målbildet innenfor IKT-innsatsområdene. Prinsippene er generelt formulert og er ikke å anse som absolutte regler, men er tenkt å virke som retningsgivende føringer. Prinsipper vil kunne kollidere. Det vil være behov for faglige vurderinger ved slike kollisjoner, og i enkelte tilfeller vil det være behov for å gjøre avklaringer i rammen av IKT-styringsmodell. (Forsvarsstaben, 2023)



Figur 4.5 DRPs prinsipper for regulering av IKT-utvikling, -drift og -forvaltning. Innerste sirkel er visjonen fra IKT-strategien til Forsvaret. Neste ring viser små symboler som representerer de åtte IKT-innsatsområdene. Ytterste ring presenterer prinsippene for regulering av IKT-utvikling, -drift og -forvaltning. (Forsvarsstaben, 2023).

4.1.4 Digitaliseringsstrategi for Forsvaret

Digitaliseringsstrategi for Forsvaret (Forsvarsstaben, 2018, s.24) har åtte digitaliserings-prinsipper som skal gjelde for «[…] alt vi gjør, og anvendes for prioritering, evaluering og gjennomføring av initiativ». Disse prinsippene fra digitaliseringsstrategien for Forsvaret (s. 24) vil påvirke utformingen av en moderne og motstandsdyktig digital grunnmur:

1) *Standardisert*: Bruk standardkomponenter og forenkle der det er mulig, identifiser sammenfallende behov og fokuser på gjenbruk på tvers.
2) *Brukerorientert*: Ta utgangspunkt i brukerbehov og involver brukerne i utvikling og implementering.
3) *Kun én gang*: Brukeren skal ikke behøve å levere samme informasjon flere ganger til flere systemer.
4) *Interoperabilitet*: Informasjon og data som kan deles skal kunne deles sømløst og effektivt, internt, i sektoren og med allierte.
5) *Verdiskapende*: Tiltak vurderes i et bærekraftperspektiv. Det skal gjennomføres jevnlige kost-/nyttevurderinger hvor tiltak med lav måloppnåelse avsluttes tidlig.
6) *Sikkerhetsorientert*: Krav til informasjonssikkerhet er retningsgivende i prioritering, utvikling, og implementering av tiltak.
7) *Robusthet*: Robuste og redundante systemer for å kunne motstå angrep og sabotasje, og unngå bortfall av tjeneste skal vektlegges.

8) *Hurtighet*: Teste levedyktigheten til tiltak så tidlig som mulig og levere «Minimum Military Requirement» (MMR) først.

4.1.5 Prosjekt Forsvarssektoren 2024

Ifølge Forsvaret (2023a) har utredninger funnet flere systemsvakheter i forsvarssektoren som reduserer den operative evnen til Forsvaret. Som en konsekvens av dette, opprettet FD prosjektet «Forsvarssektoren 2024» (F24) (Forsvaret, 2023a). F24 er en rammefaktor, ved at Forsvaret som etat ikke selv har beslutningsmyndighet. Forsvaret kan likevel påvirke F24, gjennom sine innspill til prosjektet. F24 legger opp til endringer innen flere områder i forsvarssektoren i løpet av 2024, innen styring og innretning av sektoren, hvor IKT er ett av områdene (Forsvaret, 2023a). Endringene som følge av F24-prosjektet skal føre til raskere beslutningsprosesser, høyere gjennomføringstempo og økt effektivitet. F24 har fem mål: (1) tydeligere mål i sektoren, (2) mer helhetlig beslutningsgrunnlag basert på fakta, (3) mindre fragmentering, (4) tydeligere oppgavefordeling og ansvar og (5) økt styring og kontroll (Forsvaret, 2023a).

4.2 Teknologi

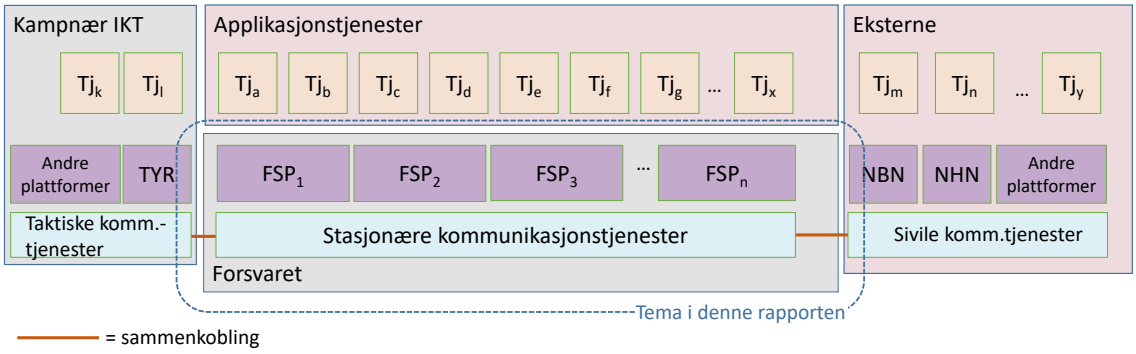
I dette underkapittelet beskriver vi nåsituasjonen for faktoren «teknologi» i vårt helthetlige rammeverk. Som beskrevet i underkapittel 3.4 inngår IKT-tjenester innen IT-plattform, infrastruktur og kommunikasjon i den digitale grunnmuren. I figur 4.6[26] benytter vi denne beskrivelsen som et utgangspunkt for vår prinsipielle skisse av hvordan Forsvarets digitale grunnmur ser ut i dag.

Dagens digitale grunnmur består av Forsvarets sikre plattformer (FSP), altså FISBasis[27]-plattformene og et antall plattformer med mer spesialiserte bruksområder. Merk at infrastrukturlaget fra DRP ikke er vist i figur 4.6 da dette laget inkluderes som en del av IT-plattform for Forsvarets IKT-systemer. Videre inngår Forsvarets kommunikasjonsinfrastruktur[28] (FKI) i dagens digitale grunnmur for Forsvaret. FKI består av stasjonære, deployerbare og mobile kommunikasjonstjenester. Den stasjonære digitale grunnmuren inkluderer blant annet fibernett, noe satellittkommunikasjon samt radiolinjer og strekker seg over store områder. I tillegg inngår også Forsvarets datasentre i den digitale grunnmuren.

Til venstre i figur 4.6 finner vi IKT som tilhører digital grunnmur i DRP, men som faller inn under kampnær IKT, det vil si taktiske (mobile og deployerbare) IT-plattformer (først og fremst TYR, som er den primære IT-plattformen på taktisk nivå), infrastrukturtjenester og kommunikasjonstjenester. Dette dekkes ikke av denne rapporten[29]. Høyre side av figur 4.6 illustrerer at den digitale grunnmuren også er knyttet mot ekstern infrastruktur, inkludert Internett[30] i

[26] Figur 4.6 er ment som en grov illustrasjon og er sterkt forenklet sammenlignet med virkeligheten.
[27] Forsvarets Informasjonssystem Basiskonfigurasjon. Dette er Forsvarets felles IT-plattformer.
[28] Tilsvarer kommunikasjonstjenester i DRP.
[29] For flere detaljer, se Bloebaum et al. (under arbeid).
[30] Forsvaret benytter Internett for datakommunikasjon, derfor inngår Internett som en del av kommunikasjonstjenestene i dagens digitale grunnmur.

tillegg til enkelte sivile IT-plattformer, som for eksempel Microsoft Azure[31]. Det er også sammenkobling med de offentlige IT-plattformene NBN og NHN[32].



Figur 4.6 Prinsipiell skisse av Forsvarets digitale grunnmur i dag. I figuren er infrastruktur-tjenestene inkludert i plattformen (FSP, TYR, NBN, osv.), og vises derfor ikke.

Som figur 4.6 illustrerer, inkluderer Forsvarets digitale grunnmur et større antall IT-plattformer,[33] dels fordi hvert graderingsnivå har én eller flere IT-plattformer og dels fordi enkelte applikasjonstjenester har egne IT-plattformer (og dermed utgjør egne IKT-systemer). Det er begrensede muligheter for informasjonsdeling og samvirke mellom IKT-systemer på ulike graderingsnivåer, og til dels også mellom IKT-systemer på samme graderingsnivå. Dette gjør at dagens digitale grunnmur i Forsvaret kan sies å være relativt fragmentert, og har begrensede muligheter for gjennomgående digital informasjonsdeling. Riktignok kan en slik fragmentering gi enkelte sikkerhetsmessige fordeler, ved at gradert informasjon blir spredt over flere IKT-systemer i stedet for at alt samles i ett system. På den annen side fører det til at prinsippene fra digitaliseringsstrategien for Forsvaret (Forsvarsstaben, 2018) ikke blir tilfredsstilt, i første rekke gjelder det prinsippene standardisert, kun én gang og interoperabilitet. Det samme gjelder flere av prinsippene fra DRP (Forsvarsstaben, 2023), for eksempel datalagring, gjenbruk og deling samt interoperabilitet.

Riksrevisjonen (2022, s. 9) har påpekt at Forsvaret har «et høyt antall kommando- og kontrollinformasjonssystemer med ulike tekniske løsninger, og at dette bidrar til å gjøre samvirket mellom systemene vanskelig». Riksrevisjonen (2022) finner det også sterkt kritikkverdig at Forsvaret ikke har lyktes i å begrense antall IKT-systemer.

Videre har Riksrevisjonen (2022) påpekt sårbarheter i FKI, og FFIs forsvarsanalyse for 2022 (Skjelland et al., 2022) viser til kritiske sårbarheter innen kommunikasjon. Riksrevisjonen påpeker også at det er mangler i Forsvarets evne til å oppdage og stanse digitale angrep.

[31] Azure er Microsofts skyplattform som tilbyr en rekke applikasjoner og IKT-tjenester som skytjenester (Microsoft, u.d.-a).
[32] Disse er utviklet av FD for behandling av gradert informasjon i statsforvaltningen (Forsvarsdepartementet, 2016).
[33] Det nøyaktige antallet kommer an på tellemåten og hvilket perspektiv tellingen har. Det vesentlige i vår sammenheng er imidlertid bare at det er et forholdsvis stort antall, ikke nøyaktig hvor mange IT-plattformer Forsvaret har.

Figur 4.7 viser en oppsummering av nåsituasjonen innenfor faktoren «teknologi» for Forsvarets digitale grunnmur.

Figur 4.7 Oppsummering av identifiserte utfordringer i nåsituasjonen innenfor faktoren «teknologi».

4.3 Eiendom, bygg og anlegg

EBA omfatter militære baser, kontorbygg, hovedkvarter, datasentre og overvåkingssentre som brukes av personellet som utfører utvikling, drift, vedlikehold og sikkerhetsovervåkning knyttet til digital grunnmur samt ubemannede bygg for IKT. Eksempler på sistnevnte er bygg som huser noder i FKI. Ved innretning og avgjørelser knyttet til den digitale grunnmuren, er behov, kostnader og sikkerhet for EBA en sentral del av beslutningsgrunnlaget.

Den bygningsmessige infrastrukturen for digital grunnmur er i liten grad trukket fram i den informasjonen denne rapporten bygger på, det vil si dokumenter og samtaler med informanter fra forsvarssektoren.[34] Vi har derfor ikke grunnlag for å si mye om nåsituasjonen for den digitale grunnmurens EBA i denne rapporten, men vi kan peke på noen mulige utfordringer som bør undersøkes nærmere.

Et helhetlig og balansert forsvarlig sikkerhetsnivå for den digitale grunnmuren, inkluderer fysisk sikkerhet for grunnmurens EBA, i tillegg til digital sikkerhet og personellsikkerhet. Formålet med fysisk sikkerhet er å etablere et forsvarlig sikkerhetsnivå som skal forebygge og håndtere eventuell uautorisert fysisk tilgang til EBA. Fysisk sikkerhet handler derfor om bygnings-messige barrierer (vegger, dører, vinduer, gjerder, m.m.), låser i tillegg til elektroniske sikker-hetstiltak slik som alarmer, kameraovervåkning og bruk av andre sensorer. Om og eventuelt i hvilken grad fysisk sikkerhet for EBA inkluderes i risikovurderinger for dagens digitale grunnmur har vi ikke innhentet informasjon om.

Det er viktig at den fysiske og elektroniske sikringen av EBA er hensiktsmessig, sett opp mot den funksjonaliteten den digitale grunnmuren skal ha for virksomhetsprosesser i forsvars-sektoren. For at EBA for den digitale grunnmuren skal gi hensiktsmessig funksjonalitet, er avhengigheten til annen infrastruktur, levert av sivile tilbydere, avgjørende. Dette gjelder i første rekke strømtilførsel, men også annen funksjonalitet som oppvarming og kjøling. Vann- og avløpssystemer er et annet eksempel. Vi er usikre på om denne avhengigheten er tilstrekkelig vurdert og hensyntatt med tanke på den digitale grunnmurens funksjonalitet.

[34] Tilgjengelig tid og ressurser tillot ikke møter med Forsvarsbygg, Forsvarets sikkerhetsavdeling eller Nasjonal sikkerhetsmyndighet. Samtidig er EBA en relevant faktor vi ønsker å framheve i et helhetlig perspektiv.

Som påpekt i underkapittel 3.5, leveres deler av den digitale grunnmuren av sivile aktører, for eksempel tilbydere av elektroniske kommunikasjonstjenester (ekom). EBA knyttet til den digitale grunnmuren omfatter derfor bygningsmessig infrastruktur som er sivil. Dersom slik EBA inkluderer skjermingsverdige verdier i henhold til sikkerhetsloven (informasjon, informasjonssystemer, objekter og infrastruktur), stilles det spesielle lovmessige krav til sikring. Selv om sikkerhetsloven ikke skulle gjelde, kan viktigheten av EBA tilsi at fysisk og elektronisk sikring er nødvendig. Vi er usikre på om eventuelle behov for sikring av sivil EBA, i fred, krise og krig, er tilstrekkelig analysert i forsvarsektorens risikovurderinger knyttet til digital grunnmur, og særlig knyttet til kontraktsinngåelse med sivile leverandører. Figur 4.8 viser en oppsummering av mulige utfordringer innenfor faktoren EBA for Forsvarets digitale grunnmur.

Figur 4.8 Oppsummering av mulige utfordringer i nåsituasjonen innenfor faktoren EBA.

4.4 Prosesser og prosedyrer

Flere offentlige rapporter har poengtert utfordringer knyttet til prosesser og prosedyrer innenfor IKT-virksomheten. F24 har, som nevnt (underkapittel 4.1.5), besluttet å gjøre endringer i både styringen og innrettingen av forsvarssektoren (Forsvaret, 2023a). Endringene som følge av F24 er koblet sammen med prosesser og prosedyrer, som omhandler hvordan strukturen implementeres i beslutningstakningsprosesser.

Riksrevisjonen (2022, s. 14–15) hevder i sin rapport at rolleforståelse og gjennomføring påvirker styring innen flere områder:

> Aktørenes forståelse og praktisering av ansvars- og rollefordelingen framstår like fullt som en medvirkende årsak til svakhetene i sikkerhetsstyringen. […] IKT-virksomheten i Forsvaret og forsvarssektoren var for fragmentert og manglet helhetlig og enhetlig ledelse og styring, og at dette hadde ført til høye kostnader, lav gjennomføringsevne og mangelfull funksjonalitet. […] Etter Riksrevisjonens vurdering er det sterkt kritikkverdig at Forsvarsdepartementet, Forsvaret og Forsvarsmateriell i liten grad har klart å oppfylle de forventningene som ble stilt i forrige langtidsplan, hverken når det gjelder IKT-porteføljen eller styring og organisering. Sektoren erkjenner utfordringene på området, men evnen til å løse disse har vært begrenset.

Sitatet viser at Riksrevisjonen (2022) trekker fram svakheter innen sikkerhetsstyring, IKT-porteføljestyring – og styring og organisering generelt. Videre eksisterer det utfordringer med «Forsvarssektorens evne til å finansiere og drive styring og prioritering ved gjennomføring av IKT-prosjekter» (Forsvarsstaben, 2021).

IKT-strategien for forsvarssektoren (Forsvarsdepartementet, 2019a) nevner manglende styring av «kompetanse på tvers av sektoren og i prosjekter». Videre pekes det på delvis manglende opplæring innen IKT og at relevante ressurser ikke finner hverandre. Manglende kompetanse-utvikling og muligheter for faglig oppdatering er én av de vanligste sluttårsakene i Forsvaret (Fauske, 2023; Fauske & Strand, 2022).

Forsvarets IKT-strategi peker på utfordringer innen, og begrenset utnyttelse av, mulighetene som ligger i samarbeid og partnerskap med industrien (Forsvarsstaben, 2021).

Figur 4.9 viser en oppsummering av nåsituasjonen innenfor faktoren prosesser og prosedyrer for Forsvarets digitale grunnmur.

Figur 4.9 Oppsummering av identifiserte utfordringer i nåsituasjonen innenfor faktoren «prosesser og prosedyrer».

4.5 Mennesker

Med faktoren «mennesker» menes i denne studien individene som arbeider i IKT-virksomheten. I IKT-strategi for forsvarssektoren (Forsvarsdepartementet, 2019a) framkommer det at kompetanse på IKT i stort er for lav i sektoren. Videre sier IKT-strategien for forsvarssektoren at det eksisterer flere sterke fagmiljøer innen IKT, men at sektoren mangler kompetanse i et helhetsperspektiv:

> Kompetansegapet [i forsvarssektoren] må også sees i sammenheng med type kompetanse som er tilgjengelig i sektoren. Det eksisterer flere sterke fagmiljøer og dyktige medarbeidere innenfor IKT-området. Deres kompetanse er gjerne knyttet til drift av spesifikke systemer eller fagområder. Det er derimot behov for økt kompetanse til å kunne vurdere og utvikle disse systemene i et helhetsperspektiv. Kompetanse på integrasjon, samt digitalisering og bruk av data og analyse, er også mangelfull. (Forsvarsdepartementet, 2019a, s. 27)

Svendsen-utvalget (2020) ble oppnevnt av Forsvarsdepartementet i 2019, for å vurdere hvordan Forsvaret kan bedre evnen til å rekruttere, beholde, utvikle og avvikle kompetanse. Svendsen-utvalget (2020, s. 4) kommer med følgende nåtidsbeskrivelse:

> Det norske Forsvaret kan aldri bli størst. Derfor må det bli smartest og best på å kombinere menneske og teknologi ved å utnytte styrkene og kompetansemangfoldet i det norske samfunnet. […] Virkemidler som verneplikt, rekruttering, utdanning og utvikling må innrettes mot å understøtte fremtidens kompetansebehov. Det gjør de ikke i dag. […] Den sterke troen på at all kompetanse må utvikles internt hindrer Forsvarets utvikling. Fremover blir vi alle raskere utdatert, og halveringstiden på relevant kompetanse sies nå å være noen få år. Evnen til å lære blir derfor viktigere enn å kunne én spesifikk ting.

Fauske (2023) har gjennomført en spørreundersøkelse med respondenter fra Sjøforsvaret, Cyberforsvaret og Forsvarets personell- og vernepliktssenter. Hensikten med spørreundersøkelsen var å undersøke hva som vil være viktig kompetanse i framtiden i Forsvaret, hva som er status for slik kompetanse i Forsvaret i dag og hvorvidt organisasjonen er i stand til å oppdatere kompetansen i takt med teknologiutviklingen. Ifølge Fauske (2023, s. 82) mente rundt 80 % av respondentene i undersøkelsen at «bedre opplæring, større faglig fellesskap og mer samarbeid med andre i Forsvaret ville medføre at de [ansatte] kunne utført arbeidsoppgavene sine mer effektivt.». Videre viser undersøkelsen til Fauske (2023, s. 82) at «noen færre [enn 80 %], men fremdeles relativt mange, mente at en mer fleksibel organisasjonsstruktur og mer samarbeid med sivile aktører ville medført at de kunne utført arbeidsoppgavene sine mer effektivt». Dette stemmer overens med at en utflating av organisasjonens hierarkiske struktur kan knyttes til økt fleksibilitet, raskere og bedre informasjonsdelings- og beslutningstakningsprosesser (Alberts & Hayes, 2003, 2007; Bjørnstad & Lichacz, 2013).

Figur 4.10 viser en oppsummering av nåsituasjonen innenfor faktoren «mennesker» for Forsvarets digitale grunnmur.

Figur 4.10 Oppsummering av identifiserte utfordringer i nåsituasjonen innenfor faktoren «mennesker».

4.6 Kultur

Menneskefaktoren omhandler individnivået – og er for eksempel knyttet til den individuelle kompetansen; «For at Forsvaret skal kunne nyttiggjøre seg teknologi må det ha personell med innsikt i den teknologien som finnes, og den som kommer.» (Svendsen-utvalget, 2020, s. 82). Kulturfaktoren handler om å sette denne innsikten sammen til felles mønstre, verdier og oppfatninger som kan ses på tvers av individene (se f.eks. Jacobsen & Thorsvik, 2007; Schein, 2004). I underkapittel 3.8 refererte vi Diesen (2020) som hevder at institusjonell konservatisme har hindret modernisering av den norske forsvarsmodellen og spesielt forholdet til ny teknologi.

I Forsvaret eksisterer det subkulturer, både mellom grenene og innad i de ulike grenene. Svendsen-utvalget (2020, s. 56) skriver følgende: «Vi har forståelse for at det er mye kultur og identitet knyttet til de tre forsvarsgrenene. Samtidig er det viktig at ikke historien står i veien for å sikre et relevant forsvar for fremtiden.».

Forsvarskommisjonen uttaler at de sterke og grenvise ulike kulturene «har gjort det vanskelig å utøve sterkt og helhetlig lederskap.» (NOU 2023: 14, s. 58). Videre påpekes det at «[…] forsvarssektoren har slitt med effektiv gjennomføring av vedtak, og å komme seg ut av en tradisjon og kultur preget av nedskalering og negativ konkurranse mellom fagmiljøer.» (NOU 2023: 14, s. 70).

For nåsituasjonen ses det innenfor IKT-området utfordringer innen kultur ved at forsvars-sektoren har

> for svak kultur for endring og nytenkning, det vil si evne til å ta i bruk ny teknologi og endre ansattes adferd deretter. [….] IKT-området i forsvarssektoren har mangler i kompetanse og kultur for å kunne maksimere utbyttet av investeringer og redusere ledetid. (Forsvarsdepartementet, 2019a, s. 27)

Utsagnet støttes av Forsvarskommisjonen (NOU 2023: 14, s. 61), som sier at «Forsvarets personell, organisasjon og kultur har utfordringer med å henge med i [den teknologiske] utviklingen». Som sitatet viser, er kulturfaktoren koblet til andre faktorer i rammeverket. Kulturen, representert av felles mønstre av meninger og holdninger som gir seg utslag i bestemte måter å handle på, påvirkes eksempelvis av enkeltindividers kompetanse (inkl. holdninger). Det er også en gjensidig avhengighet mellom faktoren «kultur» og faktoren «prosesser og prosedyrer».

I Forsvarets IKT-strategi står det at «[d]et må bygges en kultur som fremmer teknologiforståelse og innovasjon.». Svendsen-utvalget (2020, s. 64) poengterer følgende:

> En organisasjon med høye endrings- og leveransekrav fremover trenger en sterk leder som kan bygge en samlende kultur og et vinnerlag. De beste vil jobbe for ledere med god innsikt og forståelse for fagområdet, som evner å løse komplekse problemstillinger, og som sitter lenge nok i stillingen til at endringen er implementert. Hvis ikke vil ikke personellet se nytteverdien av endring.

Figur 4.11 viser en oppsummering av nåsituasjonen innenfor faktoren «kultur» for Forsvarets digitale grunnmur.

Figur 4.11 Oppsummering av identifiserte utfordringer i nåsituasjonen innenfor faktoren «kultur».

4.7 Oppsummering av nåsituasjon for digital grunnmur

I underkapittel 4.1–4.6 har vi beskrevet faktorene fra vårt rammeverk for helhetlig perspektiv, for Forsvarets digitale grunnmur i dag. Figur 4.12 oppsummerer hovedpunktene fra kapittel 4.

Faktoren «organisasjon og mål» gir en kort oversikt over de formelle delene av organisasjonen, hentet fra styrende dokumenter organisasjonen selv har kontroll over. Videre inneholder faktoren en gjennomgang av mål fra offisielle dokumenter som IKT-strategi for Forsvaret, DRP og prinsipper fra Digitaliseringsstrategi for Forsvaret. I tillegg omtales mål fra F24. I figur 4.12 har vi også valgt å ta med forsvarssektorens klima og miljøstrategi samt IKT-strategi for forsvarssektoren. Forsvaret er en bidragsyter til disse dokumentene, men har ikke alene beslutningsmyndighet for innholdet i disse dokumentene. Samtidig er dokumentene relevante i nåsituasjonsbeskrivelsen, og er derfor inkludert i vår oppsummering.

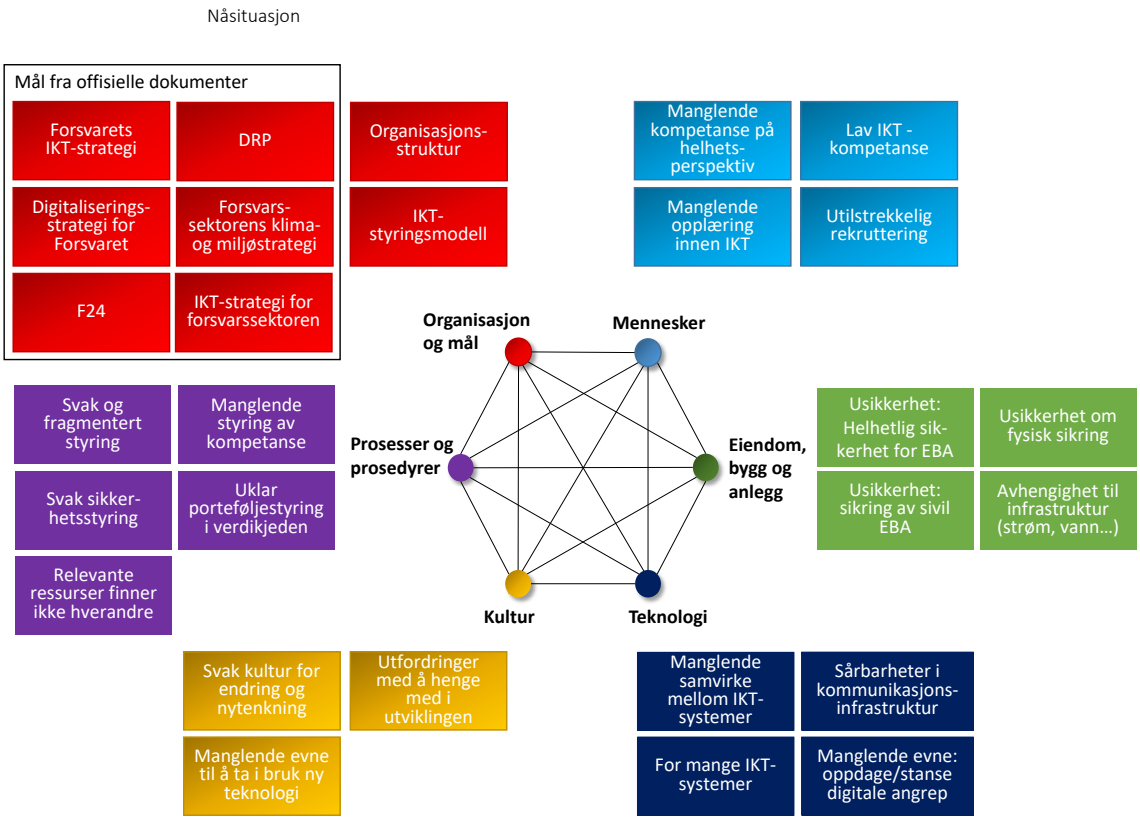
Teknologifaktoren i figur 4.12 viser oppsummert at det eksisterer manglende samvirke mellom IKT-systemer. Det eksisterer også for mange IKT-systemer, og det er sårbarheter i FKI. Videre viser nåsituasjonen manglende evne til å oppdage og stanse digitale angrep.

Behov for, og sikkerhet knyttet til, EBA er en faktor i helheten for digital grunnmur. Denne rapporten har ikke utført tilstrekkelige undersøkelser til å konkludere om nåsituasjonen for faktoren EBA, men peker på noen mulige utfordringer. Mulige utfordringer og usikkerheter for bygningsmessig infrastruktur i figur 4.12 er helhetlig sikkerhet, fysisk sikkerhet, avhengighet til annen infrastruktur (f.eks. strøm og vann), samt hvorvidt sivil EBA knyttet til digital grunnmur, har tilstrekkelig sikring.

Faktoren «prosesser og prosedyrer» i figur 4.12 viser at nåsituasjonen er preget av svak og fragmentert styring. Faktoren nevner spesielt sikkerhetsstyring og kompetansestyring. Videre preges nåsituasjonen av uklar porteføljestyring i verdikjeden og at relevante ressurser i virksomhetsprosessene ikke finner hverandre.

Menneskefaktoren i figur 4.12 viser at Forsvaret har behov for økt IKT-kompetanse med et helhetsperspektiv. I tillegg har Forsvaret manglende kompetanse på integrasjon, digitalisering samt bruk av data og analyse. Forsvaret har også manglende opplæring innen IKT, i tillegg til utilstrekkelig rekruttering.

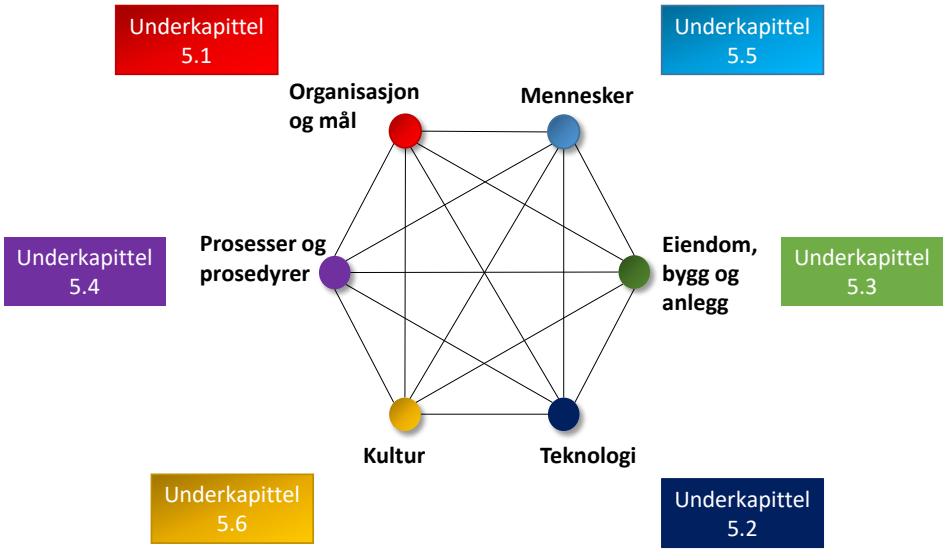
Nåsituasjonen innen faktoren «kultur» i figur 4.12 representeres gjennom felles mønstre som viser manglende evne til å ta bruk i ny teknologi og en svak kultur for endring og nytenkning. Vi har videre avdekket at det er utfordringer med å henge med i IKT-utviklingen.



Figur 4.12 Oppsummering av identifiserte utfordringer i nåsituasjonen for Forsvarets digitale grunnmur i et helhetlig perspektiv.

5 Forsvarets moderne og motstandsdyktige digitale grunnmur

I dette kapittelet beskriver vi Forsvarets moderne og motstandsdyktige digitale grunnmur i form av et sett av forslag, som vi har kommet fram til basert på resultatene fra vår dataanalyse[35]. Forslagene er kategorisert etter vårt helhetlige rammeverk. Figur 5.1 viser hvordan beskrivelsen av forslag til innhold i Forsvarets moderne og motstandsdyktige digitale grunnmur er fordelt på følgende underkapitler 5.1–5.6.



Figur 5.1 Beskrivelse av de seks faktorene i vårt rammeverk, fordelt på underkapitler.

5.1 Organisasjon og mål

Faktoren «organisasjon og mål» omhandler IKT-styringsmodell (inkl. organisasjonsstruktur samt roller, ansvar og myndighet) og mål fra styrende dokumenter Forsvaret selv har kontroll over. Overordnet ble det i beskrivelsen av nåsituasjonen pekt på utfordringer knyttet til silotilnærming og overlappende og uklare ansvarsforhold i IKT-virksomheten (se underkapittel 4.1).

5.1.1 Ha en entydig IKT-styringsmodell

Organisatoriske hindre for informasjonsdeling omhandler den formelle delen av organisasjonen, som organisasjonskartet og fordeling av roller, ansvar og myndighet i henhold til dette (Elstad, Lund, et al., 2022). Utfordringer knyttet til roller, ansvar og myndighet innenfor IKT-virksomheten som kan ha innvirkning på den digitale grunnmuren er poengtert i flere offentlige

[35] Vi har samlet inn data gjennom gruppesamtaler, workshops, sekundærdata og uformelle samtaler (se underkapittel 2.2). Hvordan vi gjennomførte selve dataanalysen er beskrevet i underkapittel 2.3. Hvordan vi har ivaretatt studiens validitet og reliabilitet gjennom dataanalysen er beskrevet i underkapittel 2.4.

dokumenter (se f.eks. Forsvarsdepartementet, 2019a; Riksrevisjonen, 2022). Våre informanter var også opptatt av disse utfordringene. Overordnet viser analysen vår at det er et behov for tydelig beskrivelse av roller, ansvar og myndighet innen IKT-virksomheten. Videre viser analysen vår at det er behov for oppdaterte styrende dokumenter, og at det ikke skal eksistere tvil om hvilke dokumenter som er gjeldende.

Nåsituasjonen (beskrevet i kapittel 4) og analysen vår indikerer behov for en tydelig ansvarsfordeling mellom forsvarssektoren og etablerte samarbeidspartnere. Etablerte samarbeidspartnere kan være strategiske partnere, leverandører av skytjenester og datasentre. IKT-styringsmodell må derfor beskrive de ulike aktørene i IKT-virksomhetens rolle, ansvar og myndighet for IKT generelt og den digitale grunnmuren spesielt.

Tydeligere rollefordeling mellom forsvarssektoren og samarbeidspartnere kan også ses i sammenheng med stadig økende kompleksitet og omfang på de digitale verdikjedene.
En digital verdikjede er

> […] en struktur av leveranser mellom virksomheter, hvor hver leveranse enten er en digital tjeneste, software eller hardware. En oversikt over en digital verdikjede består derfor i en oversikt over en fysisk infrastruktur, samt hvem som eier, vedlikeholder og opererer de forskjellige delene av denne. Videre vil den bestå av en oversikt over hvilke digitale tjenester som utveksles mellom de forskjellige delene, samt hvilken hardware og software som inngår. (Lysne, 2020, s. 10)

IKT-styringsmodell (inkl. i faktoren «organisasjon og mål») er knyttet sammen med de andre faktorene i vårt helhetlige rammeverk. Det er IKT-styringsmodell som setter den formelle strukturen for IKT-virksomheten, mens gjennomføringen av virksomhetsprosessene i praksis er representert i faktoren «prosesser og prosedyrer». IKT-styringsmodell må derfor være utformet på en slik måte at den legger til rette for effektiv utførelse av prosesser og prosedyrer. I tillegg er IKT-styringsmodell knyttet sammen med menneskefaktoren i vårt rammeverk, hvor for eksempel personlig kompetanse, inkludert holdning til IKT-styringsmodell står sentralt. I tillegg vil kulturfaktoren i vårt rammeverk ha innvirkning gjennom felles mønstre av meninger og holdninger som gir seg utslag i bestemte måter å sette IKT-styringsmodellen ut i praksis på.

Økonomien, og de finansielle rammene, må stemme overens med ønsket ambisjonsnivå og gjennomføring av prosesser innen utvikling, drift og vedlikehold. Hvilke IKT-tjenester den digitale grunnmuren tilbyr vil ha innvirkning på finansieringsbehovet til grunnmuren. Samtidig vil de økonomiske rammene også kunne påvirke hvilke IKT-tjenester den digitale grunnmuren kan tilby. Jo mer omfattende grunnmuren er jo høyere vil kostnadene normalt bli. Samtidig vil applikasjonstjenestene som kjører på grunnmuren kunne gjøres enklere, fordi de utnytter funksjoner i grunnmuren i stedet for å implementere dem selv. Dermed kan applikasjonstjenestene potensielt bli billigere. Generelt må det velges kostnadseffektive løsninger, for å sikre en økonomisk bærekraftig digital grunnmur.

IKT-porteføljestyringen i Forsvaret må tilrettelegge for tilstrekkelig finansiering for å opprettholde IKT-tjenestene i grunnmuren. Samtidig vil ønsker om fleksibilitet, automatisering, inter-

operabilitet og miljøvennlighet kunne påvirke finansieringsbehovet. Eksempelvis vil økt grad av automatisering kunne redusere personellbehov, og økt robusthet kunne bidra til å redusere tid brukt på gjenoppretting.

5.1.2 Etablere mål for alle faktorene i vårt rammeverk

Målene som angis i DRP (Forsvarsstaben, 2023) vektlegger teknologiske aspekter, og mangler de resterende faktorene i vårt rammeverk. De teknologiske kapabilitetene en moderne og motstandsdyktig digital grunnmur må inneha er bare én brikke i helheten. For det første må det være samsvar mellom faktorene «teknologi» og «prosesser og prosedyrer» i organisasjonen, og dette må gjenspeiles i målene. IKT er integrert i de fleste virksomhetsprosesser i dag, og er derfor avgjørende for verdiskaping og bærekraft. Videre vil det ikke være nok for operasjonaliseringen av de teknologiske kapabilitetene at disse er beskrevet og implementert – dersom organisasjonskulturen ikke støtter opp om for eksempel fleksibilitet og endringstakten de teknologiske kapabilitetene legger opp til. Det samme gjelder dersom det er mangel på kompetanse eller mangler innenfor EBA.

I Forsvarets IKT-strategi poengterer Forsvaret selv at

> For at Forsvaret skal være i stand til å realisere de mulighetene teknologi gir må organisasjonen ha gjennomgående digital kompetanse. Behovet for kompetanse og digital modenhet spenner fra basisforståelse av tekniske termer og digital sikkerhet, og forståelse for hvordan IKT kan effektivisere arbeidsprosesser, til kompetanse knyttet til å bestille, utnytte og forstå eksterne IKT-tjenester. Dette er faktorer Forsvaret må ta hensyn til i arbeidet med å rekruttere, videreutvikle og beholde tilstrekkelig sivil og militær kompetanse innenfor området.

Vår studie støtter opp om disse poengene. Menneskefaktoren, inkludert kompetanse, er en del av helheten for å kunne oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur. Teknologien vil gjøre at kompetansebehovet til personellet vil endre seg, og ulike nye behov for spesialistkompetanse vil dukke opp. Kompetansen menneskene bruker til å utføre aktiviteter som kan automatiseres blir mindre viktig i framtiden (Fauske, 2023). Evne til å tilegne seg ny kompetanse og omstille seg, teknologisk/digital kompetanse, evne til å kommunisere og samarbeide med andre mennesker, omsorg og empati samt kreativitet vektlegges som framtidsviktig kompetanse (Fauske, 2023). Det vil derfor også være et behov for å etablere mål innenfor de andre faktorene i vårt rammeverk for den digitale grunnmuren.

5.2 Teknologi

Vi har identifisert seks overordnede teknologiske kapabiliteter som en moderne og motstandsdyktig digital grunnmur for Forsvaret bør inneha.

5.2.1 Tilby et tilstrekkelig og relevant sett av IKT-tjenester

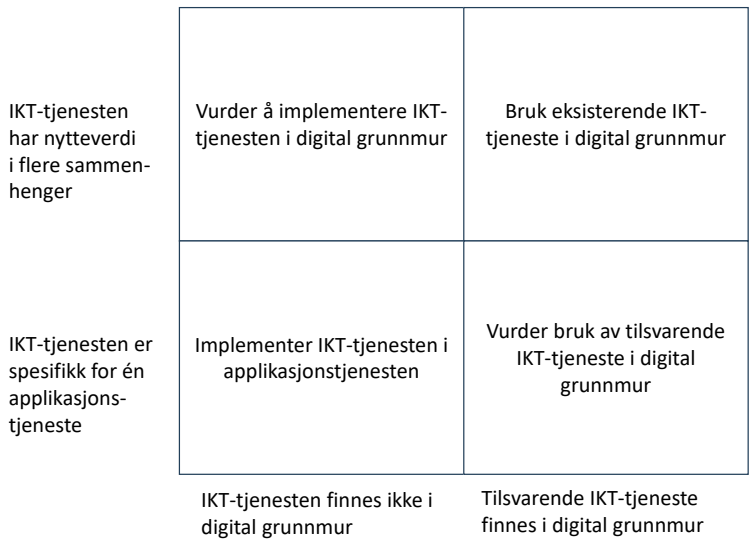
Den digitale grunnmuren må understøtte alle relevante applikasjonstjenester

DRP inkluderer mål om at digital grunnmur er en felles IKT-løsning for hele forsvarssektoren. Vår analyse viser at den digitale grunnmuren bør inkludere så mye som mulig av felles IKT-tjenester som ellers har vært implementert i hver enkelt applikasjonstjeneste. Dette er også i tråd med DRPs prinsipp om behovsprøving og variantbegrensning samt prinsippet om interoperabilitet, hvor standardisering er vesentlig.

Noen av våre informanter i forsvarssektoren mente at variantbegrensning bør håndheves strengt for digital grunnmur og dennes IKT-tjenester, men mindre strengt for applikasjonstjenestene. Begrunnelsen var at en for streng variantbegrensning av applikasjonstjenestene kan gå ut over organisasjonen sin evne til utvikling, innovasjon og smidighet. Dette er utsagn vi støtter.

I tillegg viser analysen vår at det må utarbeides prinsipper for hvilke funksjoner applikasjonstjenestene skal kunne tilby. Et mulig prinsipp kan være at dersom en IKT-tjeneste allerede tilbys av den digitale grunnmuren skal en applikasjonstjeneste ikke implementere denne på nytt, men i stedet benytte IKT-tjenesten som tilbys av grunnmuren. Vi mener det er behov for en tydeliggjøring av hvilke IKT-tjenester dette dreier seg om. Et råd er derfor at det bør gjennomføres en analyse hvor graden av felles nytte ses opp mot individuelle særbehov, som vist i figur 5.2.

En slik type kartlegging (figur 5.2) vil kunne avdekke hvor organisasjonen kan ha frihet og hvor det er behov for tydeligere føringer. Kartleggingen vil måtte ha en helhetlig tankegang, og inkludere bruksområder til teknologien og hvilke behov teknologien skal dekke. Ett av behovene kan være knyttet til gjenbruk av data, et annet kan være behovet for lokal autonomi.



Figur 5.2 Eksempel på mulig analyse av IKT-tjenester med tanke på plassering av disse.

Den digitale grunnmuren må muliggjøre moderne IKT-tjenester

Den digitale grunnmuren må legge til rette for moderne IKT-tjenester, både i grunnmuren selv, i applikasjonstjenestene som benytter grunnmuren, i utvikling, drift og vedlikehold og i forsvar mot angrep. Hva som er moderne IKT-tjenester vil endre seg fortløpende, grunnet den raske teknologiske utviklingen.

Analysen vår viser at skyteknologi er vesentlig for å kunne realisere en moderne og motstandsdyktig digital grunnmur. Et eksempel er bruk av programvaredefinerte datasentre (*Software-defined data center*). Slik teknologi vil gjøre det mulig for Forsvaret å definere virtuelle datasentre (prosesserings-, lagrings- og nettverksressurser) ved hjelp av programvare (IBM, u.d.; IONOS, 2023). Endringer kan gjøres enkelt og raskt – og kapasiteten kan skaleres opp eller ned etter behov, noe DRP (Forsvarsstaben, 2023) støtter opp om i sine prinsipper.

Videre bør den digitale grunnmuren muliggjøre bruk av KI der det er hensiktsmessig – både for grunnmurens egne IKT-tjenester, for applikasjonstjenester som kjører på grunnmuren, for mest mulig automatisert drift og for effektivt forsvar mot angrep. Strategi for kunstig intelligens i forsvarssektoren (Forsvarsdepartementet, 2023b) inkluderer mål og ambisjoner for bruk av KI for sektoren, og disse er også er relevante for den digitale grunnmuren.

Oppsummert mener vi at den digitale grunnmurens IKT-tjenester må bygge på skyteknologi[36] og muliggjøre KI der det er hensiktsmessig. For øvrig må grunnmuren inkludere effektive IKT-tjenester og tiltak for å ivareta et forsvarlig sikkerhetsnivå. Vi beskriver forsvarlig sikkerhetsnivå nærmere i underkapittel 5.2.5.

Den digitale grunnmuren må kunne håndtere og utnytte store mengder data

Ifølge strategi for kunstig intelligens i forsvarssektoren (Forsvarsdepartementet, 2023b) skal sektoren søke å fange alle data av verdi som produseres i sektoren. Dette støttes opp om av IKT-innsatsområdene «Helhetlig K2» og «Dele og utnytte informasjon og data» i DRP (Forsvarsstaben, 2023). Den digitale grunnmuren må ha evne til å støtte applikasjonstjenester basert på KI. KI-tjenester kan både benyttes innen operasjoner, for eksempel til beslutningsstøtte til operasjoner eller innen defensive cyberoperasjoner (Forsvaret, 2022) og innen virksomhetsstyring.

5.2.2 Fremme interoperabilitet

Den digitale grunnmuren må legge til rette for informasjonsdeling mellom samarbeidspartnere – i hele krisespekteret

Forsvaret har i dag begrenset evne til gjennomgående digital informasjonsdeling både internt og med samarbeidspartnere (se f.eks. Elstad, Lund, et al., 2022). En framtidig grunnmur må derfor

[36] Virtualisering, mikrotjenester og orkestreringsrammeverk. Virtualisering er relevant for alle deler av den digitale grunnmuren – IT-plattform, infrastruktur- og kommunikasjonstjenester.

legge til rette for og inneha føringer som sikrer informasjonsdeling mellom samarbeidspartnere, som ivaretar forsvarlig sikkerhetsnivå.

Det er behov for å lette informasjonsdeling innad i totalforsvaret: «[…] totalforsvarsaktørenes evne til effektiv krisehåndtering er avhengig av koordinering, samarbeid og situasjonsforståelse som grunnlag for beslutninger» (Endregard & Rongved, 2022, s. 175). Grunnmuren bør derfor legge til rette for gradert informasjonsdeling i totalforsvaret, der totalforsvarsaktørene har behov for dette. Gjennom Nasjonalt beredskapssystem (Beredskapssystem for forsvarssektoren (BFF) og Sivilt beredskapssystem (SBS)), underliggende planverk sammen med Forsvarets skarpe planverk og sivil-militære samarbeidsavtaler, kan det utledes hvilke sivile totalforsvarsaktører som har behov for informasjonsdeling med Forsvaret og på hvilket graderingsnivå – og legge til rette for dette. Et forsvarlig sikkerhetsnivå må ivaretas i denne samhandlingen (se også underkapittel 5.2.5 og underkapittel 5.4.4).

Videre må den digitale grunnmuren legge til rette for teknisk interoperabilitet mellom totalforsvarsaktører og allierte partnere. For eksempel er dette nødvendig ved mottak av allierte styrker i Norge. IKT-innsatsområdet «Samvirke med allierte og totalforsvaret» i DRP (Forsvarsstaben, 2023) inkluderer mål om føderert samhandling med allierte, muligheter for standardiserte sammenkoblinger i totalforsvaret samt alliert mottak og tilstedeværelse. Oppsummert viser analysen at utviklingen av den digitale grunnmuren blir en sentral faktor for å kunne nå disse målene.

Den digitale grunnmuren må støtte effektiv tilkobling via moderne grensesnitt

Den digitale grunnmuren må støtte effektiv tilkobling via moderne grensesnitt jamfør DRPs (Forsvarsstaben, 2023) prinsipp om interoperabilitet. Prinsippet sier at standardiserte dataformater, protokoller og grensesnitt skal benyttes så langt det er hensiktsmessig. Interoperabilitetsprinsippet henger sammen med DRP-prinsippet om løse koblinger – for ivaretakelse av endringstakt i den digitale grunnmuren – med nødvendig grad av uavhengighet.

Grunnmuren må tilby løsninger for tilkobling av ulike aktørers utstyr, slik at applikasjonstjenestene og andre nettverk (f.eks. tilhørende allierte eller sivile samarbeidspartnere) så enkelt og raskt som mulig, kan kobles til grunnmuren. Disse tilkoblingsløsningene må være sikre. I henhold til DRP er den digitale grunnmuren en premissgiver for enheter som skal kobles til grunnmuren. Den digitale grunnmuren må også stemme overens med relevante FMN-spesifikasjoner, jamfør Forsvarets IKT-strategi (Forsvarsstaben, 2021).

5.2.3 Fremme fleksibilitet

Den digitale grunnmuren må kunne moderniseres kontinuerlig

Modernisering av den digitale grunnmuren må være et kontinuerlig arbeid og grunnmuren vil inneholde både gammel og ny IKT over tid. Det å kunne bytte ut IKT-tjenester på en enkel måte legger til rette for innovasjon. Dersom det er behov for kritiske oppdateringer i grunnmuren på kort sikt, må ikke slike oppdateringer være til hinder for senere modernisering.

Den digitale grunnmuren må kunne tilpasses raskt nok når behov endrer seg

Den digitale grunnmuren må raskt nok kunne tilpasses endrede behov samtidig som et forsvarlig sikkerhetsnivå opprettholdes. Tilpasning av grunnmuren til en oppstått situasjon kan for eksempel innebære at data og/eller IKT-tjenester flyttes geografisk eller virtuelt – eventuelt også ut av landet eller til en offentlig sky hvis det er nødvendig. Grunnmuren bør inneholde mekanismer som kan bidra til «lokal autonomi», slik at Forsvaret og eventuelle samarbeidspartnere kan få tilgang til IKT-tjenester der de opererer, også uten forbindelse til sentraliserte IKT-tjenester. Dette er nødvendig for enkelt å kunne reetablere evne til å utveksle informasjon lokalt selv om forbindelsen til den øvrige digital grunnmuren skulle forsvinne.

Mottak av allierte styrker i Norge er et eksempel på en situasjon der skalerbarhet er relevant for den digitale grunnmuren. Grunnmuren må kunne differensiere trafikk, for eksempel for å kunne sikre at enheter som krever høy overføringskapasitet får dette til rett tid. Grunnmuren trenger derfor mekanismer for dynamisk prioritering og tildeling av kapasitet. Moderne teknologier basert på virtualisering[37] kan bidra til å realisere behovene som er eksemplifisert over.

5.2.4 Støtte og ivareta effektiv utvikling, drift og vedlikehold

Den digitale grunnmuren sine løsninger for styring og kontroll må håndtere kompleksitet

Den framtidige digitale grunnmuren vil være et komplekst system av systemer, med ulike teknologier og ulikt eierskap. Den vil inneholde både teknologisk arv og moderne IKT-tjenester basert på ulike teknologier, og den vil inneholde IKT-tjenester som dels eies av forsvarssektoren og dels av sivile leverandører. I tillegg vil grunnmuren ha grensesnitt mot en rekke ulike informasjonssystemer, tilhørende forsvarssektoren selv, sivile samarbeidspartnere og allierte samarbeidspartnere. IKT-tjenestene for styring og kontroll av den digitale grunnmuren må kunne håndtere en slik kompleksitet. Dette krever samvirke mellom IKT-tjenestene for styring og kontroll av forskjellige (del)systemer, både innenfor og utenfor den digitale grunnmuren.

Bruk av skyteknologi i den digitale grunnmuren muliggjør en moderne driftsmodell basert på DevSecOps (*Development, Security, and Operations*). Kjernen i en slik driftsmodell vil være én eller flere grupper som vedlikeholder programkode for å levere grunnmurstjenester, enten på infrastruktur eller IT-plattformnivå (Microsoft, u.d.-b). I tillegg inkluderer det evne til å integrere sikkerhet i hele livsløpet.

For å kunne gjøre de endringene som er nødvendige når grunnmuren blir angrepet, må løsningene for styring og kontroll kunne fungere godt sammen med løsningene for å forsvare grunnmuren (se underkapittel 5.2.5).

[37] Virtualisering innebærer å emulere (etterlikne) fysisk maskinvare ved hjelp av programvare. Programvaren som kjører på den emulerte maskinvaren, vil normalt ikke vite at den ikke kjører på fysisk maskinvare. (Nätt, 2023).

Den digitale grunnmuren sine løsninger for styring og kontroll må støtte både raske endringer og kontinuerlig modernisering

Under en militær operasjon kan det bli behov for å gjøre raske og omfattende endringer i den digitale grunnmuren for å sikre tilgang til nødvendige IKT-tjenester. Grunnmurens løsninger for styring og kontroll må kunne gjøre slike endringer innenfor de kravene som gjelder for tidsbruk og ytelse i den militære operasjonen, samtidig som grunnmuren holder seg stabil. Slike raske og omfattende endringer kan også kreve IKT-tjenester i grunnmuren som raskt gjør det mulig å endre ressurstildelinger, informere tilgrensende applikasjonstjenester og håndtere sikkerhet.

Den digitale grunnmuren sine løsninger for styring og kontroll bør være mest mulig automatiserte

Grunnmuren bør ha mest mulig automatiserte løsninger for styring og kontroll, slik at behovet for manuell inngripen minimeres. Den framtidige digitale grunnmuren vil utvikle seg til å bli et komplekst system av systemer. Styring og kontroll av grunnmuren må derfor forventes å bli utfordrende, kanskje umulig, å gjøre manuelt på en hensiktsmessig måte. Analysen viser at det derfor er nødvendig at den digitale grunnmuren legger til rette for KI-baserte tjenester for styring og kontroll. For eksempel kan slike KI-baserte tjenester gi mulighet for raskt å opprette en hensiktsmessig ny forbindelse hvis det oppstår brudd i en eksisterende forbindelse. En slik automatisering kan imidlertid åpne opp for nye sårbarheter. Vi kommer nærmere inn på sikkerhetsaspekter i underkapittel 5.2.5.

5.2.5 Ha et forsvarlig sikkerhetsnivå

Den digitale grunnmuren må ha teknologiske sikkerhetstiltak som ivaretar et forsvarlig sikkerhetsnivå

Vår analyse viser at grunnmuren må ha effektive teknologiske sikkerhetsmekanismer. Formålet med disse mekanismene er å sørge for at den digitale grunnmuren er motstandsdyktig mot både tilsiktede og utilsiktede hendelser og har et akseptabelt risikonivå der hensynet til forsvarssektorens ulike verdier balanseres. Motstandsdyktighet inkluderer både robusthet og redundans (Cyberforsvaret, 2020). Sikkerhetsloven (2018) krever at det skal etableres et forsvarlig sikkerhetsnivå for skjermingsverdige verdier basert på vurderinger av risiko. Teknologisk sett må derfor den digitale grunnmuren være både robust og redundant og samtidig ivareta sikkerhetsegenskapene konfidensialitet, integritet og tilgjengelighet.

Den digitale grunnmuren må ivareta sikkerhetsegenskapene konfidensialitet, integritet og tilgjengelighet

For å kunne styre risiko og sikkerhet for den digitale grunnmuren som en helhet, bør det klargjøres hvilke IKT-tjenester som er en del av grunnmuren og hvilke IKT-tjenester som er tilgrensende. En slik oversikt kan baseres på Natos C3-taksonomi (Nato, 2021). Det er også nødvendig å forstå hvordan de ulike bestanddelene av grunnmuren henger sammen. Dette vil bidra til å svare ut Riksrevisjonens kritikk (2022) om manglende oversikt på IKT-området. Videre bør

det etableres tydelige og gjensidige krav til grensesnittene for tilkobling av ulike IKT-systemer til grunnmuren.

NSM har etablert et sett med grunnprinsipper for IKT-sikkerhet, hvor formålet er å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk gjennom å etablere sikkerhetsfunksjonalitet (Nasjonal sikkerhetsmyndighet, 2020a):

- *identifisere og kartlegge*, dvs. skaffe oversikt,
- *beskytte og opprettholde*, dvs. ivareta forsvarlig sikring,
- *oppdage*, dvs. oppdage og fjerne kjente sårbarheter og trusler og etablere sikkerhetsovervåkning, og
- *håndtere og gjenopprette*, dvs. håndtere sikkerhetshendelser.

Disse grunnprinsippene og de konkrete teknologiske rådene NSM gir, er et godt utgangspunkt for å etablere et grunnleggende sikkerhetsnivå.

Den digitale grunnmuren må ivareta ulike sikkerhetsdomener, siden operative behov tilsier at informasjon må kunne utveksles mellom informasjonssystemer med ulike graderingsnivåer, inkludert evnen til å utveksle informasjon med sivile informasjonssystemer. Sikker informasjonsutveksling (SIU-er) og andre teknologiske løsninger for informasjonsutveksling vil være nødvendige og inngår som en del av grunnmuren.

Å etablere teknologiske løsninger for overvåkning og deteksjon i den digitale grunnmuren er avgjørende for å oppdage uautorisert tilgang og kunne forebygge og håndtere sikkerhetstruende virksomhet slik som etterretning og sabotasje mot informasjonssystemene. Dette er blant annet presisert i NSMs grunnprinsipper (Nasjonal sikkerhetsmyndighet, 2020a). Grunnmuren må derfor ha effektiv identitetshåndtering og tilgangsstyring for å ivareta sikkerhetsegenskapene, inkludert å autentisere og kontrollere aktører som ønsker å koble seg til grunnmuren. Dette er en forutsetning for at data skal kunne gjøres tilgjengelig, deles sikkert, og ved behov lagres og prosesseres i grunnmuren istedenfor i hver enkelt applikasjonstjeneste. Den digitale grunnmuren kan videre inneholde både sensorer og mulighet for stordataanalyser for deteksjon og hendelseshåndtering. For eksempel kan KI-baserte tjenester brukes for å oppdage unormal aktivitet.

Den digitale grunnmuren må være motstandsdyktig mot manipulering av data. Grunnmuren må ivareta sikkerhetsegenskapene, det vil si konfidensialitet, integritet og tilgjengelighet. Integritetsperspektivet blir stadig viktigere, spesielt ved automatisert behandling av data.

Den digitale grunnmuren må ivareta sikkerhet i hele utviklingsløpet

Det er viktig å tenke sikkerhet på en helhetlig måte og tidlig nok i forbindelse med utvikling av grunnmuren. DevSecOps er for tiden et mye brukt begrep som indikerer at utvikling, sikkerhet og drift/operasjon bør foregå side om side gjennom hele levetiden til et informasjonssystem. IKT-innsatsområdet «Forsvarlig sikkerhetsnivå» i DRP (Forsvarsstaben, 2023) inkluderer mål om evne til DevSecOps.

IKT-systemer basert på skyteknologi kan etableres i en offentlig eller en privat sky. Sikkerhetsgraderingen på informasjonen som skal behandles vil påvirke hvordan IKT-systemet bør utformes og om det bør etableres i en offentlig eller privat sky. Forsvarssektoren må derfor vurdere hvor det vil være forsvarlig å ta i bruk skytjenester for gradert, særlig høygradert, informasjon.

Den digitale grunnmuren må ha hensiktsmessige kryptoløsninger

Riktig bruk av kryptografi er en nødvendig forutsetning for sikkerhet, men kryptografi er aldri verken tilstrekkelig eller et mål i selv. I Forsvaret forbindes kryptografi først og fremst med fysiske bokser som utgjør grensen mellom gradert og ugradert side, eller potensielt mellom autorisasjonsskiller. Disse boksene bruker symmetriske kryptoalgoritmer som gir innholdet konfidensialitet og integritet mens det fraktes over det ugraderte nettet. Disse boksene er nødvendige på grunn av regulatoriske krav til kryptomekanismer, som igjen følger fra kunnskap om sikker implementasjon.

Dersom man skal oppnå mulighetene som skisseres med programvaredefinerte nettverk og datasentre, vil kryptoløsningene i dagens digitale grunnmur bli for lite fleksible. Det kan derfor være nødvendig å undersøke konsekvensene av å tillate kryptering med programvare, og hvordan mulige forbedringer når det gjelder tilgjengelighet og fleksibilitet – som kan ha positive følger for systemsikkerheten – skal veies mot mulige lempinger på den spesifikke sikkerheten ved kryptoforvaltningen. Den digitale grunnmuren må også legge til rette for at kryptografi alltid skal brukes for ugraderte data.

Asymmetrisk kryptografi går gjennom et paradigmeskifte i dag, der eksisterende algoritmer skal pensjoneres og nye algoritmer som ikke er sårbare mot kvantedatamaskiner skal fases inn (Strand, 2023). Så vidt vi vet bruker Forsvaret i liten grad asymmetrisk kryptografi i dag. Den digitale grunnmuren må legge til rette for fortløpende nøkkelutvekslinger i framtiden, slik at verdien av hver enkelt nøkkel blir betydelig mindre. Vi må også ta høyde for endringer i framtiden, så grunnmuren må ha *kryptosmidighet*[38].

Utover den vanlige sikringen av kommunikasjon mellom to likeverdige parter, kan kryptografi også bidra til andre sikkerhetsmål. Med attributtbasert kryptering (ABE) (Goyal et al., 2006) kan man for eksempel merke dataene, slik at kryptografien i seg selv håndhever graderings- og autorisasjonsskiller. Bare IKT-tjenester og brukere som har de riktige nøklene kan da dekryptere informasjonen. ABE er ikke tilstrekkelig modent i dag, men vil med nødvendig utvikling og sertifisering kunne løse mange problemer knyttet til datasentrisk sikkerhet.

Tradisjonelt sett har organisasjoner primært sikret nettverkene sine gjennom perimetersikring. Strenge brannmurer og internettprotokollfiltreringer skiller det bedriftsinterne nettverket fra omverdenen: Alle på innsiden får uhindret (ev. behovsbasert) tilgang til alle tjenester, de på utsiden

[38] Kryptosmidighet innebærer å ta høyde for at det over tid kan være nødvendig å rette implementasjonsfeil, oppdatere parametere eller kanskje bytte ut en kryptoalgoritme fullstendig, men med det samme grensesnittet.

har ingen tilgang. Ved hjelp av VPN (*virtual private network*)-tjenester kan man få tilgang til det indre nettverket hjemmefra.

Denne modellen taper nå terreng for nulltillitsarkitektur (Zero Trust Architecture, ZTA), der en har som grunnantakelse at angriperen har tilgang på nettverket. Konsekvensen er at en tilfeldig datamaskin på nettverket ikke skal kunne ha mulighet til å utføre uautoriserte handlinger. I tillegg må alle IKT-systemer til enhver tid kunne verifisere (1) brukeren og dennes rettigheter og (2) datamaskinen til brukeren. National Institute of Standards and Technology (NIST) i USA har skrevet utførlig om nulltillitsarkitektur (National Institute of Standards and Technology (NIST), 2020), og president Biden har beordret at all offentlig nyutvikling i USA skal bruke ZTA (The White House, 2021).

Riktig bruk av kryptografi, også internt i nettverkene, er en nødvendig betingelse for å sikre at informasjon og rettigheter forbeholdes autoriserte brukere og IKT-systemer.

5.2.6 Ivareta klima og miljø

Som nevnt i underkapittel 3.9.4 har forsvarssektoren gitt ut en egen klima- og miljøstrategi (Forsvaret et al., 2022), som sier at forsvarssektoren må ivareta klima og miljø når den anskaffer, bruker, utvikler, drifter, vedlikeholder og faser ut bestanddeler i grunnmuren. Inspirasjon til dette underkapittelet er hentet fra Forsvaret et al. (2022), Arnfinnsson og Tønsberg (2023), Arnfinnsson og Kirkhorn (2021) og Granlund et al. (2022).

Den digitale grunnmuren må belaste klima og miljø minst mulig

Den digitale grunnmuren bør kunne legge til rette for nye og innovative IKT-løsninger som kan endre måten Forsvaret og sektoren opererer på, slik at klima- og miljøbelastningen blir mindre. Forsvaret må stille tekniske miljøkrav ved anskaffelse av bestanddeler i den digitale grunnmuren, og klima og miljø må vurderes ved anskaffelser sammen med de tradisjonelle aspektene tid, kost og ytelse (Forsvaret et al., 2022). Dette inkluderer å være bevisst på miljøprofilen til samarbeidspartnere. Slik kan inkludering av nye bestanddeler i grunnmuren bidra til at grunnmuren, i et livsløpsperspektiv, får lavest mulig klima- og miljøbelastning.

Grunnmuren bør være mest mulig energieffektiv, den bør ha lavest mulig energiforbruk og den bør i størst mulig grad kunne benytte fornybare energikilder. Før teknologi som krever mye energi eventuelt inkluderes i grunnmuren, bør nytten av teknologien vurderes opp mot energiforbruket og hvilke energikilder som er tilgjengelige.

Videre bør bruk, utvikling, drift, vedlikehold og utfasing av bestanddeler i grunnmuren bidra minst mulig til uønsket miljøpåvirkning i form av giftstoffer, støy, terrenginngrep og annen forurensning. Et eksempel på forurensning er bruk av helikopter eller snøscooter for vedlikehold på vanskelig tilgjengelige lokasjoner.

Den digitale grunnmuren må legge til rette for mest mulig sirkulær økonomi, det vil si minst mulig bruk og kast av bestanddeler i grunnmuren. Når bestanddeler i grunnmuren kommer til

enden av livsløpet, må de kunne avhendes på en ansvarlig måte. For å minimere avfall må mest mulig av bestanddelene som avhendes resirkuleres.

Den digitale grunnmuren må tilpasses et endret klima

Forsvarssektorens klima- og miljøstrategi (Forsvaret et al., 2022) sier at organisasjonen må tilpasses et endret klima. Dette gjelder også for den digitale grunnmuren. Grunnmuren må kunne fortsette å fungere selv om det oppstår hendelser som for eksempel ekstremvær, flom eller skred. Grunnmuren må derfor forberedes for videre endringer i klima, og dette vil kunne påvirke utvikling (inkludert anskaffelser), drift og vedlikehold av grunnmuren. Slike tilpasninger til klimaendringer er nødvendig for at grunnmuren skal ha tilstrekkelig robusthet og redundans (motstandsdyktighet) mot uønskede hendelser.

5.2.7 Oppsummering

Forsvarets moderne og motstandsdyktige digitale grunnmur må ha følgende seks teknologiske kapabiliteter:

Figur 5.3 Oversikt over de seks teknologiske kapabilitetene Forsvarets moderne og motstandsdyktige digitale grunnmur må inneha, i tillegg til en detaljering av disse.

5.3 Eiendom, bygg og anlegg

EBA omfatter de stasjonære fysiske installasjonene som benyttes av forsvarssektoren for utvikling, drift, vedlikehold og sikkerhet for den fysiske IKT-infrastrukturen som inngår i digital grunnmur. EBA som benyttes i sammenheng med en digital grunnmur, bør inneha flere egenskaper knyttet til egnethet og sikkerhet. Utgangspunktet for krav til EBA er operative evner og de funksjonene knyttet til digital grunnmur som EBA er der for å ivareta i fred, krise og krig.

5.3.1 Ha sikkerhet mot tilsiktede og utilsiktede hendelser

Grunnlaget for sikkerhetstiltak knyttet til EBA bør være basert på helhetlige verdi- og risikobaserte vurderinger og inngå i den helhetlige risiko- og sikkerhetsstyringen for den digitale grunnmuren (se også underkapittel 5.4.4). Vi har identifisert tre nødvendige kapabiliteter:

(1) Forebyggende sikkerhetstiltak for å motvirke sikkerhetstruende aktiviteter mot nasjonale sikkerhetsinteresser, det vil si spionasje, sabotasje, kriminalitet og terror, i hele krisespekteret. Forebyggende sikkerhetstiltak omfatter både digital sikkerhet, fysisk sikkerhet og personellsikkerhet.

(2) Sikre robusthet mot utilsiktede hendelser slik som naturhendelser og ulykker, og sørge for at EBA opprettholder sin understøttende funksjon for den digitale grunnmuren. Det inkluderer også tilkobling til annen infrastruktur slik som kraftforsyning, vann og avløpstjenester og fysisk tilgang via vei. Hvor EBA og annen fysisk infrastruktur plasseres, bør inngå i risikovurderinger. Basert på slike vurderinger kan det være nødvendig å iverksette tiltak for å beskytte den digitale grunnmuren mot uønskede effekter. Å ta hensyn til klimaendringer, er en viktig faktor som bør inngå.

(3) Redundans og gjenopprettingsevne for kritisk EBA, uavhengig av type uønsket hendelse. I en helhetlig og balansert tilnærming til sikkerhet er redundans og gjenopprettingsevne for EBA en integrert del. Det kan også inkludere alternative lokasjoner for å huse viktige funksjoner som er en del av den digitale grunnmuren.

5.3.2 Ha forsvarlig sikring av sivile eiendommer, bygg og anlegg

I og med at sivile aktører leverer tjenester til den digitale grunnmuren, kan den digitale grunnmurens EBA også omfatte deler av den sivile leverandørens EBA. Med sivil EBA mener vi EBA som forsvarssektoren ikke selv eier eller drifter, men som inngår i verdikjedene for den digitale grunnmuren. Et eksempel kan være datasentre. Hvorvidt sivil EBA skal benyttes og inkluderes som en del av den digitale grunnmuren, er avhengig av en verdivurdering ut fra hvor kritisk sivil EBA er for grunnmurens funksjonalitet. Det må avgjøres og reguleres i forsvarssektorens avtaler med leverandørene.

5.3.3 Ha tilstrekkelig fortifikatorisk beskyttelse mot våpenvirkninger

Fortifikatoriske tiltak (Kiran, 2022) er en del av et helhetlig og balansert beskyttelseskonsept mot ulike typer våpenvirkninger for den digitale grunnmurens EBA. Kiran (2022) gir en oversikt over de ulike fysiske truslene et objekt kan bli utsatt for – og de viktigste våpenvirkningene er forklart. Videre presenterer Kiran (2022) hvordan fortifikatoriske tiltak kan bidra til å redusere effekten av våpenvirkningene og dermed øke beskyttelsen av objekter. Overvekten av militære våpen vil benytte kinetisk energi, trykk og fragmenter som primære våpenvirkninger, gjerne i kombinasjon.

Fordi elektronisk utstyr er sårbart mot elektromagnetisk påvirkning, er det nødvendig å vurdere den digitale grunnmurens behov for beskyttelse mot elektromagnetiske våpen. Elektronisk utstyr er spesielt sårbart mot elektromagnetisk puls (EMP) som følge av kjernefysiske detonasjoner. I tillegg kan radiofrekvente våpen, for eksempel High Power Microwave (HPM), forårsake stor skade på elektronisk utstyr. Beskyttelse mot EMP/HPM må derfor også inngå i forebyggende sikkerhetstiltak for digital grunnmur.

5.3.4 Ha vakt- og beredskapsordninger

Vaktordninger i kombinasjon med elektronisk sikring av EBA ved adgangskontroll, alarmer og kameraovervåkning er en sentral del av grunnsikringen. Ved en forhøyet trusselsituasjon kan beredskapen omkring utvalgt EBA eventuelt høynes ved bruk av sikringsstyrker. Hvorvidt forsvarssektorens planverk på dette området er hensiktsmessig og oppdatert for den digitale grunnmurens EBA, bør gjennomgås.

5.4 Prosesser og prosedyrer

Underkapittel 4.4 viste at det eksisterer en rekke mangler ved dagens digitale grunnmur, også knyttet til prosesser og prosedyrer. Oppsummert handler det om overlappende og uklare ansvarsforhold og at relevante ressurser ikke finner hverandre.

5.4.1 Ha samsvar mellom struktur og prosess

Utviklingen går fort innen IKT, og en grunnmur som er moderne i dag er ikke nødvendigvis moderne om få år. Både den kontinuerlige utviklingen innen IKT og eventuelle endringer i sourcingstrategi vil kunne kreve endringer i grunnmuren. Slike endringer må kunne gjøres raskt, slik at nye IKT-løsninger hurtig kan tas i bruk, og gamle IKT-løsninger kan fases ut. Samtidig trenger organisasjonen en viss stabilitet. Organisasjonen må gjennom sine prosesser og prosedyrer legge til rette for at en slik tilnærming skal fungere i praksis. Dette gjøres gjennom tydelige roller, ansvar og myndighet og fleksibilitet i gjennomføringen av rammene i organisasjonens ulike arbeidsprosesser.

Forsvarssektoren har per høsten 2023 en organisering hvor drift og vedlikehold ligger hos én etat (Forsvaret, ved Cyberforsvaret) mens utviklingsansvaret ligger hos en annen etat (FMA). FD har varslet å «[…] rydde opp i roller og ansvarsfordelingen mellom etatene […]» og at dette «innebærer gjennomgående endringer både i Forsvarsdepartementet og i etatene når det gjelder hvordan forsvarssektoren forvalter, utvikler, investerer og styrer innenfor IKT-området» (Forsvarsdepartementet, 2023a). Dersom Forsvaret skal ta i bruk DevSecOps må organisasjonen innrettes på en måte som tillater en slik type praksis. En mulig løsning er at organisasjonsstrukturen legger til rette for at ansvaret for både utvikling og drift er i samme enhet. Samtidig er det ikke tilstrekkelig at organisasjonsstrukturen tilrettelegger for DevSecOps, dersom prosessene og prosedyrene ikke følger samme praksis. En informant uttalte at det «må bygge[s] inn evner [i den digitale grunnmuren] som gir fleksibilitet med tanke på organisering, deployering

også videre». Fleksibilitet er også relevant, ved at organisasjonen gjennom sin formelle struktur potensielt ikke evner å tilpasse seg komplekse og uforutsigbare krav (Elstad, Lund, et al., 2022).

Det er nødvendig med samsvar mellom organisasjonsstruktur og gjennomføringen av samhandlings- og beslutningsprosesser i praksis (DeSanctis & Poole, 1997). Strukturen må ha en slik form at den evner å tilpasse seg komplekse og uforutsigbare krav (Hatum & Pettigrew, 2006). For eksempel, hvis strukturen i en IKT-porteføljestyringsmodell legger til rette for at ansvar og beslutningsmyndighet for IKT ikke tas på høyere nivå enn nødvendig, gir dette bedre rom for fleksibilitet og bedre tilpasningsevne til komplekse og uforutsigbare krav (jf. Hatum & Pettigrew, 2006). Forsvarsstaben har startet implementeringen av en slik IKT-porteføljestyringsmodell[39].

5.4.2 Sikre interoperabilitet med samarbeidspartnere

Forsvaret samarbeider med sine allierte i gjennomføring av operasjoner. For å oppnå interoperabilitet med allierte bør Federated Mission Networking (FMN)-rammeverket benyttes, jamfør Forsvarets IKT-strategi (Forsvarsstaben, 2021). Overordnet er FMN et rammeverk som består av mennesker, prosesser og teknologiske løsninger for å understøtte kommunikasjon mellom deltakere fra flere land under internasjonale operasjoner (Nato, 2022). Forsvarets IKT-strategi sier: «Konseptet [FMN] skal legges til grunn for utveksling av informasjon med allierte samarbeidspartnere. Dette innebærer at relevant IKT må være kompatibel med gjeldende standarder […] i FMN». I tillegg til kompatibel IKT må prosesser og prosedyrer være kompatible.

TYR, som er den primære plattformen Forsvaret i dag bruker både i nasjonale og internasjonale operasjoner, er FMN-kompatibel, og dermed i henhold til IKT-strategien (Forsvarsstaben, 2021). Imidlertid bør også den digitale grunnmuren være FMN-kompatibel så langt det er hensiktsmessig. Dette er dels fordi TYR-plattformer skal kunne knyttes til den digitale grunnmuren, og da er det mest kosteffektivt å benytte de samme grensesnittene som ved sammenkobling med allierte plattformer. I tillegg må det, ved alliert mottak, være mulig å koble de alliertes plattformer til den digitale grunnmuren, og disse plattformene vil være FMN-kompatible.

For å sikre at det til enhver tid er nødvendig FMN-kompatibilitet i den digitale grunnmuren må Forsvaret som et minimum følge utviklingen i FMN tett. Ved å bidra aktivt inn i FMN-utviklingsarbeidet, vil Forsvaret i tillegg ha mulighet til å påvirke FMN i en retning som er hensiktsmessig med tanke på Forsvarets digitale grunnmur. Det bør derfor også i framtiden settes av ressurser i Forsvarets IKT-virksomhet til å delta i relevante FMN-fora og bringe informasjon derfra tilbake til IKT-virksomheten.

5.4.3 Etterleve lover og regler

Forsvarssektoren er forpliktet til å etterleve en rekke lover og regler i all sin virksomhet i fred, krise og krig. Etterlevelse av lover og regler er en rammefaktor, som beskrevet i underkapittel

[39] For flere detaljer henviser vi til samarbeidsrommet «IKT-styring i forsvarssektoren» på FISBasis BEGRENSET.

3.9.1. Der nevnte vi eksempler på sentrale lover og regler, henholdsvis sikkerhetsloven, krigens folkerett, personvernlovgivningen og arbeidsmiljøloven. Framstillingen av disse lovene og reglene er ikke komplett, men viser til noen sentrale forhold som gjelder for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur.

Sikkerhetslovens (2018) formål er å beskytte nasjonale sikkerhetsinteresser og opprettholde grunnleggende nasjonale funksjoner (GNF). I henhold til loven påligger det forsvarssektoren å opprettholde et forsvarlig sikkerhetsnivå for IKT-virksomheten, herunder digital grunnmur (se anbefalinger for et forsvarlig sikkerhetsnivå for Forsvarets IKT i Flathagen et al. (2023) og Endregard et al. (2023)). Riksrevisjonen (2022) påpekte blant annet at det er sterkt kritikkverdig at kartleggingen av skjermingsverdige informasjonssystemer ikke er sluttført, og at forsvarlig sikkerhetsnivå ikke er fastsatt for alle informasjonssystemene. Forsvaret har et helhetlig ansvar for å sørge for et forsvarlig sikkerhetsnivå for IKT-virksomheten, uavhengig av sourcing (Elstad, Endregard, et al., 2022).

Som nevnt i kapittel 3.9.1 ble bestemmelsene om eierskapskontroll strammet inn gjennom endringer i sikkerhetsloven (Endringslov til sikkerhetsloven, 2023). I tillegg til de krav og føringer som legges av sikkerhetsloven for sikkerhetsgraderte anskaffelser og eierskapskontroll, kan internasjonale sanksjoner hindre anskaffelser av spesifikt materiell og tjenester for IKT som kunne inngått i forsvarssektorens digitale grunnmur. Det kan eksempelvis gjelde produsenter og leverandører fra land Norge eller allierte nasjoner ikke har et sikkerhetsmessig samarbeid med.

Forsvarets IKT-strategi (Forsvarsstaben 2021) forutsetter at den digitale grunnmuren skal virke i hele krisespekteret. Krigens folkerett regulerer væpnet konflikt og forutsetter et skille mellom militær og sivil virksomhet. Vurderinger av folkerettslige forhold er nødvendig når militær og sivil virksomhet knyttes sammen. I den grad deler av den digitale grunnmuren leveres av sivile aktører, for eksempel ekom-tilbydere eller leverandører innen skytjenester, forutsetter politiske myndigheter at dette skjer i henhold til krigens folkerett (Forsvarsdepartementet, 2020a). Elstad, Endregard, et al. (2022) gir en kort introduksjon til sentrale folkerettslige bestemmelser og anbefalinger knyttet til sourcing innen IKT-virksomheten, kort gjengitt i det følgende.

Konkrete folkerettslige vurderinger må gjøres fra sak til sak. Dette innebærer å konkretisere hvilke arbeidsoppgaver innen IKT-virksomheten som utgjør en direkte deltakelse i fiendtligheter. Slike arbeidsoppgaver skal utføres av militært personell som da er lovlig stridende personell. Videre må en spesifisere hvilke oppgaver sivile leverandører kan utføre, inkludert om dette innebærer indirekte støtte til fiendtlighetene eller er mer generell støtte. Av dette vil det følge om sivile leverandører skal gis en status som sivile som følger de væpnede styrker, og dermed får eget ID-kort og potensiell krigsfangestatus. Dersom utførelse av en funksjon innebærer fare for følgeskade for sivilt personell, er det krav om opplyst samtykke fra det sivile personellet.

En mulig utfordring er knyttet til funksjoner som forutsettes utført av sivilt personell i en krigssituasjon, for eksempel innen beredskap og evne til gjenoppretting. Ved avtaleinngåelse med sivile leverandører bør leveranseevne i hele krisespekteret inngå i vurderingene. Som forklart i Elstad, Endregard, et al. (2022, s. 38–39) har Forsvaret begrensede muligheter til å inngå avtaler om tjenesteplikt med sivile kontraktører. En annen utfordring kan være sammenblandingen

mellom militær og sivil infrastruktur og objekter. Krigens folkerett innebærer et forbud mot å angripe sivile mål, siden det kun er militære mål som er lovlige. Forsvaret må derfor innrette seg på en slik måte at risikoen for sivil følgeskade på kritiske samfunnsfunksjoner og sivilbefolkningen er akseptabel.

For anskaffelse, drift, vedlikehold og bruk av den digitale grunnmuren må regler om personvern overholdes. Personvern er nært knyttet til enkeltindividers muligheter for privatliv, selvbestemmelse og selvutfoldelse. «Retten til privatliv følger blant annet av den europeiske menneskerettskonvensjon (EMK) artikkel 8 og står sentralt i EUs personvernforordning (2016/679)» (Regjeringen, 2019). Disse internasjonale regelsettene er grunnlaget for nasjonal personvernlovgivning, det vil si lov om behandling av personopplysninger (2018) og forskrift om behandling av personopplysninger (2018).

Arbeidsmiljøloven gir som nevnt i underkapittel 3.9.1 rammer for rettigheter og plikter for arbeidsgivere og arbeidstakere. Arbeidsmiljøloven sikrer alle ansatte retten til å bli hørt gjennom tillitsvalgte og verneombud. Framforhandlede avtaler mellom partene i arbeidslivet, det vil si tariffavtaler, har bestemmelser om arbeidstakers rett til medvirkning og medbestemmelse. For forsvarssektoren gjelder Hovedavtalen i staten (Regjeringen, 2022). Den regulerer når og hvordan medbestemmelse skal praktiseres. For IKT-virksomheten og den digitale grunnmuren er dette blant annet aktuelt ved omstillingsprosesser og sourcing, og eventuelle endringer i arbeidsdelingen mellom militært personell, sivilt personell i forsvarssektoren og oppgaver utført av sivile kontraktører eller strategiske partnere.

5.4.4 Etablere og opprettholde et forsvarlig sikkerhetsnivå

Den digitale grunnmuren er fundamentet for at Forsvaret skal kunne planlegge og gjennomføre operasjoner, både i fredstid og ved sikkerhetspolitisk krise og væpnet konflikt. Sikkerhet for at den digitale grunnmuren er tilgjengelig, beskyttet mot uautorisert tilgang og til å stole på, er derfor av avgjørende betydning for Forsvarets operative evner.

Det er behov for økt oppmerksomhet omkring sikkerhet, herunder IKT-sikkerhet, personellsikkerhet, fysisk sikkerhet og *safety*. Ifølge en informant «[…] trenger [forsvarssektoren] en rigg for å tenke sikkerhet hele veien – det har manglet […]».

Etablere verdisentrisk risiko- og sikkerhetsstyring

Sikkerhetslovens (2018) perspektiv er primært beskyttelse mot sikkerhetstruende virksomhet. Formålet er å beskytte nasjonale sikkerhetsinteresser mot tilsiktede handlinger som direkte eller indirekte kan skade nasjonal sikkerhet. Alle virksomheter som omfattes av loven, skal sørge for å oppnå et forsvarlig sikkerhetsnivå for sine skjermingsverdige verdier, det vil si skjermingsverdig informasjon (både fysisk og digital) samt skjermingsverdige informasjonssystemer, objekter og infrastruktur.

Sikkerhetsloven krever at risikobaserte vurderinger legges til grunn for å avgjøre hva som er et forsvarlig sikkerhetsnivå for en virksomhets funksjoner. Loven setter også et krav til at risiko-

vurderinger skal være verdibaserte, slik at sikkerhet, og ikke minst kostnaden ved sikkerhet, til enhver tid skal være tilpasset den verdien et informasjonssystem har for brukerne eller eierne av systemet. I forarbeidene til sikkerhetsloven påpeker 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» (Forsvarsdepartementet, 2017b).

Helhetlig risiko- og sikkerhetsstyring for den digitale grunnmuren handler om forebygging, beredskap, håndtering og gjenoppretting av alle typer uønskede hendelser og å oppnå et akseptabelt sikkerhetsnivå (Endregard et al., 2023). En verdisentrisk tilnærming innebærer å ta utgangspunkt i Forsvarets kjerneverdier og -oppgaver, det vil si Forsvarets operative evner, for å utlede hva et forsvarlig sikkerhetsnivå for den digitale grunnmuren innebærer. Fra et teknologisk perspektiv kan den digitale grunnmuren karakteriseres som en infrastruktur for hele forsvarssektoren, da Forsvarets digitale grunnmur er felles for brukerne og helt nødvendig for at Forsvaret skal fungere.

For Forsvarets digitale grunnmur er det nødvendig at den er beskyttet mot et vidt spekter av trusler og farer, både tilsiktede og utilsiktede uønskede hendelser, med både fysiske, digitale og cyberfysiske[40] konsekvenser. Målet med helhetlig risiko- og sikkerhetsstyring er å oppnå tilstrekkelig sikkerhet og sikre den digitale grunnmurens funksjonalitet, tilgjengelighet, integritet og konfidensialitet, samtidig som andre verdier ivaretas, for eksempel personvern. Sikkerhetstiltak må derfor balanseres og avveies både mot hverandre og ut fra kost/nytte-hensyn.

Verdisentrisk risiko- og sikkerhetsstyring må inkluderes i den helhetlige virksomhetsstyringen. Videre er det ikke tilstrekkelig at dette kun utføres av de etater som utvikler og drifter den digitale grunnmuren. Brukerne, i første rekke de operative miljøene på ulike nivåer, må delta aktivt og ta eierskap til verdi- og risikovurderingene. I tillegg må annen nødvendig kompetanse inn i vurderingene (se underkapittel 5.5.2 og Endregard et al., 2023). Ansvar, roller og myndighet knyttet til risiko- og sikkerhetsstyringsprosessen bør avklares i IKT-styringsmodellen. I tillegg kreves kompetanse- og metodeutvikling på tvers av sektoren.

Risiko- og sikkerhetsstyringen må være dynamisk og evne å ta hensyn til endringer. Dette er særlig relevant på IKT-området der endringer kan skje raskt. At et informasjonssystem er sikkerhetsgodkjent før det ble tatt i bruk, er ikke tilstrekkelig dersom det senere skjer endringer i programvaren eller leverandørkjeden. Da må nye risiko- og sikkerhetsvurderinger utføres. Tidligere var sikkerhetsstyring mer basert på sjekklister. Et moderne sikkerhetsregime for en moderne og motstandsdyktig digital grunnmur krever kontinuerlig risiko- og sikkerhetsstyring.

Sørge for robusthet og redundans

For å kunne sørge for at grunnmuren får tilstrekkelig robusthet og redundans, er det nødvendig å kartlegge både Forsvarets behov til den digitale grunnmuren og hvilke trusler grunnmuren kan

[40] «Med et cyberfysisk system mener vi smarte systemer som inkluderer konstruerte samhandlende fysiske og digitale komponenter» (Endregard et al., 2023, s. 21)

stå overfor. Deretter stilles det krav basert på denne kartleggingen. Det vil typisk være ulike krav til robusthet og redundans i ulike deler av konfliktspekteret. Informanter påpekte at nytteverdi må balanseres med motstandsdyktighet, og at den digitale grunnmuren må være robust og sikker nok samt ha tilstrekkelig redundans i tråd med PACE-prinsippet[41].

Det bør finnes en oversikt over hvilke deler av grunnmuren som fortsatt skal virke hvis andre deler faller bort. Det bør også finnes en oversikt over hvordan ulike deler av grunnmuren vil fungere under press i hele konfliktspekteret. Sivile IKT-systemer og infrastrukturer kan utnyttes ved behov. I tillegg bør det vurderes om IKT-tjenester som normalt tilbys av grunnmuren, skal kunne flyttes ut av landet ved behov.

Muliggjøre sikkerhetsmessig overvåking, hendelseshåndtering og defensive cyber-operasjoner

Riksrevisjonen (2022) påpekte mangler i evnen til å oppdage og stanse digitale angrep. Våre informanter påpekte betydningen av sikkerhetsstyring og -kontroll samt evner til å gjennomføre deteksjon og håndtering av hendelser i cyberdomenet. Dette er nødvendig for å beskytte de militære operasjonene som er avhengige av den digitale grunnmuren. Ettersom den digitale grunnmuren utgjør felles IKT, er det essensielt at Forsvaret har evne til å oppdage, varsle om og håndtere ulike typer uautorisert tilgang. Flere informanter påpekte at evnen til defensive cyber-operasjoner er en del av den digitale grunnmuren, og at det er behov for robuste kompetansemiljøer som kan gi råd innenfor dette temaet.

Defensive cyberoperasjoner er ifølge Cyberforsvaret aktiviteter for å beskytte og forsvare egne operasjoner mot cybertrusler og bevare Forsvarets handlefrihet i cyberdomenet. Det pågår en styrking av Cyberforsvarets verktøy for sikkerhetsmessig overvåkning og en videreutvikling av IKT-responsmiljøet Military Computer Emergency Response Team for forsvarssektoren (MilCERT) (varslet i Meld. St. 10 (2021–2022)). Forsvaret etablerte i 2022 et konsept for defensive cyberoperasjoner (Cyberforsvaret, 2022).

Tydeliggjøring av roller, ansvar og myndighet i forbindelse med hendelseshåndtering ble også nevnt som sentralt av våre informanter. Eksempelvis er det behov for tydeliggjøring av ansvar for hendelseshåndtering mellom aktører som jobber med den digitale grunnmuren og aktører som jobber med applikasjoner.

Ivareta sikkerhet i samarbeid med sivile totalforsvarsaktører og eksterne leverandører

Forsvaret er avhengig av å samarbeide med en rekke sivile totalforsvarsaktører, både offentlige og private, for å kunne håndtere kriser (se f.eks. Endregard, 2019). Den digitale grunnmuren må derfor tilrettelegge for informasjonsdeling mellom militære og sivile totalforsvarsaktører i hele krisespekteret (se også underkapittel 5.2.2). Dette kan innebære at utvalgte sivile totalforsvars-

[41] Prinsippet Primary, Alternate, Contingency, Emergency (PACE) er beskrevet i DRP. Det «[…] skal ligge til grunn for IKT-tjenester i hele konfliktspekteret. Prinsippet gjelder alle relevante deler av forsvarssektorens IKT, med vekt på den digitale grunnmuren samt applikasjoner og tjenester hvor dette er påkrevd. PACE er en metodikk som beskriver en rekkefølge av alternative kommunikasjonstjenester og/eller tjenesteleveranser.».

aktører får benytte Forsvarets digitale grunnmur, eventuelt at data kan overføres fra sivile IKT-systemer til og fra grunnmuren, og at dette kan skje mellom ulike graderingsnivåer. Et forsvarlig sikkerhetsnivå må ivaretas i denne samhandlingen.

Leverandørkjedeperspektivet er vesentlig for et forsvarlig sikkerhetsnivå. Et relevant spørsmål stilt av en informant er: «Hvem samarbeider man med, og hvor mye tillit har man til dem?». Dette henger tett sammen med digitale verdikjeder, beskrevet i underkapittel 5.1.1.

Når Forsvaret vurderer å inngå samarbeid med sivile aktører om leveranser av IKT-tjenester, kreves en rekke vurderinger, herunder verdi- og risikovurderinger. Et forsvarlig sikkerhetsnivå må ivaretas i interaksjonen med aktører utenfor forsvarssektoren. Som presisert av Elstad, Endregard, et al. (2022): «I henhold til sikkerhetsloven har Forsvaret et helhetlig ansvar for å sørge for et forsvarlig sikkerhetsnivå for Forsvarets IKT-virksomhet, uavhengig av sourcing».

Forsvaret er avhengig av sivil ekom-infrastruktur. Telenor ble trukket fram i vår datainnsamling som et eksempel på en sentral leverandør av IKT-tjenester til Forsvaret. Det ble påpekt at Telenor som aktør ikke er en del av grunnmuren, men at IKT-tjenestene de leverer, er det. Dette stemmer overens med hvordan vi har forklart digital grunnmur tidligere i rapporten. Telenor og andre ekom-tilbydere er avgjørende samarbeidspartnere for Forsvaret i en totalforsvarsramme i sikkerhetspolitisk krise og væpnet konflikt. Deres deltakelse er inkludert i sivilt-militært plan-verk, og for eksempel deltok både Telenor og Broadnet i kommandoplassøvelsen under øvelsen Trident Juncture i 2018 (Endregard, 2020).

I global sammenheng er Forsvaret en liten kunde, og en utfordring kan være at leverandører ikke nødvendigvis prioriterer å skreddersy løsninger for å dekke Forsvarets spesifikke behov. En mulig løsning som ble foreslått av informantene er å samarbeide og samle flere nasjoner for å bli en stor nok kunde til at leverandører vil gjøre tilpasninger eller skreddersøm.[42]

5.4.5 Ha effektive endringsprosesser

Endringsprosesser var et tema under gruppesamtalene med informantene – og spesielt om Forsvarets evne til faktisk å prioritere og levere endringer som er nødvendige for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur. Dette henger også tett sammen med andre faktorer i vårt rammeverk – som «mennesker» og «kultur».

Flertallet av informantene oppfattet at det var sentralt at IKT-virksomheten måtte evne å prioritere og levere endringer. Nytenkning og risikovilje ble oppfattet av enkelte informanter som nødvendige betingelser for å lykkes med den digitale grunnmuren. Inkludert i dette var både evne og vilje til å gjennomføre endringer for både prosess, organisasjon og mennesker. Det ble for eksempel uttalt at Forsvaret «trenger en organisasjon som kan lykkes, menneskelige ressurser og kompetanse, mandat og finansiering samt risikovilje».

[42] Vi har ikke gjort noen analyser for å evaluere denne løsningen, løsningen er kun presentert som et alternativ fra våre informanter.

Flere av informantene var opptatt av ledernes rolle i forbindelse med endringsprosesser. For eksempel uttalte en informant at for å lykkes med grunnmuren, «må [vi] ha like engasjerte ledere som medarbeidere. Lederne må drive dette [endringen]». En annen uttalte at «Riktig *commitment* på riktig nivå i organisasjonen er viktig». Disse uttalelsene støttes av litteraturen (se f.eks. Barth & Koch, 2019; Laureani & Antony, 2018), hvor toppledelsens støtte og involvering er en av KSF-ene som oftest er nevnt. Toppledelsesstøtte og involvering antas derfor å være sentralt for at den digitale grunnmuren.

5.5 Mennesker

Dette kapittelet tar for seg menneskefaktoren, som er sentral i gjennomføringen av prosesser og prosedyrer. Menneskefaktoren i vårt helhetlige rammeverk omfatter individene i organisasjonen. Kompetanse er en sentral del av menneskefaktoren, og beskrivelsen av nåsituasjonen pekte på manglende kompetanse som påvirker den digitale grunnmuren.

5.5.1 Ha oversikt over kompetansebehov

Underveis i datainnsamlingen ble det avdekket ulike kompetansebehov som informantene mente Forsvaret er avhengige av for å kunne oppnå og opprettholde grunnmuren. Listen over framtidsviktig kompetanse, handler om mer enn bare en persons digitale kompetanse – den inkluderer også for eksempel evne til å tilegne seg ny kompetanse og omstille seg, evne til å kommunisere og samarbeide med andre mennesker, kreativitet samt omsorg og empati (Fauske, 2023; Fauske & Strand, 2022). Det er derfor behov for flere typer kompetanse som vi kommer nærmere inn på i dette kapittelet, nemlig endringskompetanse, helhetskompetanse, teknologisk spesialistkompetanse samt risiko- og sikkerhetskompetanse.

Ha endringskompetanse

Fauske (2023, s. 13) identifiserer «evne til å tilegne seg ny kompetanse og å omstille seg» som en framtidsviktig kompetanse. Forskeren argumenterer med at noen bruker begrepet halveringstid for kompetanse – sett i lys av at arbeidsoppgaver vil forsvinne, endre seg eller komme til raskere enn tidligere. En arbeidsprosess som potensielt vil endres ved innføring av en moderne grunnmur er gjennomføring av driftsoppgaver. I dag er en av driftsoppgavene at personell konfigurerer nettverksbokser. Automatisering og virtualisering vil gjøre at deler av disse oppgavene automatiseres, mens nye oppgaver knyttet til orkestrering av programvarebaserte nettverksfunksjoner vil måtte utføres. Det vil si at personellet som skal gjennomføre slike aktiviteter sannsynligvis vil ha behov for en annen type kompetanse enn aktiviteten krever i dag.

Flere av informantene var opptatt av ledernes endringskompetanse, blant annet effektiv kommunikasjon og rasjonale bak beslutninger som gjøres, noe som stemmer overens med teorien (se f.eks. Elstad, 2014). Inkludert i endringskompetanse er holdninger, engasjement for endringen, samt vilje, støtte og forpliktelse til å gjennomføre denne. Videre var informantene også opptatt av behovet for kompetanse innen det å prioritere mellom tiltak og kompetanse til å levere nødvendige endringer for den digitale grunnmuren. Oppsummert mener vi at det å inneha

endringskompetanse vil være en nødvendig betingelse for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur.

Ha helhetskompetanse

Flere av informantene var opptatt av behovet for helhetskompetanse innen IKT. Helhetskompetanse kan ses på som en kombinasjon av virksomhetskompetanse og teknologikompetanse. Elstad, Endregard, et al. (2022) beskriver ulike kompetansetyper forsvarssektoren har behov for i utøvelsen av strategisk IKT-styring. Virksomhetskompetanse handler om forståelse for virksomheten til forsvarssektoren, inkludert eksisterende mål, prosesser, verdier og operative behov. Teknologikompetanse handler om forståelsen av teknologiske muligheter og begrensninger ved den digitale grunnmuren og hvilke teknologier som best møter operative behov. Som en av informantene uttalte, er det et behov for teknologiforståelse, også hos sjefer: «Vi har fortsatt en generasjon med sjefer som ikke helt skjønner hva det er snakk om.»

Flere av informantene nevnte at Forsvaret er gode til å løse problemer fra dag til dag, men ikke til å tenke helhetlig og langsiktig. Flere knyttet helhetskompetanse til faktoren «organisasjon og mål», og spesifikt til utarbeidelse av mål. En informant uttalte at «Vi må sammen eie IKT-landskapet og de fremtidige målene». En annen informant sa at «valg av enkeltdeler kan potensielt få konsekvenser for resten av systemet». Dette er i tråd med sosioteknisk systemteori, hvor endring i én del av systemet får konsekvenser innenfor andre deler av systemet (se f.eks. Davis et al., 2014; Leavitt, 1965; Lyytinen & Newman, 2008).

Oppsummert mener vi derfor at det er et behov for en overordnet teknologisk kompetanse, samtidig som det er behov for virksomhetskompetanse. Det er nødvendig å ha en forståelse for kompleksiteten og sammenhengen mellom de ulike delene i systemet. Det er nødvendig å se disse delsystemene i en overordnet sammenheng, og ikke kun se på detaljer innenfor hvert enkelt delsystem.

Ha teknologisk spesialistkompetanse

Kompetanse innen utvikling, installasjon, drift og vedlikehold omfatter ulike former for teknologisk spesialistkompetanse. De som innehar slik kompetanse, er gjerne eksperter med ulike former for IKT-utdannelse og erfaring innen IKT (Elstad, Lund, et al., 2022). Mennesker med slik kompetanse er nødvendige for at Forsvaret skal kunne opprettholde daglig drift, vedlikehold og utvikling av den digitale grunnmuren.

I moderne systemutvikling (DevSecOps) utføres utvikling og drift av den samme gruppen av personell. Arbeidsprosessene og dermed også kravet til spesialistkompetanse innenfor moderne systemutvikling krever derfor en annen type kompetanse enn den tradisjonelle drifts- og vedlikeholdskompetansen. Eksempelvis vil kompetansebehovet endre seg ved en overgang fra tradisjonell nettverksdrift til drift av virtuelle nettverk. I stedet for kompetanse på konfigurering og drift av fysiske nettverksbokser er det blant annet nødvendig med kompetanse på orkestrering av programvarebaserte nettverksfunksjoner.

Ha risiko- og sikkerhetskompetanse

Flere av informantene påpekte behovet for sikkerhetskompetanse, inkludert kompetanse for å kunne gjennomføre risiko- og sikkerhetsvurderinger. En informant uttalte at en «Kan ikke outsource sikkerhetsvurderinger». Videre var informantene opptatt av at det muligens kunne undervurderes hvor mye kompetanse som kreves for å gjøre gode risiko- og sikkerhetsvurderinger – og at organisasjonen er avhengig av riktige folk til å gjennomføre disse vurderingene.

Endregard et al. (2023) anbefaler at «En god risikovurderingsprosess bør utføres av en tverrfaglig sammensatt analysegruppe. Det krever at flere kompetanseområder bringes inn og aktivt deltar.» De viser til at det er nødvendig med domenekompetanse; det vil i vårt tilfelle være kompetanse på militære operasjoner, den digitale grunnmurens oppbygning, funksjonalitet, IKT-sikkerhetsmekanismer og sårbarheter. Videre er det behov for trusselfaglig kompetanse på motstanderes intensjoner, midler og mulige angrepsmåter. Til slutt er det nødvendig med risiko- og sikkerhetsfaglig kompetanse, det vil si (1) metodekompetanse, (2) IKT-sikkerhetsfaglig kompetanse for å kunne vurdere IKT-sikkerhetskrav og -tiltak og (3) prosesskompetanse for å kunne tilrettelegge og gjennomføre en egnet risikovurderingsprosess.

5.5.2 Ha tilgang til tilstrekkelig kompetanse

Tilgang til tilstrekkelig personell med relevant kompetanse vil bidra både direkte og indirekte til å sikre IKT-virksomhetens leveranseevne i hele krisespekteret, og dermed Forsvarets operative evne (Birkemo et al., 2021; Elstad, Endregard, et al., 2022; Svendsen-utvalget, 2020). Ifølge Fauske (2023, s. 89):

> [kan kompetanse] også fungere som muliggjører som setter Forsvaret i stand til å transformere virksomheten. Slik har det alltid vært, men det som er nytt, er at endringstakten knyttet til teknologi og kompetansebehov er raskere enn før og at teknologisk kompetanse vil være mangelvare i samfunnet.
>
> Dette skiftet i arbeidsmarkedet gjør at mye forskning på fremtidens arbeidsliv påpeker viktigheten av å se fremover, forsøke å være i forkant, sette seg mål for fremtidig kompetansebeholdning og lage en plan for å nå målene som tar innover seg de raske endringene.

En informant uttalte at kompetanse var den viktigste KSF-en for å klare noe som helst. En annen informant uttalte at Forsvaret må ha en plan for hvordan man til enhver tid skal ha tilgang til kompetent personell som man stoler på. Disse uttalelsene stemmer overens med Fauske (2023), som sier at Forsvaret må være i forkant av den endringen som skal skje, og sette seg mål for den framtidige kompetansebeholdningen. Oppsummert må derfor Forsvaret lage en plan for å nå de målene som er satt for en framtidig kompetansebeholdning.

En informant var opptatt av at Forsvaret konkurrerer med resten av samfunnet og industri om kompetanse – og at Forsvaret derfor var nødt til å samarbeide og finne et grensesnitt mot industri. Utviklingen innen IKT-området går raskt, og «de digitale verdikjedene blir mer og mer

komplekse» (Elstad, Endregard, et al., 2022, s. 26), så det er et åpent spørsmål hvordan forsvarssektoren skal få tilgang til nødvendig personell:

> [Det kan] spørres om det er realistisk for forsvarssektoren å ha nok kompetanse internt til å ivareta alle kompetanseområder innen IKT. Forsvarssektoren er i dag avhengig av ekstern kompetanse, grunnet større grad av komplekse digitale verdikjeder, hvor det i fremtiden vil bli vanskeligere å skille de ulike bestanddelene i den digitale verdikjeden fra hverandre (se f.eks. Lysne, 2020). (Elstad, Endregard, et al., 2022, s. 26)

Et mulig tiltak for å skaffe nødvendig kompetanse kan være å satse på å hente tilbake personell som har sluttet. Studier av sluttårsaker i Forsvaret viser nemlig at omtrent halvparten av de som slutter i Forsvaret kunne tenke seg å komme tilbake (Fauske og Strand, 2019; Fauske og Strand, 2020), så potensialet er stort (Fauske, 2023, s. 95).

5.6 Kultur

I dette kapittelet beskriver vi den siste faktoren i rammeverket, nemlig «kultur», og forslag til momenter som bør inngå i kulturfaktoren for Forsvarets moderne og motstandsdyktige digitale grunnmur.

5.6.1 Ha endringsdyktighet og evne til å ta beslutninger

Under gruppesamtalene snakket informantene om kultur. En av informantene var opptatt av at Forsvaret skulle oppgi perfeksjonisme og heller etablere en gradvis utvikling, tildele midler og finne ut av ting underveis. En annen informant snakket om beslutningsdyktighet og evnen til å ta beslutninger – selv om ikke beslutningen var omforent eller at det var etablert en total oversikt over situasjonen. Informantene var også opptatt av tillit til å gjennomføre beslutninger og at det burde vært mindre bekymringskultur i Forsvaret. Informantene snakket også om at i dag var det en del omkamper på beslutninger som var tatt, noe de ønsket å unngå i framtida.

Sammenstiller vi disse uttalelsene representerer de en kultur gjennom et sett felles mønstre av meninger og holdninger som gir utslag i bestemte måter å handle på. Denne kulturen indikerer til en viss grad motstand mot endring, noe som stemmer overens med det Diesen (2022) kaller institusjonell konservatisme (se underkapittel 3.8).

Forsvaret ønsker en kultur som fremmer endringsvilje og innovasjon, og det er en slik type kultur som bør inngå i en framtidig grunnmur. I Forsvarets IKT-strategi (Forsvarsstaben, 2021) står følgende:

> For at Forsvaret bedre skal kunne utnytte IKT, fordrer det en kultur som fremmer teknologi og innovasjon. Forsvaret må tilnærme seg IKT helhetlig og målrettet som en strategisk ressurs som kan øke operativ evne, og ha et bevisst forhold til å utvikle IKT-virksomheten i ønsket retning.

Det er flere momenter knyttet til kulturfaktoren i sitatet. Forsvaret ønsker en kultur som fremmer teknologi og innovasjon – noe som kan ses i sammenheng med den digitale grunnmuren. For å oppnå en slik kultur vil det være behov for en kulturendring (jf. Forsvarsstaben, 2021). Forsvarets IKT-strategi sier videre at kulturen følger prinsipper som endringsdyktighet, fleksibilitet, robusthet, autonomi, og evne og vilje til å ta ansvar og raske beslutninger – i alle deler av organisasjonen. Det er derfor et gap mellom dagens kultur og den kulturen Forsvaret ønsker. Et slikt gap oppstår dersom en av faktorene i rammeverket blir inkompatibel med én eller flere av de andre faktorene. Dersom slike gap eksisterer, vil systemets ytelse og levedyktighet reduseres (Lyytinen & Newman, 2008). Det vil si at det må lages en plan for hvordan Forsvaret skal endre sin kultur i ønsket retning.

5.6.2 Forstå lederens rolle i bygging av kultur

For å bygge en kultur som støtter opp om endringen som må til for å oppnå en moderne og motstandsdyktig digital grunnmur, står lederens rolle sentralt. De lederne som har ansatte som er berørte av endringen, må vektlegge arbeid for å etablere et sett med felles antakelser rundt nytteverdien av denne grunnmuren for Forsvaret. Det må etableres en felles forståelse blant lederne for nytteverdien av endringen og det mulighetsrommet endringen gir, gjennom kontinuerlig forankring. Dette henger tett sammen med menneskelige faktorer knyttet til kompetanse. For at lederne skal kunne oppnå denne felles forståelsen fordrer det en viss digital kompetanse generelt, men også kompetanse på helheten (som nevnt i underkapittel 5.5.1). I tillegg er strategisk IKT-kompetanse sentralt for at lederne skal forstå nytten av den teknologiske endringen.

Forsvarets IKT-strategi (Forsvarsstaben, 2021) sier følgende:

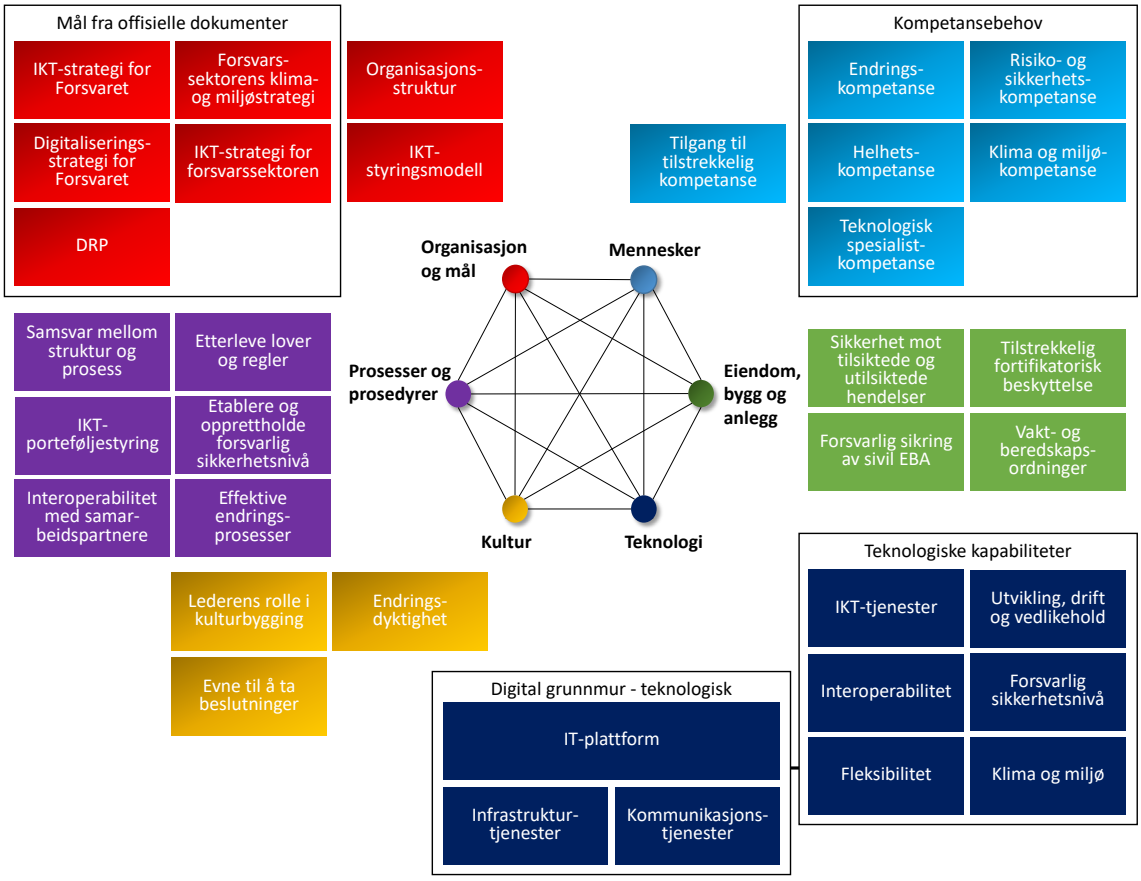
> Ledere på alle nivå i Forsvaret har ansvar for at IKT prioriteres slik at mulighetene for digitalisering og effektivisering kan utnyttes. I Forsvaret i dag følges ledere i liten grad opp på anvendelsen av IKT. Forsvaret må jobbe med å skape insentiver for å prioritere og verdsette IKT og kompetanse knyttet til dette. Det er også viktig at dette ikke er begrenset til kun personell direkte tilknyttet fagområdet; teknologi må ha en sentral plass som en del av organisasjonsutviklingen. Lederens rolle i dette må være å forstå viktigheten av og mulighetsrommet teknologi gir, og basert på dette prioritere, sette rammer og gi ressurser på en måte som styrker området. Både ledere og ansatte på alle nivå må også forholde seg til løpende endringer som følge av teknologiutviklingen og det å bygge en endringsdyktig organisasjon er også en viktig del av lederansvaret.

Ledere kan påvirke de ansattes felles oppfattelse gjennom opplæring og kommunikasjon (se f.eks. Elstad, 2014). Med felles oppfattelse menes at de ansatte har en delt forståelse (felles kultur) av fordelen ved endringene en ny digital grunnmur fører til (Amoako-Gyampah & Salam, 2004). En felles oppfattelse av fordelene ved endringen vil videre påvirke individuell opplevd nytte og brukervennlighet (Amoako-Gyampah & Salam, 2004). Sitatet fra IKT-strategien (Forsvarsstaben, 2021) støtter opp om lederens rolle i bygging av kultur – og skal organisasjonen unngå gap mellom faktorene i vårt helhetlige rammeverk, vil en prioritering av kulturbygging stå sentralt. Som Forsvarets IKT-strategi sier, er lederens kompetanse på mulig-

hetene ved og viktigheten av teknologi sentralt, og Forsvaret må prioritere en styrking av dette området.

5.7 Oppsummering av Forsvarets moderne og motstandsdyktige digitale grunnmur

I dette kapittelet har vi gått gjennom de ulike faktorene som inngår i vårt helhetlige rammeverk for Forsvarets moderne og motstandsdyktige digitale grunnmur i framtiden. Figur 5.4 oppsummerer hovedpunktene fra dette kapittelet.



Figur 5.4 Oppsummering av Forsvarets moderne og motstandsdyktige digitale grunnmur.

Faktoren «organisasjon og mål» gir oversikt over organisasjonsstruktur og en entydig IKT-styringsmodell. En framtidig digital grunnmur vil inneholde mål fra offisielle dokumenter som Forsvarets IKT-strategi, DRP og Digitaliseringsstrategi for Forsvaret. Det bør etableres mål for alle faktorene i vårt rammeverk, for å se en helhet og ikke enkeltfaktorer i isolasjon. På samme måte som for beskrivelsen av nåsituasjonen, har vi valgt å ta med forsvarssektorens klima og miljøstrategi samt IKT-strategi for forsvarssektoren, selv om Forsvaret ikke alene har beslutningsmyndighet for innholdet i dokumentene.

Teknologifaktoren i figur 5.4 viser at fra et teknologisk perspektiv består den digitale grunnmuren av maskin- og programvare som tilbyr et sett med IKT-tjenester (innenfor IT-plattform, infrastruktur og kommunikasjon). Den digitale grunnmuren må inneha følgende seks teknologiske kapabiliteter: (1) tilby et tilstrekkelig og relevant sett av IKT-tjenester, (2) fremme interoperabilitet, (3) fremme fleksibilitet, (4) støtte og ivareta effektiv utvikling, drift og vedlikehold, (5) ha et forsvarlig sikkerhetsnivå og (6) ivareta klima og miljø.

EBA-faktoren bør inneha nødvendige kapabiliteter knyttet til egnethet og sikkerhet for den digitale grunnmuren. Denne studien omtaler følgende kapabiliteter: (1) ha sikkerhet mot tilsiktede og utilsiktede hendelser, (2) ha forsvarlig sikring av sivil EBA, (3) ha tilstrekkelig fortifikatorisk beskyttelse mot våpenvirkninger og (4) ha vakt- og beredskapsordninger.

Faktoren «prosesser og prosedyrer» viser at det er nødvendig med samsvar mellom struktur og prosess, for eksempel i IKT-porteføljestyring. Interoperabilitet med samarbeidspartnere er også inkludert. Videre beskrives det overordnede behovet for å etterleve lover og regler. Etablering og overholdelse av et forsvarlig sikkerhetsnivå er et sentralt tema. For å oppnå og opprettholde en framtidig digital grunnmur må også effektive endringsprosesser gjennomføres.

Menneskefaktoren beskriver ulike kompetansebehov som bør være til stede for at Forsvaret skal kunne oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur. Følgende kompetansebehov blir overordnet beskrevet: (1) endringskompetanse, (2) helhetskompetanse, (3) teknologisk spesialistkompetanse og (4) risiko- og sårbarhetskompetanse. I tillegg må Forsvaret ha tilgang til tilstrekkelig personell med relevant kompetanse. Klima og miljø-kompetanse kommer vi nærmere tilbake til i kapittel 6.1.2, som en del av strategisk IKT-kompetanse.

Det er nødvendig med felles mønstre, holdninger og verdier. I kulturfaktoren beskrives endringsdyktighet og evne til å ta beslutninger, samt lederens rolle i å bygge kultur.

6 Kritiske suksessfaktorer for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur

Dette kapittelet beskriver seks overordnede kritiske suksessfaktorer (KSF-er) for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur. Disse KSF-ene (figur 6.1) er videre delt opp i ulike temaer, hvor vi kommer med anbefalinger til Forsvaret.[43]

Figur 6.1 Liste over overordnede KSF-er, og hvilke faktorer de er knyttet til, for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur – i ikke-prioritert rekkefølge.

6.1 Sikre tilgang til nødvendig kompetanse

Informantene påpekte mangler innen IKT-kompetansen i forsvarssektoren, noe som også er påpekt i offentlige dokumenter (se f.eks. Svendsen-utvalget, 2020; Forsvarsdepartementet, 2019a). Vi identifiserte derfor KSF-en «sikre tilgang til nødvendig kompetanse» for å oppnå og opprettholde en digital grunnmur. For å forstå kompetansebehovet og sikre at det blir ivaretatt, må Forsvaret sette kompetanse på dagsorden i sitt daglige virke. Kompetanse er gjennomgående nødvendig for at Forsvaret skal kunne løse sine oppgaver, og forståelse for og tilgang til nødvendig kompetanse inngår derfor som en sentral del av dette. Videre er det nødvendig at

[43] Datagrunnlaget for vår KSF-analyse er gruppesamtalene med forsvarssektoren, den andre workshopen, dokumentene (underkapittel 2.2.) og resultatene fra kapittel 5. Underkapittel 2.3 og tabell 2.2 viser stegene vi har gjennomført i vår dataanalyse for å komme fram til KSF-ene. Hvordan vi har ivaretatt studiens validitet og reliabilitet gjennom dataanalysen er beskrevet i underkapittel 2.4.

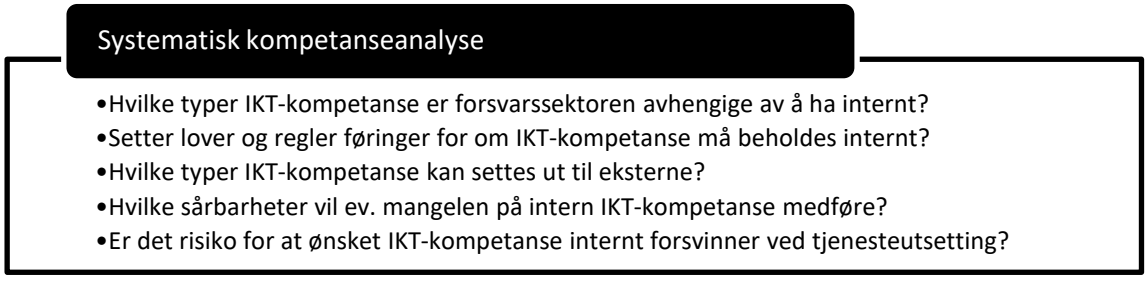
Forsvaret oppretter og opprettholder den strategiske IKT-kompetansen, som en del av det å prioritere kompetanse. Figur 6.2 viser temaene vi omtaler i dette underkapittelet:

Figur 6.2 En identifisert KSF for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur er «Sikre tilgang til nødvendig kompetanse».

6.1.1 Ha tilgang til nødvendig spesialistkompetanse

I underkapittel 5.2 beskrev vi teknologiske kapabiliteter som den digitale grunnmuren bør ha. Det er nødvendig med tilgang til personell med kompetanse innenfor nettopp disse teknologiske kapabilitetene. Forsvaret har behov for spesialistkompetanse innenfor eksempelvis skyteknologi og KI. Spesialistkompetanse på data som strategisk ressurs i organisasjonen er også nødvendig. Videre er det behov for spesialistkompetanse innen interoperabilitet generelt og FMN spesielt, for å forstå hva som skal til for å støtte føderert samhandling med allierte – og muligheter for standardiserte tilkoblinger til relevante deler av totalforsvaret.

Der Forsvaret har teknologiområder eller aktiviteter med manglende kompetanse, kan Forsvaret velge å kombinere interne ressurser med eksterne ressurser. Eksterne ressurser kan være strategiske partnere eller andre samarbeidspartnere som for eksempel konsulentfirmaer. Vi anbefaler at Forsvaret gjennomfører en systematisk kompetanseanalyse (jf. Elstad, Endregard, et al., 2022), for å avdekke hvilke typer IKT-kompetanse som er nødvendig for gjennomføring av Forsvarets kjernevirksomhet. Forslag til spørsmål som kan inkluderes i en slik analyse vises i figur 6.3:



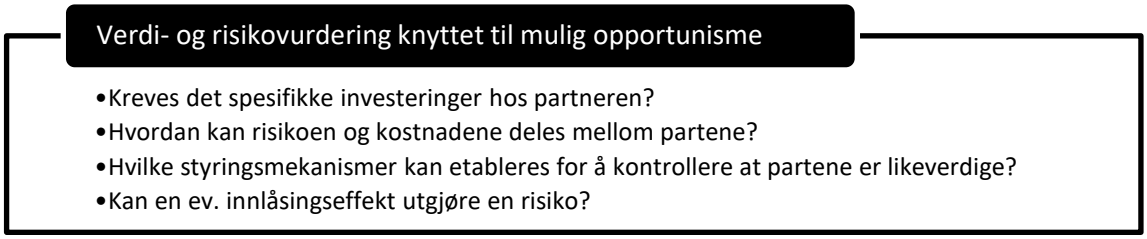
Figur 6.3 Forsvaret bør gjennomføre en systematisk kompetanseanalyse for å avdekke IKT-kompetansebehov. Kilde: Elstad, Endregard, et al., (2022), s. 53–54).

Gjennom en systematisk kompetanseanalyse vil Forsvaret få svar på hvilke kompetansetyper forsvarssektoren er avhengige av internt for å gjennomføre kjernevirksomheten. Ikke-kontrollerbare faktorer, som lover og regler, påvirker den systematiske kompetanseanalysen. Analysen

bør også inneholde en vurdering av potensielle sårbarheter ved manglende intern kompetanse – og hvilke konsekvenser slike mangler eventuelt kan få. Risikoen ved bruk av ekstern kompetanse må avveies mot det å ikke ha kompetansen i det hele tatt. Ved en eventuell avgjørelse om tjenesteutsetting bør Forsvaret også inkludere en vurdering av risikoen for at kompetanse og personell som forsvarssektoren ønsker å beholde internt forsvinner. Basert på den systematiske kompetanseanalysen kan det utarbeides en kompetanseutviklingsplan.

Ved en kombinasjon av interne og eksterne ressurser må Forsvaret være bevisst en økt risiko for opportunisme. Det vil si at en samarbeidspartner utnytter sårbarheten(e) til en annen partner (Barney, 2002). Et eksempel på opportunisme er at en strategisk partner utnytter transaksjonsspesifikke investeringer (f.eks. IKT-tjenester) fra forsvarssektoren i andre markeder (Elstad, Endregard, et al., 2022, s. 57). Dersom Forsvaret velger å kombinere interne og eksterne ressurser, er risikoen for opportunisme en type kostnad Forsvaret må være villig til å ta for å skaffe tilgang til nødvendige ressurser eksternt (jf. Barney, 2002).

Når interne og eksterne ressurser kombineres, kan en eventuell innlåsingseffekt utgjøre en risiko (Elstad, Endregard, et al., 2022). Forsvaret må gjøre en vurdering av hvor mye innlåsing som er akseptabelt. Det er behov for gjensidig avhengighet mellom kontraktspartene for å unngå en skjev maktbalanse (Elstad, Endregard, et al., 2022). Det må utføres helthetlige verdi- og risikovurderinger basert på en god systemforståelse når interne ressurser kombineres med strategiske partnere eller andre samarbeidspartnere (f.eks. konsulentfirmaer), som vist i figur 6.4:



Figur 6.4 Forsvaret bør gjennomføre verdi- og risikovurderinger knyttet til mulig opportunisme. Kilde: Elstad, Endregard, et al., (2022, s. 57–58).

I tillegg til opportunisme er det andre rammefaktorer, som forsvarlig sikkerhetsnivå og krigens folkerett, som kan være til hinder for at Forsvaret kan sette ut aktiviteter til strategiske partnere eller andre samarbeidspartnere (f.eks. konsulenter). Konkrete vurderinger er nødvendig for å identifisere hvilke aktiviteter som Forsvaret selv må utføre i henhold til krigens folkerett. For flere detaljer rundt denne problemstillingen, se Elstad, Endregard, et al. (2022). For å sørge for å ivareta et forsvarlig sikkerhetsnivå for IKT-virksomheten, er det nødvendig med helhetlig risiko- og sikkerhetsstyring, se underkapittel 6.6 og Endregard et al. (2023).

6.1.2 Ha tilgang til strategisk IKT-kompetanse

Strategisk kompetansemålbilde i staten har et mål om at lederne i staten skal ha tilstrekkelig kompetanse på hvordan ny teknologi påvirker utviklingen av virksomheten (Direktoratet for forvaltning og økonomistyring, 2022). En del av den strategiske IKT-kompetansen omhandler

helheten og den overordnede forståelsen for IKT-ens rolle i organisasjonen, inkludert hvordan og innenfor hvilke rammer organisasjonen ønsker å utvikle seg (se f.eks. Elstad, Lund, et al., 2022).

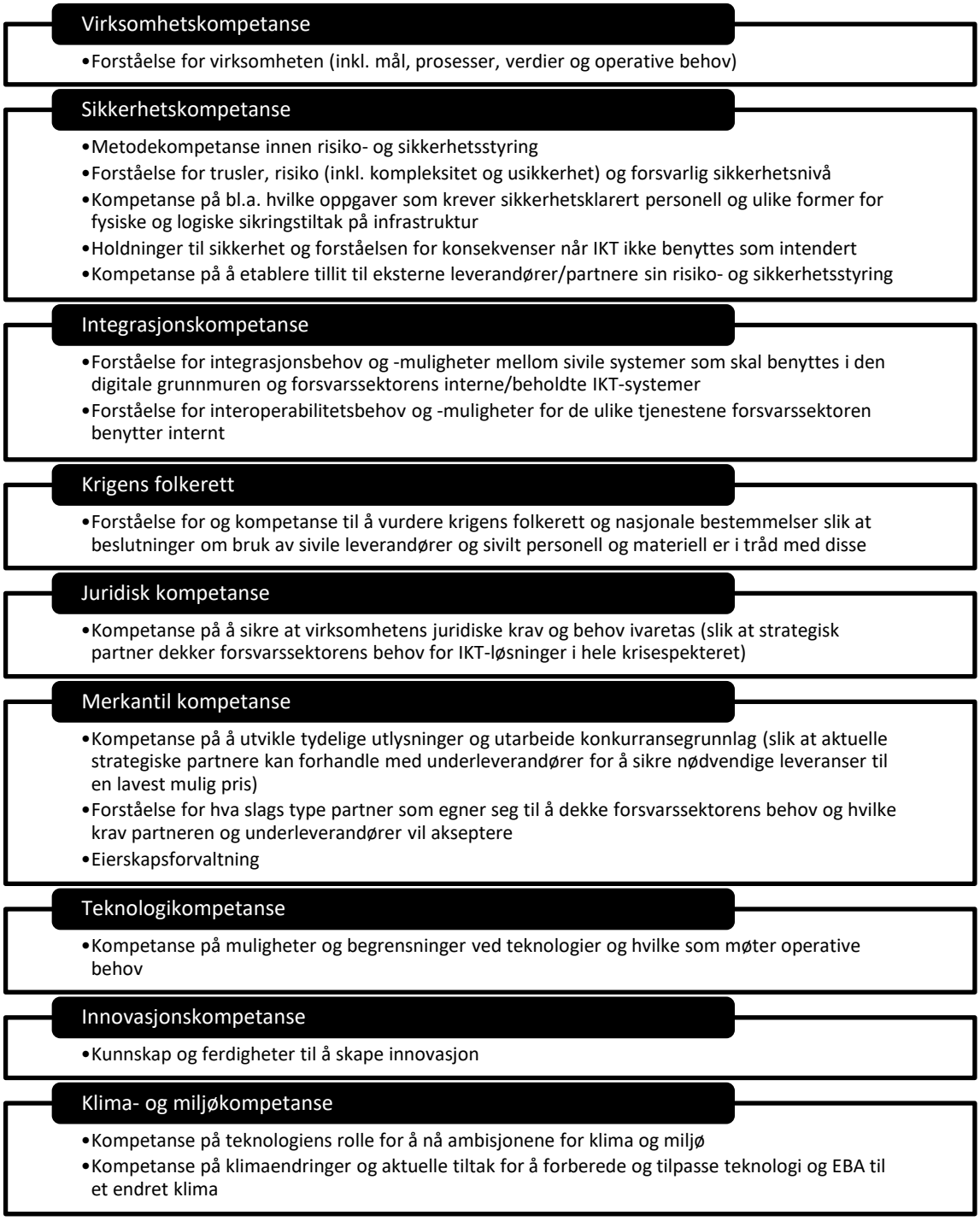
> Det rettes ofte kritikk mot moderne vitenskap om at den har blitt så oppstykket i små spesialiserte disipliner at den til slutt mister grepet om helheten. Ja, ikke bare forstår en disiplin et utsnitt av verden på sin måte, de tenderer hver og en til å redusere verden til det begrepsapparatet de rår over. […] [Det handler om] å skape oversikt over genuint ulike faglige bidrag og synssett, hvert enkelt med sin riktige forståelse. (Nyeng, 2004, s. 185–186)

Sitatet fra Nyeng (2004) har flere sentrale poeng, som er relevante i sammenheng med den digitale grunnmuren. Det vil være nødvendig å inkludere en rekke spesialiserte disipliner eller miljøer. Hver og en av disse disiplinene har sitt eget tankesett, mål og kompetansebehov for den digitale grunnmuren, og er en brikke i helheten. Noen miljøer har spesialistkompetanse innen kommunikasjonsprotokoller, mens andre miljøer har spesialistkompetanse på fortifikatorisk beskyttelse. Begge eksemplene er nødvendige brikker, men representerer ikke helheten.

Figur 6.5 viser kompetanseområder forsvarssektoren har behov for innen strategisk IKT-styring.[44] En analogi kan være at hver kompetansetype er en puslespillbrikke – en bestanddel. Puslespillbrikkene kan ikke alene forklare strategisk IKT-kompetanse. Jo flere brikker som settes sammen, jo tydeligere kommer puslespillmotivet fram. Det er først når alle puslespill-brikkene er satt sammen at motivet vises i sin helhet.

Vi har valgt å legge til kompetanse på klima og miljø i figur 6.5, siden dette er en rammefaktor Forsvaret må ta hensyn til i arbeidet med den digitale grunnmuren. Forsvaret har derfor behov for kompetanse på FNs bærekraftsmål innenfor klima og miljø (FN-sambandet, 2023b) og oversikt over hvilke ambisjoner Forsvaret og forsvarssektoren må ha for å bidra til å nå disse målene (jf. Forsvaret et al., 2022; Forsvarsdepartementet, 2020a). Videre er det nødvendig med kompetanse i Forsvaret på hvordan organisasjonen kan bidra til å nå disse ambisjonene. I tillegg trengs det kompetanse på klimaendringer og aktuelle tiltak for å forberede og tilpasse den digitale grunnmurens teknologiske kapabiliteter og EBA til et endret klima. Forsvaret har også behov for kompetanse på ny og innovativ teknologi og EBA som kan endre måten Forsvaret opererer på i retning av lavere klima- og miljøbelastning. Videre er det behov for kompetanse på energi-effektivitet, inkludert hvordan fornybare energikilder kan utnyttes best mulig, også for grunn-muren.

[44] Enkeltpersoner kan ikke inneha all type kompetanse som er beskrevet i figur 6.5. Det vil være tverrfaglige team som til sammen innehar kompetansetypene (som tidligere beskrevet i Elstad, Endregard, et al., 2022).

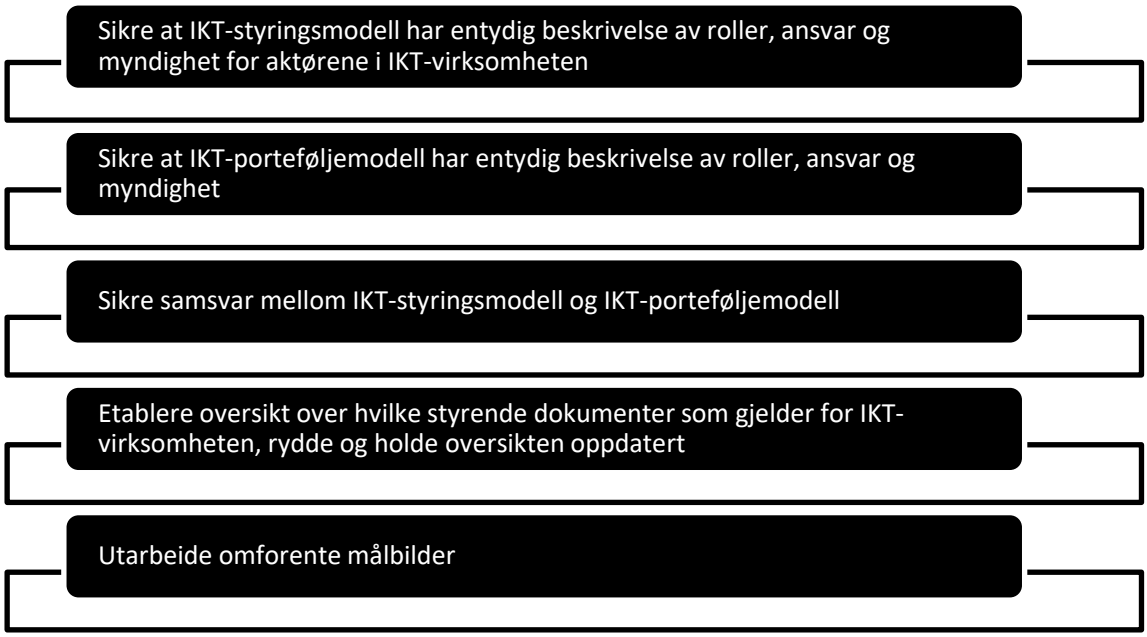


Figur 6.5 Ulike typer kompetanse det er behov for i forsvarssektoren for å utøve strategisk IKT-styring, hentet fra Elstad, Endregard, et al. (2022, s. 25). De ulike delene er inspirert av Birkemo et al. (2021, s.68–74) og Elstad, Lund, et al. (2022). I tillegg har vi valgt å legge til kompetanse på klima og miljø i oversikten.

6.2 Etablere strukturert fleksibilitet i styringen

Strukturert fleksibilitet i styringen er identifisert som en KSF for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur. Ordene «strukturert» og «fleksibilitet» er i seg selv noe motsigende. Det som menes med strukturert fleksibilitet er at det er et behov for å sette tydelige rammer, og at det er fleksibilitet innenfor disse rammene (Elstad, Lund, et al., 2022). Dersom det for eksempel blir en for sterk struktur og for lite handlingsrom, vil det bli vanskelig å oppnå og opprettholde den digitale grunnmuren. På den annen side, dersom det er for lite struktur, som avdekket i nåsituasjonen (se kapittel 4), oppstår det mangel på krav og helhet. Dette vil i sin tur føre til at Forsvaret vil stå i fare for omkamper, som kunne vært unngått dersom det hadde vært noe mer struktur. Det vil si at det er nødvendig å finne en balanse mellom struktur og fleksibilitet.

I figur 6.6 vises temaene vi kommer nærmere inn på i dette kapittelet:



Figur 6.6 En identifisert KSF for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur er «Etablere strukturert fleksibilitet i styringen».

6.2.1 Sikre at IKT-styringsmodell har entydig beskrivelse av roller, ansvar og myndighet for aktørene i IKT-virksomheten

Informantene oppfattet at fullmakt til å gjennomføre endringer var kritisk for å kunne oppnå og opprettholde den digitale grunnmuren. Et tema er derfor å sikre at IKT-styringsmodell har en entydig beskrivelse av roller, ansvar og myndighet for aktørene i IKT-virksomheten. Dette temaet er også vesentlig i det videre arbeidet med F24.

IKT-virksomheten, slik den er organisert i dag, er fordelt over flere etater som er underlagt FD. Det er avgjørende at IKT-styringsmodell blir autoritativ, og FD bør derfor utgi denne. Alternativt kan FD delegere ansvar og myndighet for utarbeidelsen av IKT-styringsmodell til Forsvaret. Denne delegeringen må være entydig, slik at beslutningene som Forsvaret tar om IKT-styringsmodell ikke kan bestrides i resten av forsvarssektoren.

Roller, ansvar og myndighet i IKT-virksomheten må være entydig beskrevet i IKT-styrings-modell, som gir den formelle beskrivelsen av roller, ansvar og myndighet i organisasjons-strukturen. Dersom IKT-styringsmodell er uklar, ufullstendig eller ikke i samsvar med andre relevante dokumenter, kan det medføre ulike hindre i gjennomføring av virksomhetsprosessene. Aktørene i IKT-virksomheten kan også bli usikre på hvem som har ansvar og myndighet til å gjennomføre de ulike prosessene. Aktørene kan også benytte usikkerheten til omkamper.

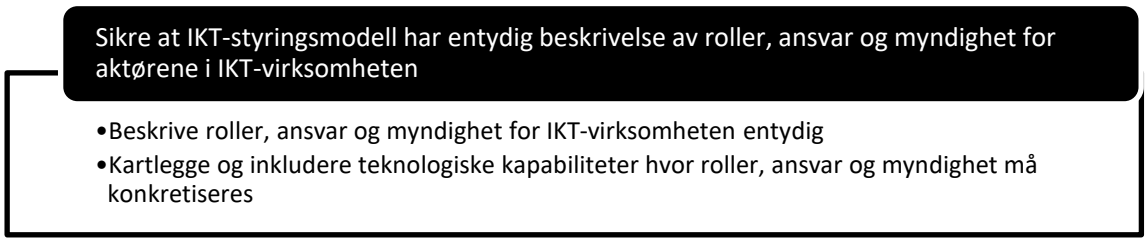
Vi foreslår at Forsvaret gjennomfører en kartlegging av hvilke teknologiske kapabiliteter som bør konkretiseres i IKT-styringsmodell. Et eksempel på en slik kapabilitet er «støtte og ivareta effektiv utvikling, drift og vedlikehold», som beskrevet i underkapittel 5.2.4, hvor det kan være behov for en tydeliggjøring av roller, ansvar og myndighet.

Behovet for tydelige roller, ansvar og myndighet forsterkes ved at digitale verdikjeder gjerne strekker seg over flere sektorer og landegrenser (Endregard et al., 2023). Lysne (2020, s. 13) bruker framtidens Nødnett som eksempel på en digital verdikjede. Realiseringen vil skje ved hjelp av kommersielle tilbydere, som er avhengig av andre, for eksempel regionale nettleveran-dører som 5G-basestasjoner er koblet til. De regionale tilbyderne er igjen avhengige av at det landsdekkende nettet de er tilkoblet fungerer, for å kunne levere de tjenestene de skal. Ulike former for systemer samvirker med basestasjonene, og disse systemene må fungere for at 5G-nettet kan fungere, eksempelvis kundedatabaser og styringssystemer.[45] Det er derfor nødvendig med avklaringer innen roller, ansvar og myndighet.

Vi anbefaler at FD utgir[46] en oppdatert versjon av IKT-styringsmodell ved endring i roller, ansvar og myndighet i IKT-virksomheten. Den gamle IKT-styringsmodellen må da settes ut av kraft, og den nye IKT-styringsmodellen må settes i kraft. Endringer av IKT-styringsmodell anbefales ikke gitt i ordre, tildelingsbrev eller andre skriv. Det må aldri eksistere usikkerhet i IKT-virksomheten om hvilken IKT-styringsmodell som er gjeldende.

Figur 6.7 oppsummerer punkter som bør inkluderes i arbeidet:

[45] Avsnittet er hentet fra Elstad, Endregard, et al. (2022 s. 14).
[46] Eller alternativt delegerer ansvar og myndighet for utarbeidelsen av IKT-styringsmodell til Forsvaret, som foreslått tidligere i underkapittelet.



Figur 6.7 IKT-styringsmodell må ha entydig beskrivelse av roller, ansvar og myndighet for aktørene i IKT-virksomheten.

6.2.2 Sikre at IKT-porteføljemodell har entydig beskrivelse av roller, ansvar og myndighet

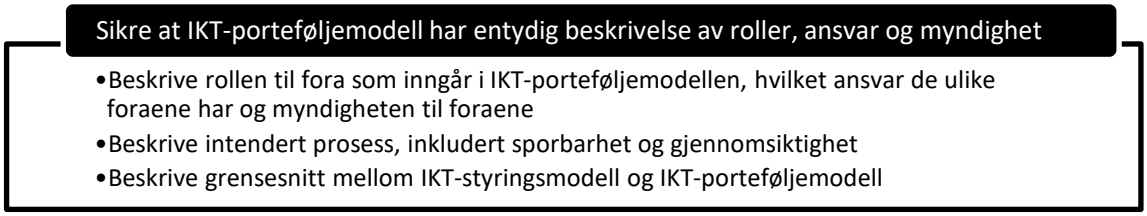
Som en del av arbeidet med IKT-styringsmodell har Forsvarsstaben utarbeidet en IKT-porteføljemodell.[47] I denne modellen er det definert en rekke fora, som IKT-porteføljestyre og behovseiermøter innen hovedområdene digital grunnmur, operasjoner og virksomhetsstyring. Disse foraene går på tvers av organisasjonsstrukturen i forsvarssektoren, og IKT-porteføljemodellen må derfor beskrive rollen, ansvaret og myndigheten til disse foraene på en entydig måte. I tillegg er det nødvendig å avklare grensesnittet mot øvrig porteføljestyring (dvs. for materiell som ikke er en del av IKT-porteføljen) i FST og FD.

IKT-porteføljestyringen slik den nå er tenkt, representerer en endring fra tidligere praksis ved at DRP setter rammer for utvikling, forvaltning og drift av IKT.[47] Disse rammene angir retning for forsvarssektorens IKT innenfor områder relevante for Forsvarets samfunnsoppdrag. DRP er derfor sentral for IKT-porteføljestyringsarbeidet.

I IKT-porteføljemodellen er det behov for en prosedyrebeskrivelse for aktørene, for at disse kan oppnå innsikt i intendert prosess. En for sterk struktur eller for detaljert beskrivelse kan i seg selv bli et hinder for prosessen, slik at det også må legges til rette for en viss fleksibilitet i den intenderte gjennomføringen. Beskrivelsen av intendert prosess bør si hvordan sporbarhet og gjennomsiktighet for beslutninger skal ivaretas, inkludert hvor beslutningsdokumenter skal lagres samt bruk av metadata. Sporbarhet vil si at det er mulig å finne tilbake til beslutningens opprinnelse (Hofstad, 2017). Ved sporbare beslutninger har de ansatte mulighet til å følge stegene i beslutningsprosessen, hvilke kriterier som har vært lagt til grunn og vurderinger knyttet til disse. Gjennomsiktighet vil si den oppfattede kvalitet på informasjon som er bevisst delt av en avsender (Schnackenberg & Tomlinson, 2016). Gjennomsiktighet handler derfor om åpenhet rundt beslutninger og påfølgende endringsprosesser overfor ansatte (og andre berørte aktører) som ikke direkte har deltatt i prosessen.

[47] For flere detaljer henviser vi til samarbeidsrommet «IKT-styring i forsvarssektoren» på FISBasis BEGRENSET.

Figur 6.8 oppsummerer punkter som bør inkluderes i arbeidet:



Figur 6.8 Forsvaret må sikre at IKT-porteføljemodell har entydig beskrivelse av roller, ansvar og myndighet.

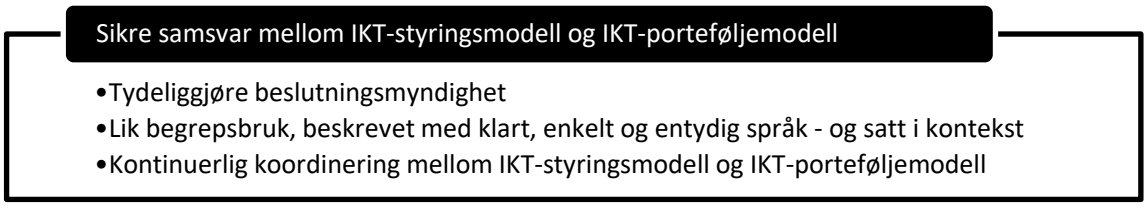
6.2.3 Sikre samsvar mellom IKT-styringsmodell og IKT-porteføljemodell

Det å sikre samsvar mellom IKT-styringsmodell og IKT-porteføljemodell er avdekket som et tema for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur. IKT-styringsmodell er tett knyttet til IKT-porteføljestyring. Det vil derfor være et behov for samsvar mellom disse modellene, slik at modellene ikke beskriver motstridende roller, ansvar og myndighet.

Språket i disse modellene må være klart, enkelt og entydig. Begrepsbruken i de to modellene må være lik. Ved nyanseforskjeller i begrepsbruken kan det oppstå tvil og usikkerhet, som kan skape misforståelser. Dette må i så fall adresseres, slik at beslutningsmyndigheten framkommer entydig.

IKT-virksomheten må ha avklarte ansvarsforhold, inkludert beslutningsmyndighet. Ved en eventuell uklarhet eller uenighet i ansvarsforhold kan motstridende beslutninger skje, beslutninger kan bli forsinket eller ikke gjennomført. Et eksempel kan være at IKT-porteføljestyret vedtar en prioritering som en aktør i IKT-virksomheten ikke har ressurser til å gjennomføre. Eller motsatt, kan en aktør i IKT-virksomheten gjennomføre en aktivitet som er nedprioritert av IKT-porteføljestyret. Utarbeidelsen av IKT-styringsmodell og IKT-porteføljemodell fordrer en fortløpende koordinering mellom de to, siden de beskriver hver sin del av en helhet som er avhengig av samsvar på tvers.

Figur 6.9 oppsummerer punkter som bør inkluderes i arbeidet:

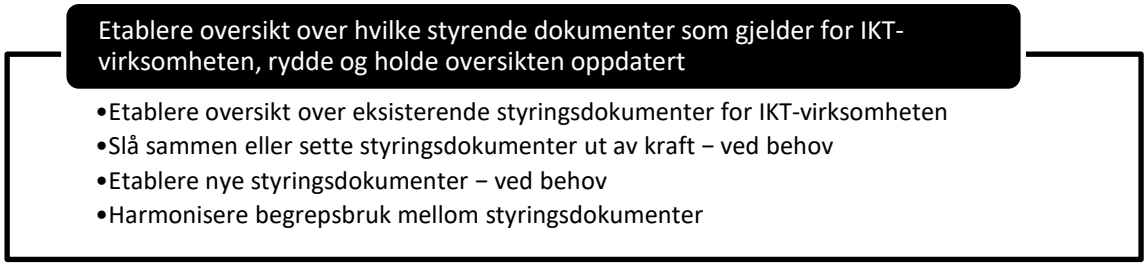


Figur 6.9 Forsvaret må sikre samsvar mellom IKT-styringsmodell og IKT-porteføljemodell.

6.2.4 Etablere oversikt over hvilke styrende dokumenter som gjelder for IKT-virksomheten, rydde og holde oversikten oppdatert

Det er nødvendig å etablere en oversikt over hvilke styrende dokumenter som gjelder for IKT-virksomheten, rydde og holde oversikten oppdatert. Et hvert styringsdokument må ha en avklart plass i dokumenthierarkiet. Det må ikke være tvil om hvilke styrende dokumenter som er gjeldende for IKT-virksomheten, inkludert plassen i dokumenthierarkiet. Det vil si at dersom det skulle oppstå konflikter mellom styringsdokumenter, vil plasseringen i dokumenthierarkiet avgjøre hvilket dokument som har forrang.

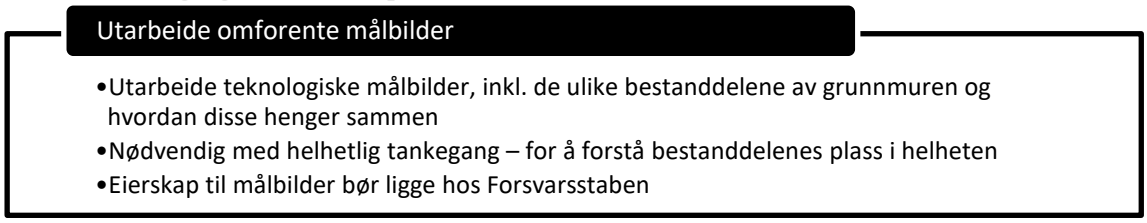
Vi anbefaler at Forsvaret etablerer en oversikt over alle gjeldende styringsdokumenter for IKT-virksomheten. Dette arbeidet kan avdekke behov for nye dokumenter, og vel så viktig, behov for å slå sammen dokumenter eller sette dokumenter ut av kraft. Arbeidet kan også avdekke hvilke dokumenter som har behov for en oppdatering, slik at beskrivelsen av roller, ansvar og myndighet blir i henhold til gjeldende IKT-styringsmodell. Figur 6.10 oppsummerer punkter som bør inkluderes i arbeidet:



Figur 6.10 Forsvaret må etablere oversikt over hvilke styrende dokumenter som gjelder for IKT-virksomheten, rydde og holde oversikten oppdatert.

6.2.5 Utarbeide omforente målbilder

Informantene var opptatt av at Forsvaret må utarbeide målbilder, og at det må sikres en felles forståelse og tilslutning til disse målbildene. Dette inkluderer også en felles forståelse for hvilke steg som må gjennomføres. Vi har derfor valgt å inkludere det å utarbeide omforente målbilder som et tema, og figur 6.11 viser punkter som bør inkluderes i arbeidet:



Figur 6.11 Forsvaret må utarbeide omforente målbilder.

I løpet av 2024 skal det, ifølge DRP, utarbeides målbilder og veikart både for den digitale grunnmuren som helhet og for bestanddelene (IT-plattform-, infrastruktur- og kommunikasjons-

tjenester). Den digitale grunnmuren består av et komplekst system av systemer med ulike teknologier, ulikt eierskap og ulik grad av modernitet, og dette vil utfordre etablering av separate målbilder for bestanddelene. I tillegg vil ny teknologi, særlig virtualisering, føre til at skillet mellom de ulike bestanddelene vil bli mer uklart, og delene vil til dels flyte over i hverandre. Arbeidet med målbilder og veikart vil derfor kreve en koordinering mellom miljøer i IKT-virksomheten, og helhetlig tankegang er avgjørende for å avdekke og ivareta avhengigheter. Eierskapet til disse dokumentene bør ligge i Forsvarsstaben.

6.3 Bedre evne og vilje til å gjennomføre endringer

I kapittel 4 ble det avdekket at Forsvaret har en svak kultur for endring og nytenkning, manglende evne til å ta i bruk ny teknologi og utfordringer med å henge med i utviklingen. Vår analyse viser også noen svakheter ved kulturen – ved at ord som «bekymringskultur» og «bikkjeslagsmål» ble nevnt under gruppesamtalene. Informantene ytret også et behov for «mer halleluja-stemning i Forsvaret – en felles forståelse». En informant uttalte at Forsvaret «må gjøre de riktige tingene, selv om det føles ubehagelig». Informantene ønsket at forsvarssektoren må klare å ta beslutninger om å gjennomføre ting selv om det ikke er perfekt. En informant uttalte at «det jobbes med beslutningsprosesser som ser ut til å kreve absolutt rasjonalitet. Det er ikke mulig. Vi må ta høyde for begrenset rasjonalitet». Derfor er «Bedre evne og vilje til å gjennomføre endringer» identifisert som en KSF for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur.

Forsvarssektoren har gjennomgående behov for tillit og tilhørighet mellom de ulike aktørene som inngår. Sektoren har subkulturer som nå både har ulike orienteringer, til dels overlapper hverandre og i enkelte tilfeller står i konflikt med og motarbeider hverandre. Slike subkulturer må ikke stå i veien for gjennomføring av de nødvendige endringene (Svendsen-utvalget, 2020).

I figur 6.12 vises temaene vi kommer nærmere inn på i dette kapittelet:

Figur 6.12 En identifisert KSF for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur er «Bedre evne og vilje til å gjennomføre endringer».

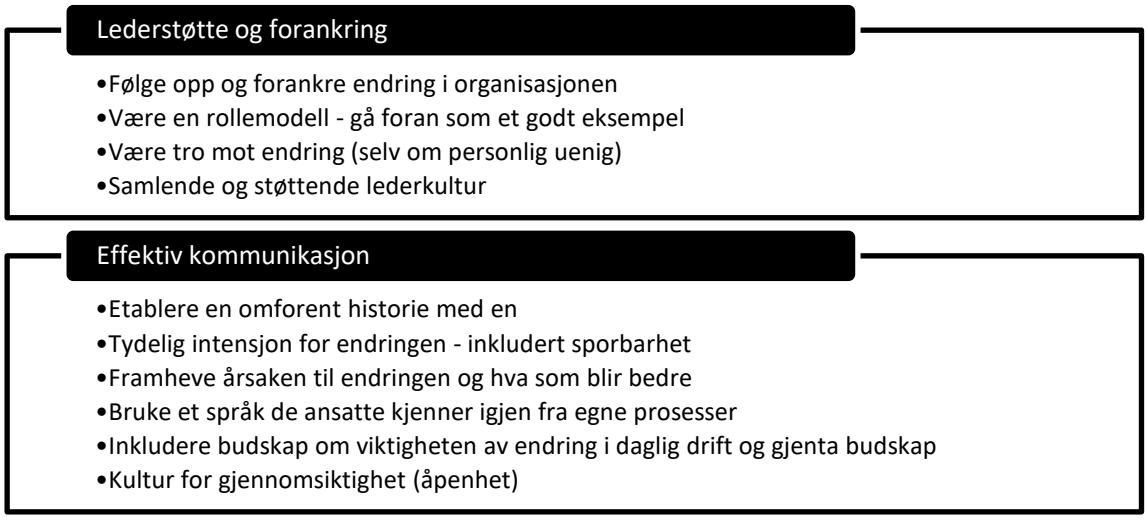
6.3.1 Videreutvikle kultur for lederstøtte, forankring og effektiv kommunikasjon

Effektiv kommunikasjon, lederstøtte (både på topp- og mellomledernivå) og lederengasjement er identifisert i litteraturen som noen av de mest sentrale faktorene for å oppnå en vellykket endringsprosess (se f.eks. Barth & Koch, 2019; Laureani & Antony, 2018). I en endringsprosess

er det nødvendig å ha en lederkultur med felles mønstre, hvor lederne jobber aktivt for at de ansatte skal oppfatte endringen som nyttig.

Lederne i IKT-virksomheten bør etablere et sett med felles mønstre av meninger og holdninger, som gir seg utslag i bestemte måter å handle på ved gjennomføringen av endringene. Lederne i IKT-virksomheten må følge opp endringene i praksis og forankre disse i den delen av IKT-virksomheten de er ansvarlige for. Det innebærer også at lederne i IKT-virksomheten må være tro mot endringene som er besluttet, selv om de i utgangspunktet er personlig uenig. For å oppnå aksept for endringene må ikke lederne i IKT-virksomheten undergrave beslutningene som er fattet. Ved endringer i virksomhetsprosesser anbefaler vi at det etableres en felles historie, som både topp- og mellomledere i IKT-virksomheten kan kommunisere til de ansatte. Kotter (2007) argumenterer for inkorporering av beskjeder i daglig arbeid, for å synliggjøre budskapet. Lederne må være tro mot den etablerte historien, hvor de ansatte får en forklaring fra ledelsen i egen avdeling om intensjonen bak endringen (hvorfor endringen gjennomføres) og hva som blir bedre med gjennomføringen av denne endringen. Historien må inneholde kjente begreper, og være knyttet til de ansattes egne arbeidsprosesser. Et eksempel på endring er innføring av produktområder i IKT-porteføljestyringen. Innenfor et produktområde vil det være tverrfaglige team. I teamene vil personer fra ulike fagmiljøer og kulturer måtte jobbe sammen, noe som kan kreve en viss tilpasning og evne til kompromiss fra deltakerne.

Figur 6.13 oppsummerer punkter som må inkluderes i arbeidet:



Figur 6.13 Forsvaret bør videreutvikle en kultur for lederstøtte, forankring og effektiv kommunikasjon.

6.3.2 Videreutvikle kultur for læringsfellesskap og tillit

Sosial påvirkning fra andre i organisasjonen kan ha en innvirkning på endringsatferd. Et tiltak som kan påvirke endringsatferd positivt er læringsfellesskap. Deltakernes motivasjon til å dele kunnskap er identifisert som en faktor for å lykkes med læringsfellesskap (Ardichvili et al.,

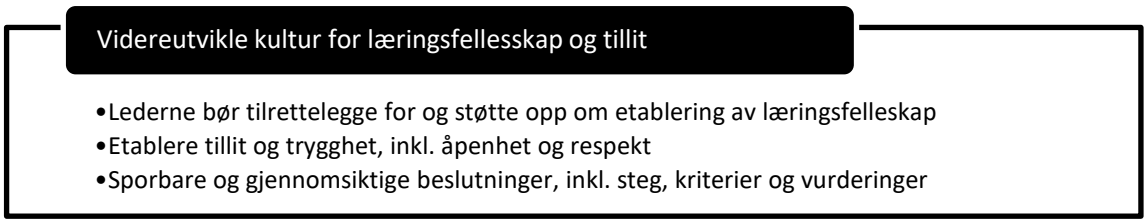
2003). Et læringsfellesskap kan legge til rette for utveksling av kunnskap om en moderne og motstandsdyktig digital grunnmur og være en kunnskapskilde for de ansatte under endrings-prosessene.

Lederne i IKT-virksomheten bør legge til rette for at ansatte kan delta i et læringsfelleskap underveis i endringsprosessene. Læringsfellesskapene kan bli fora for læring hvor kollegaer bygger hverandre opp underveis i endringsprosessene. Tillit og trygghet vil stå sentralt i slike læringsfellesskap. Kulturen må legge til rette for at det er lov å feile. Kulturen skal videre være støttende og inkluderende, hvor åpenhet og respekt for kollegaer er et felles mønster.

Ledelsesutfordringen med å bygge læringsfellesskap er ifølge McDermott (1999) å skape et miljø som ser på kunnskapsdeling som en verdi. Kunnskapsdeling og læring i organisasjoner foregår for det meste uformelt, og uformell læring kan i så måte være minst like viktig som formell læring. Selv om læringsfellesskapene bør være mest mulig autonome, kan de ha behov for støtte og hjelp. McDermott (1999) foreslår å opprette en støttefunksjon for fellesskapet. Vi foreslår at et medlem kan få rollen som koordinator, og hjelpe de andre medlemmene til å komme i kontakt med hverandre, tilføre nye ideer når fellesskapet begynner å miste energi eller lignende. Vi foreslår også at IKT-virksomheten kan etablere læringsfellesskap for ledere som håndterer endringen, slik at disse lederne kan dele kunnskap og erfaringer med hverandre.

Sporbarhet og gjennomsiktighet i beslutninger kan påvirke tillit. Sporbare beslutninger gir ansatte mulighet til å følge stegene og vurderingene som er gjort i beslutningsprosessen. I en kultur som innebærer gjennomsiktighet, tas ikke beslutningene «bak lukkede dører». Vi anbefaler derfor at det i IKT-virksomheten er en åpenhet rundt beslutningsprosessen, inkludert hvordan og hvorfor det endelige valget av tiltak (beslutning) ble som det ble. Gjennomsiktighet i beslutningsprosesser kan være med på å redusere bevisst skjevfordeling for egen vinning, korrupsjon, maktmisbruk og så videre og kan potensielt påvirke tilliten (Schnackenberg & Tomlinson, 2016).

Figur 6.14 oppsummerer mulige punkter som kan inkluderes i arbeidet:

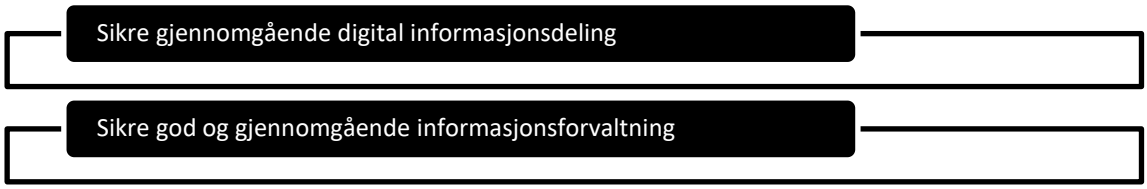


Figur 6.14 Forsvaret bør videreutvikle en kultur for læringsfellesskap og tillit.

6.4 Muliggjøre en datadrevet virksomhet

Data blir sett på som en strategisk ressurs, og styrende dokumenter legger vekt på behovet for deling, gjenbruk og utnyttelse av data i Forsvaret. Både IKT-strategi for forsvarssektoren

(Forsvarsdepartementet, 2019) og DRP (Forsvarsstaben, 2023) inkluderer mål om å være datadrevet. I tillegg sier strategi for kunstig intelligens i forsvarssektoren (Forsvarsdepartementet, 2023b, s. 23) at «Forsvarssektoren skal søke å fange alle data av verdi som produseres gjennom virksomhetene». Vi har derfor identifisert det å muliggjøre en datadrevet virksomhet som en KSF. Det må altså legges til rette for at Forsvaret kan bli datadrevet. Figur 6.15 viser temaene i dette kapittelet:[48]



Figur 6.15 En identifisert KSF for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur er «Muliggjøre en datadrevet virksomhet».

I dag eksisterer Forsvarets data i stor grad i IKT-systemene eller applikasjonstjenestene som produserte dem, og det er varierende om og i hvilken grad de kan deles ut av IKT-systemet eller applikasjonstjenesten. Dette resulterer i både teknologiske, sikkerhetsmessige og prosessuelle hindre for informasjonsdeling. Teknologiske og prosessuelle hindre kan reduseres ved å frigjøre dataene fra IKT-systemene, og sørge for at alle i Forsvaret som er autorisert og har nytte av dataene også får tilgang. Sikkerhetsmessig vil det imidlertid kunne oppstå nye utfordringer som må håndteres, for eksempel når det gjelder eierskap til data og autorisasjon for tilgang.

Data kan lagres i og tilbys fra grunnmuren. Alternativt kan applikasjonstjenesten eller IKT-systemet som produserer dataene lagre dem og gi tilgang gjennom standardiserte grensesnitt. Det må legges til rette for at grunnmuren skal kunne tilgjengeliggjøre data, og hvis det er hensiktsmessig, bør data også kunne lagres og prosesseres i grunnmuren. Brukeren skal ikke behøve å levere samme informasjon flere ganger til flere IKT-systemer, jamfør prinsipp i digitaliseringsstrategien (Forsvarsstaben, 2018).

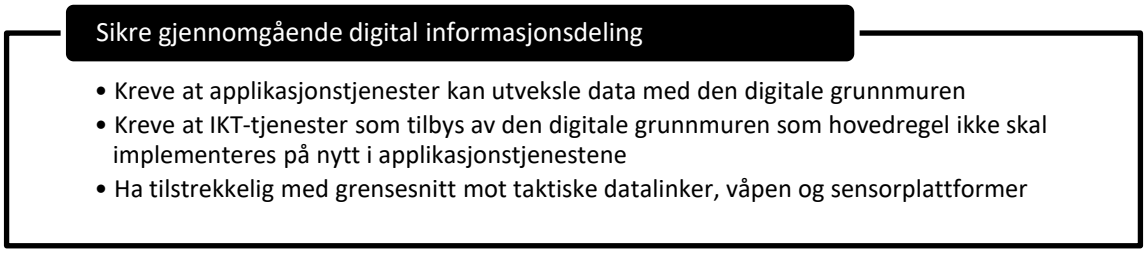
6.4.1 Sikre gjennomgående digital informasjonsdeling

I Elstad, Lund, et al. (2022) ble det å skape gjennomgående digital informasjonsdeling identifisert som en KSF for å oppnå kvalitet i beslutningsprosesser. Gjennomgående deling av data kan enten skje ved at applikasjonstjenester snakker direkte med hverandre («punkt-til-punkt»), eller ved at dataene sendes over en felles «buss» med standardiserte grensesnitt og formater. Normalt er det sistnevnte alternativet å foretrekke, da det gir større muligheter for deling – og nye applikasjonstjenester kan utnytte eksisterende delte data.

Den digitale grunnmuren vil med fordel kunne benyttes som en slik «buss» for datadeling, og kan dermed utgjøre den teknologien som muliggjør gjennomgående informasjonsdeling. Dette

[48] Vi har valgt å bruke ordet informasjonsforvaltning for det engelske begrepet *information management*.

krever imidlertid at det legges til rette for en slik datadeling, både teknologisk og i prosesser og prosedyrer. Figur 6.16 oppsummerer punkter som bør inkluderes i arbeidet:



Figur 6.16 Forsvaret bør bruke den digitale grunnmuren til å sikre gjennomgående digital informasjonsdeling.

Applikasjonstjenester som kjører på den digitale grunnmuren, og som enten produserer data av interesse for andre eller som kan utnytte data andre har produsert, må kunne utveksle data med den digitale grunnmuren. Dette fordrer at grunnmuren har grensesnitt som applikasjonstjenestene kan benytte for dataoverføring. Slike grensesnitt bør være standardiserte, jamfør Forsvarets IKT-strategi (Forsvarsstaben, 2021), som sier at «Forsvaret skal være en pådriver for bruk av standardiserte sammenkoblinger og informasjonsutvekslingsmekanismer». Der hvor det er hensiktsmessig og relevant bør Forsvaret benytte de samme standardene som Nato, og da særlig FMN. Forsvarets IKT-strategi (Forsvarsstaben, 2021) sier at «[FMN] skal legges til grunn for utveksling av informasjon med allierte samarbeidspartnere. Dette innebærer at relevant IKT må være kompatibel med gjeldende standarder (spirals) i FMN». Ved mottak av allierte styrker i Norge vil det å kunne koble IKT-systemer fra allierte nasjoner til Forsvarets digitale grunnmur øke muligheten for informasjonsutveksling og samvirke.

Den digitale grunnmuren skal legge premissene for informasjonsdeling og sikre informasjonsdeling og interoperabilitet mellom aktører. Ved å stille krav til grensesnittet mellom applikasjonstjenesten og den digitale grunnmuren (dvs. krav til dataformater, versjonsangivelse, osv.), gis det et handlingsrom for hvordan selve applikasjonstjenesten kan utformes. Som beskrevet i underkapittel 5.2.1 må det settes rammer for hvor omfattende en applikasjonstjeneste kan være, og generelt skal ikke applikasjonstjenester implementere IKT-tjenester som allerede tilbys av den digitale grunnmuren.

Hvis grunnmuren skal fungere som en «buss» for datadeling, må den også ha tilstrekkelig med grensesnitt mot Forsvarets mange våpen- og sensorplattformer. Disse produserer store mengder data som kan være til nytte også utenfor den enkelte plattform. Forsvarets IKT-strategi (Forsvarsstaben, 2021) sier at «Skal IKT være driver for K2 og samvirke er det essensielt å utnytte og integrere [kampplattformer, sensorer og effektorer] godt med øvrig IKT». For hver våpen- og sensorplattform bør det gjøres vurderinger av hvor nyttige dataene som produseres der kan være for andre deler av Forsvaret. Jo høyere nytteverdi, jo mer kan det forsvares å investere i grensesnitt mot den digitale grunnmuren.

6.4.2 Sikre god og gjennomgående informasjonsforvaltning

Forsvaret må ha et forvaltningsregime for all informasjon som skal kunne deles. Digitaliseringsdirektoratet definerer informasjonsforvaltning slik (Digitaliseringsdirektoratet, u.d.):

> Informasjonsforvaltning betyr eit heilskapleg syn på aktivitetar, verktøy og andre tiltak for å sikre best mogleg kvalitet, utnytting og sikring av informasjon i ei verksemd. Organiseringa av informasjonen skal vere systematisk og henge saman med verksemda sine arbeidsprosessar.

Det er en rekke spørsmål Forsvaret må ta stilling til i forbindelse med informasjonsforvaltning, og avklaringene på disse bør gjøres i regi av Forsvarsstaben. Eksempler på slike spørsmål er:

- Hvilke data skal deles og hvem eier dem?
- Hvilke formater skal dataene være tilgjengelige på?
- Hvor og hvordan skal de ulike dataene lagres (datastrukturer og lagringsmekanismer)?
- Hvordan håndtere livsløpet til dataene (*life cycle management)*?
- Hvordan sikre sporbarhet, integritet, autentisitet og konfidensialitet?

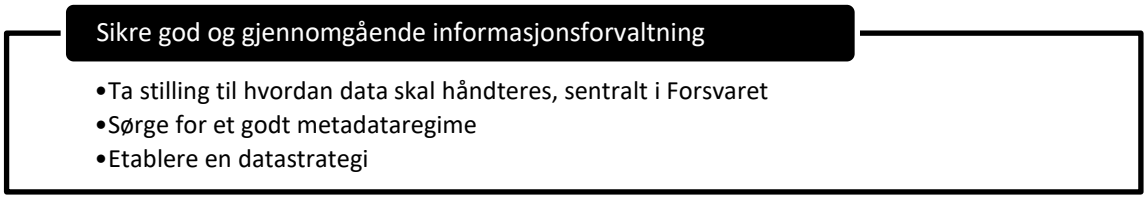
Som nevnt i Elstad, Lund, et al. (2022) er metadata nødvendig for å sikre god forvaltning og utnyttelse av data. Så langt som mulig bør Forsvaret benytte det samme metadataregimet som i Nato og FMN for å sikre interoperabilitet mot internasjonale allianse- og samarbeidspartnere.

UK MoD har gitt ut en Data Defence Strategy (Ministry of Defence, 2021) som inneholder et sett med regler for hvordan data skal håndteres. Ifølge disse reglene skal data ikke holdes i siloer. Videre skal organisasjonen vite hvilke data den har og hvor disse dataene befinner seg. Reglene sier også at data er varige og at de forvaltes og vedlikeholdes. I tillegg skal data være standardiserte, utnyttbare, sikre og pålitelige.

Det amerikanske forsvarsdepartementet (Department of Defense – DoD) har etablert et sett med mål for sine data i sin DoD Data Strategy (Department of Defense, 2020). Disse målene sier at data kan lokaliseres og at de er tilgjengelige og forståelige. Målene sier at dataene er pålitelige, at alle brukere har den samme representasjonen av dataene, og at dataene er sikret mot uautorisert bruk og manipulasjon.

Vår vurdering er at essensen i UK MoDs dataregler og DoDs mål er fornuftige og bør være til inspirasjon for en datastrategi eller -policy for forsvarssektoren. Et slikt dokument er det også ambisjoner om, da strategi for kunstig intelligens i forsvarssektoren (Forsvarsdepartementet, 2023b) sier at «Forsvarssektoren skal etablere en strategi eller policy for data som blant annet skal definere og identifisere hvordan data kan understøtte utviklingen av blant annet kunstig intelligens i sektoren.» Vi mener at det er nødvendig å utarbeide en slik strategi for datahåndtering for å sikre god deling og utnyttelse av data i hele sektoren.

Figur 6.17 oppsummerer mulige punkter som bør inkluderes:



Figur 6.17 For å sikre at data som deles kan gjenbrukes, må Forsvaret sørge for god og gjennomgående informasjonsforvaltning.

6.5 Utvikle en tilpasningsdyktig digital grunnmur

Som vi har vist i denne rapporten må Forsvarets moderne og motstandsdyktige digitale grunnmur være tilpasningsdyktig på en rekke måter, og i underkapittel 5.2 beskrev vi seks teknologiske kapabiliteter en digital grunnmur må inneha. Det å utvikle en tilpasningsdyktig digital grunnmur er derfor identifisert som en KSF.

Ved mottak av allierte styrker i Norge er skalerbarhet en nødvendig egenskap for grunnmuren. Antall brukere og tilknyttede informasjonssystemer øker kraftig på kort tid, og dette må den digitale grunnmuren håndtere. Om nødvendig må grunnmuren kunne differensiere trafikk og prioritere dynamisk, for å kunne sikre tilstrekkelig kapasitet for de høyest prioriterte IKT-tjenestene til enhver tid.

Videre må grunnmuren kunne konfigureres for en rekke ulike scenarioer, den må tillate endringer i hvor den brukes,[49] hvem som bruker den og hva den tilbyr av IKT-tjenester. Den må også støtte sentraliserte, lokale (autonome) og eksterne tjenester (f.eks. forsvarssektorens Office 365-løsning). I tillegg må grunnmuren håndtere grensesnitt mot en rekke ulike IKT-systemer (både forsvarssektorens egne, samarbeidspartneres og alliertes) og våpen- og sensorplattformer.

For å oppnå en slik tilpasningsdyktighet innenfor realistiske økonomiske rammer, er det nødvendig å basere grunnmuren på moderne virtualiserings- og skyteknologi. Både nettverk og plattform må virtualiseres så langt det er mulig og hensiktsmessig. Mens Forsvaret allerede har mye erfaring innen virtualisering av plattformer, så er det en lengre vei å gå på områder som skyteknologi og virtuelle kommunikasjonstjenester. Særlig sistnevnte vil kreve en annen måte å tenke på innenfor kommunikasjonstjenester, og kan bli utfordrende både med tanke på kompetanse og vilje til endring. Rapportene Lund et al. (2021), Flathagen et al. (2023) og Voldhaug et al. (2021) gir noen eksempler på hvilke muligheter som ligger i bruk av skyteknologi i Forsvaret.

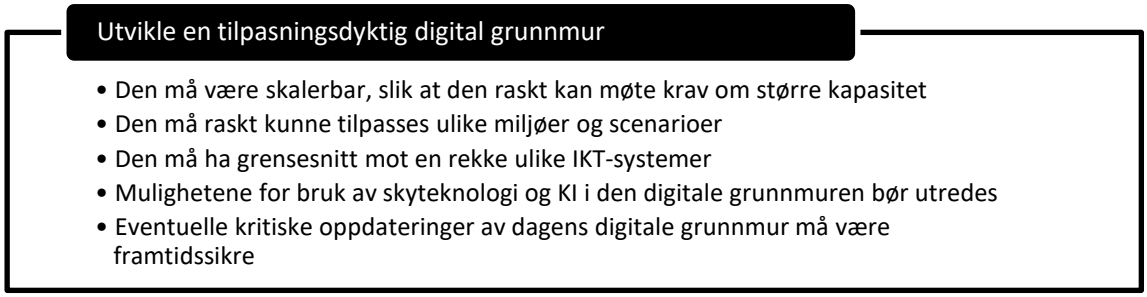
[49] Det bør også vurderes om den digitale grunnmuren skal støtte at applikasjonstjenester og data flyttes ut av landet i en krisesituasjon.

I tillegg til skyteknologi bør også KI utredes med tanke på å oppnå tilstrekkelig tilpasnings-dyktighet i den digitale grunnmuren. Begge teknologiene ble beskrevet i underkapittel 5.2. I en utredning bør blant annet disse spørsmålene undersøkes:

- Hvordan kan skyteknologi og KI bidra til økt grad av automatisering av styring og kontroll av den digitale grunnmuren?
- Hvilke oppgaver må fortsatt gjøres manuelt?
- Hvordan kan skyteknologi og KI gi bedre sikkerhet ved styring og kontroll av den digitale grunnmuren?
- Hvordan egner skyteknologi og KI seg for bruk på ulike graderingsnivåer?
- Hva skal til for å få sikkerhetsgodkjenning av løsninger basert på skyteknologi og KI – og kan noe bli enklere enn i dag?
- Hvilke IKT-tjenester kan etableres i ulike typer skyer – fra offentlig til privat?
- Hvordan kan IKT-tjenester og data flyttes ved behov?
- Hvilke krav stilles til EBA og infrastruktur som strømforsyning og vann, inkludert redundans?

I tillegg, ved kritiske oppdateringer for å opprettholde funksjonalitet i dagens digitale grunnmur, må ikke disse være til hinder for en kommende modernisering av grunnmuren. Investeringer gjort i dagens digitale grunnmur må heller ikke brukes som et argument mot en senere nødvendig modernisering av grunnmuren.

Figur 6.18 oppsummerer mulige punkter som kan inkluderes i arbeidet:



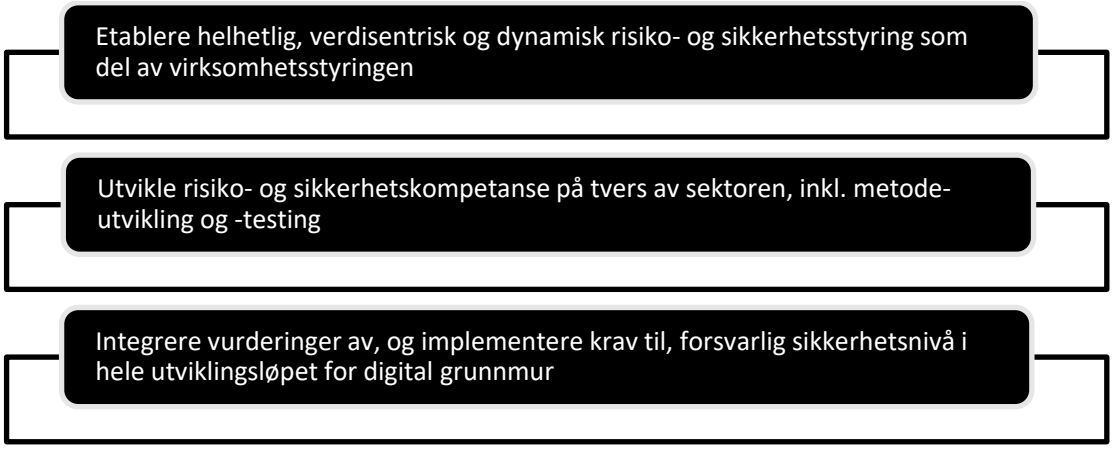
Figur 6.18 Forsvaret bør utvikle en tilpasningsdyktig digital grunnmur.

6.6 Etablere og vedlikeholde et forsvarlig sikkerhetsnivå

Informanter trakk fram hvor viktig det er å oppnå og ivareta helhetlig sikkerhet og inkludere sikkerhetsaspektene tidlig nok i design og utvikling av elementene og innretningen av den digitale grunnmuren. I 2022 påpekte Riksrevisjonen alvorlige sårbarheter i sikkerheten for Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner. Det pågår et omfattende arbeid for å rette på svakhetene og manglene, jamfør styrende dokumenter, prosesser og budsjetter. Det å etablere og vedlikeholde et forsvarlig sikkerhetsnivå

er derfor identifisert som en KSF for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur.

I figur 6.19 vises temaene vi kommer nærmere inn på i dette kapittelet:



Figur 6.19 En identifisert KSF for å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur er «Etablere og vedlikeholde et forsvarlig sikkerhetsnivå».

6.6.1 Etablere helhetlig, verdisentrisk og dynamisk risiko- og sikkerhetsstyring som del av virksomhetsstyringen

Forsvarssjefen har det overordnede og helhetlige ansvaret for strategisk IKT-styring og for å etablere et forsvarlig sikkerhetsnivå for den digitale grunnmuren og IKT-tjenestene som inngår i den. Ansvaret gjelder også for de IKT-tjenestene i grunnmuren som leveres av sivile tjenestetilbydere. Det er et lovkrav at risiko- og sikkerhetsstyring skal ivaretas som en integrert del av virksomhetsstyringen (jf. sikkerhetsloven § 4-2).

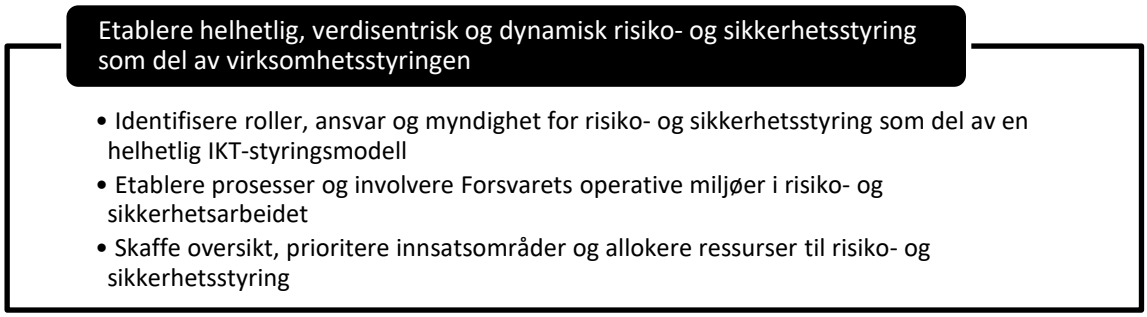
Et sentralt punkt for denne KSF-en er at risiko- og sikkerhetsstyringen må være helhetlig med klart definerte roller, ansvar og myndighet. Videre må risiko- og sikkerhetsstyring være en del av styringen og utviklingen for IKT-virksomheten og Forsvaret i sin helhet. Risiko- og sikkerhetsstyring kan ikke utføres i isolasjon fra resten av prosessene i Forsvaret. Med andre ord, dette temaet henger tett sammen med det å etablere strukturert fleksibilitet i styringen og bedre evne og vilje til å gjennomføre endringer.

Formålet med verdisentrisk risiko- og sikkerhetsstyring er å sikre Forsvarets kjerneoppgaver, nemlig at Forsvaret evner å utføre sine militære oppgaver i fred, krise og krig. Det betyr at forsvarlig sikkerhetsnivå for IKT-tjenestene i den digitale grunnmuren må utledes ut fra hvordan disse inngår i operative evner. Det er i tråd med systematikken i sikkerhetsloven at verdi- og skadevurderinger utføres ut fra hvordan IKT-tjenestene bidrar til forsvarssektorens grunnleggende nasjonale funksjoner og overordnede nasjonale sikkerhetsinteresser. Det er også i tråd med prinsippet om brukerorientering i digitaliseringsstrategien for Forsvaret (Forsvarsstaben, 2018). Operative miljøers behov og deltakelse er helt avgjørende i risiko- og sikkerhetsarbeidet.

En dynamisk risiko- og sikkerhetsstyring er nødvendig av to grunner. For det første skal Forsvarets behov for IKT-tjenestene i den digitale grunnmuren dekkes i det daglige arbeidet, i øvelser, og ikke minst i krise og væpnet konflikt. Omfanget og tilgjengelighet av IKT-tjenester i den digitale grunnmuren må derfor ta høyde for at operativ kontekst og dermed operative behov er dynamiske. For det andre skjer det stadige endringer i IKT-tjenestene i seg selv. Det kan være teknologiske endringer og oppdateringer, lukking av sårbarheter i programvare, med mer. Det kan også være endringer i digitale verdikjeder som endrer risikobildet, og ikke minst endringer i trusselbildet som påvirker behovet for sikkerhetstiltak.

Selv om det lovpålagte ansvaret er klart og mye arbeid er i gang for å styrke sikkerhetsstyringen innen IKT i Forsvaret, tar dette tid. En årsak er at arbeidet er omfattende og krever nye prosesser, samarbeid mellom aktører på ulike nivåer, kompetanseutvikling og nye metoder. I tillegg trengs det tid og ressurser for å etablere oversikt, gjøre gode prioriteringer og gjennomføre risikovurderinger som grunnlag for sikkerhetstiltak. Blant annet bør en slik oversikt inkludere hvilke IKT-tjenester som er en del av den digitale grunnmuren og hvilke IKT-tjenester som er tilgrensende. Vi anbefaler derfor Forsvaret å skaffe en god oversikt, prioritere innsatsområder og allokere ressurser til de mest presserende oppgavene i risiko- og sikkerhetsarbeidet.

Figur 6.20 oppsummerer noen viktige momenter som bør prioriteres i arbeidet:



Figur 6.20 Forsvaret bør intensivere arbeidet med å etablere risiko- og sikkerhetsstyring. Figuren peker på noen viktige momenter som bør prioriteres.

6.6.2 Utvikle risiko- og sikkerhetskompetanse på tvers av sektoren, inkludert metodeutvikling og -testing

Riksrevisjonen påpekte manglende kompetanse som én av årsakene til den utilstrekkelige sikkerheten. Behovet for sikkerhetskompetanse ble også trukket fram av informantene våre. Forsvaret må derfor utvikle nødvendig risiko- og sikkerhetskompetanse hos personell på ledernivå og hos ansatte ellers i organisasjonen. En del av denne kompetansen inkluderer også holdninger. Det må ikke undervurderes hva som kreves for å gjøre gode risiko- og sikkerhetsvurderinger og inkludere disse vurderingene i utviklingen av den digitale grunnmuren.

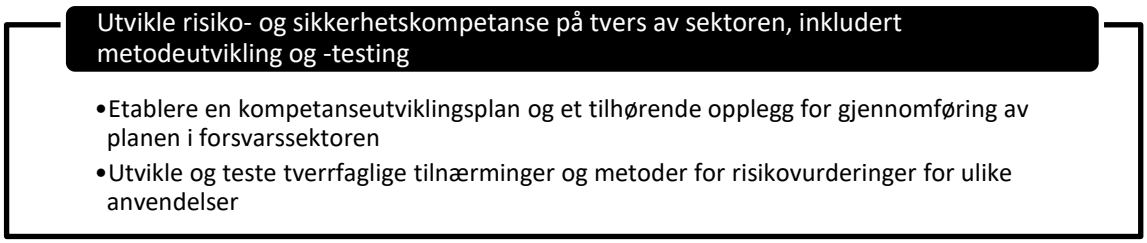
Som trukket fram i underkapittel 6.1, er det behov for en systematisk kompetanseanalyse og påfølgende kompetanseutviklingsplan. Vi framhever dette også spesifikt i forbindelse med

risiko og sikkerhet, fordi en slik plan er avgjørende for å lykkes med å etablere et forsvarlig sikkerhetsnivå. En felles kompetanseutviklingsplan og et tilhørende opplegg for å gjennomføre planen vil være et bidrag til etableringen av et forsvarlig sikkerhetsnivå. Hvilken type risiko- og sikkerhetskompetanse som er nødvendig, vil variere avhengig av personellets funksjon, men vi anbefaler en helhetlig plan og implementering av denne.

Det er behov for risiko- og sikkerhetsvurderinger på ulike nivåer og for ulike formål for den digitale grunnmuren. Det er behov for risikovurderinger på et overordnet nivå knyttet opp til strategiske valg for grunnmuren, det vil si om IKT-tjenestene dekker operative behov og har tilstrekkelig redundans i lys av ulike operasjonsscenarioer. Tekniske risikovurderinger for skjermingsverdige informasjonssystemer er nødvendig for sikkerhetsgodkjenning. Videre er risikovurderinger for IKT-tjenestene avgjørende for å vurdere om et forsvarlig sikkerhetsnivå med hensyn til tilgjengelighet, integritet og konfidensialitet er ivaretatt gjennom hele livsløpet.

Risikovurderinger er nødvendig i forbindelse med sourcing, det vil si som underlag for beslutninger om hele eller deler av en IKT-tjeneste skal utføres av forsvarssektoren selv eller *outsources* til en leverandør utenfor sektoren. En god risikovurderingsprosess er tverrfaglig, det vil si at kompetanseområder bringes sammen. Forsvaret bør utvikle og teste tilnærminger til risikovurderinger og metodiske verktøy, for ulike formål og sammen med interessentene på tvers av sektoren. Vi anbefaler å benytte konkrete caser til dette.

Figur 6.21 oppsummerer hvordan arbeidet med å utvikle risiko- og sikkerhetskompetanse på tvers av sektoren kan starte:



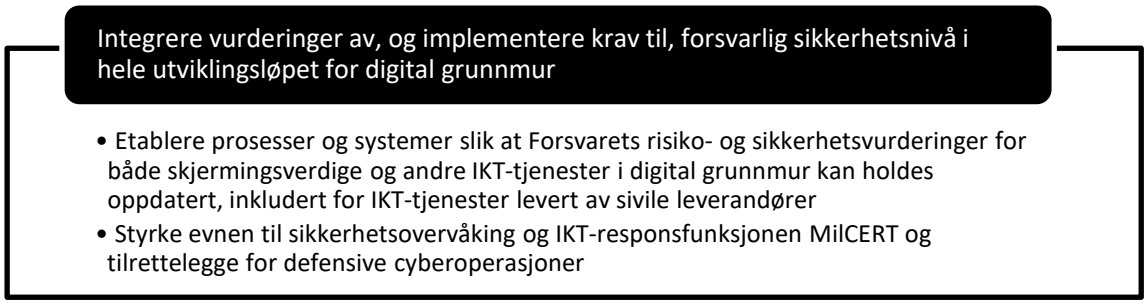
Figur 6.21 Forsvaret bør utvikle risiko- og sikkerhetskompetanse på tvers av sektoren. Figuren peker på hvordan arbeidet kan starte.

6.6.3 Integrere vurderinger av, og implementere krav til, forsvarlig sikkerhetsnivå i hele utviklingsløpet for digital grunnmur

Riksrevisjonen (2022) påpekte manglende oversikt over informasjonssystemer og tilhørende kommunikasjonsinfrastruktur samt dokumentasjon på IKT-området. Videre trakk Riksrevisjonen frem at verdi- og risikovurderinger for skjermingsverdige informasjonssystemer ikke er sluttført og dermed mangler sikkerhetsgodkjenning. Dette gjelder sannsynligvis også en del IKT-systemer som inngår i den digitale grunnmuren. Sikkerhetsgodkjenning er viktig, men er kun et første steg for å oppnå et forsvarlig sikkerhetsnivå og opprettholde det. Derfor bør det også, gjennom strategisk IKT-styring, etableres prosesser og utvikles egnede verktøy slik at

risiko- og sikkerhetsvurderinger for IKT-tjenester oppdateres av ansvarlige etater i tråd med de endringer som skjer, og at sikkerhetsgodkjenningen tilpasses deretter.

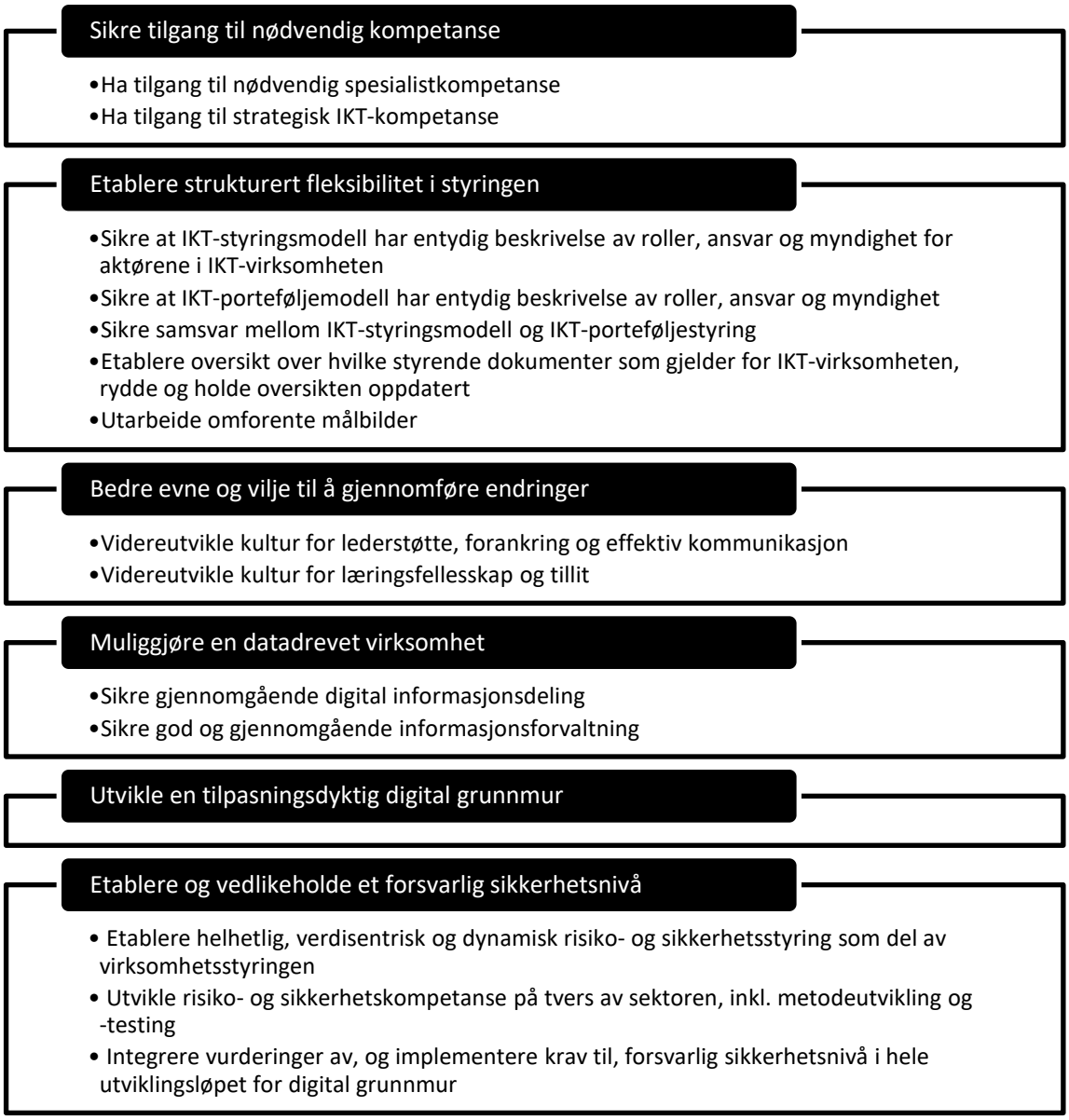
Forsvarssektoren er utsatt for trusler i og gjennom det digitale domenet. Et viktig aspekt ved IKT-sikkerhet er å kunne forebygge og motvirke trusler i og gjennom cyberdomenet. Et forsvarlig sikkerhetsnivå betyr at IKT-tjenestene skal fungere som intendert, at uautorisert tilgang hindres og at informasjonen i IKT-systemene ikke endres eller går tapt. Fortsatt styrking og utvikling av sikkerhetsovervåking og IKT-responsfunksjonen (MilCERT) er derfor viktig. Videre må den digitale grunnmuren legge til rette for defensive cyberoperasjoner slik at Forsvaret sikres handlefrihet i cyberdomenet og kan operere i fred, krise og krig. Figur 6.22 oppsummerer hva Forsvaret bør vektlegge:



Figur 6.22 Forsvaret bør integrere vurderinger av, og implementere krav til, forsvarlig sikkerhetsnivå i hele utviklingsløpet for den digitale grunnmuren.

6.7 Oppsummering av kritiske suksessfaktorer

I kapittel 6 har vi presentert KSF-er for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur. KSF-ene er oppsummert i figur 6.23:



Figur 6.23 Oppsummering av KSF-er for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur.

7 Oppsummering og anbefalinger

En forutsetning for at Forsvaret skal løse sine oppgaver i fred, krise og krig er tilgang til tilstrekkelig og hensiktsmessig IKT. Forsvaret har et mål om å oppnå og opprettholde en moderne og motstandsdyktig digital grunnmur. Problemstillingen i denne rapporten er hva Forsvaret, på et strategisk nivå, bør gjøre for å oppnå dette målet. Studien har følgende forskningsspørsmål:

- Hva innebærer Forsvarets moderne og motstandsdyktige digitale grunnmur i et helhetlig perspektiv?
- Sett i et helhetlig perspektiv, hvilke kritiske suksessfaktorer må til for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur?

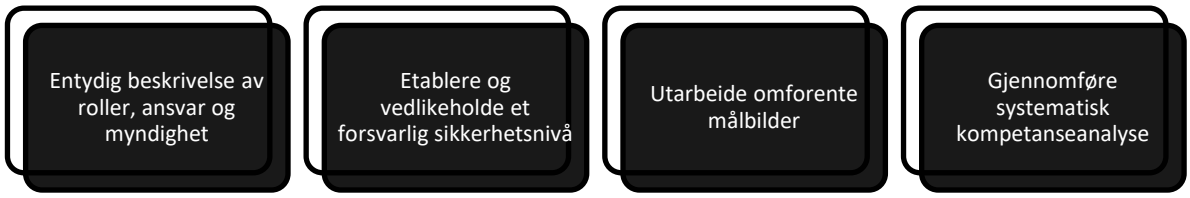
Vi har foreslått et rammeverk for et helhetlig perspektiv basert på Davis et al. (2014). Vårt rammeverk bygger på sosioteknisk systemteori. De sosiale og teknologiske faktorene er i et slikt perspektiv gjensidig avhengig av hverandre. I vårt helhetlige rammeverk inngår følgende faktorer (1) organisasjon og mål, (2) teknologi, (3) eiendom, bygg og anlegg, (4) prosesser og prosedyrer, (5) mennesker og (6) kultur.

Basert på analyser av innsamlede data (fra gruppesamtaler, workshops, uformelle samtaler og sekundærdata) beskrev vi i kapittel 4 nåsituasjonen for Forsvarets digitale grunnmur innenfor hver av de seks faktorene i rammeverket. Videre, i kapittel 5, beskrev vi hva Forsvarets moderne og motstandsdyktige digitale grunnmur innebærer.

I kapittel 6 identifiserte vi følgende KSF-er for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur:

- sikre tilgang til nødvendig kompetanse,
- etablere strukturert fleksibilitet i styringen,
- bedre evne og vilje til å gjennomføre endringer,
- muliggjøre en datadrevet virksomhet,
- utvikle en tilpasningsdyktig digital grunnmur og
- etablere og vedlikeholde et forsvarlig sikkerhetsnivå.

Hver av disse KSF-ene inneholder anbefalinger, og ettersom vi har benyttet en helhetlig tilnærming er det, naturlig nok, relativt mange av dem. Alle disse anbefalingene kan ikke håndteres på en gang. Forsvaret må starte et sted, og figur 7.1 viser hva Forsvaret først bør prioritere av våre foreslåtte anbefalinger.



Figur 7.1 Oppsummering av våre anbefalinger til hva Forsvaret først bør prioritere for å oppnå og opprettholde Forsvarets moderne og motstandsdyktige digitale grunnmur. Disse fire anbefalingene bør prioriteres likt.

Det å sikre en entydig beskrivelse av roller, ansvar og myndighet er en forutsetning for resten av anbefalingene. Vi anbefaler derfor at Forsvaret prioriterer dette. En entydig beskrivelse av roller, ansvar og myndighet legger grunnlaget for gjennomføring av prosesser og prosedyrer og gir rammer som mennesker og kultur må forholde seg til.

Som kritikken fra Riksrevisjonen (2022) viste, er det mangler og sårbarheter i sikkerheten for Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner. Disse må rettes opp for å etablere og vedlikeholde et forsvarlig sikkerhetsnivå. Dette krever arbeid i hele organisasjonen, og inkluderer alle faktorene i vårt rammeverk. Et avgjørende sted å starte er å skaffe god oversikt, prioritere innsatsområder og allokere ressurser til risiko- og sikkerhetsstyring.

Vi foreslår også at Forsvaret starter utarbeidelsen av omforente målbilder innenfor de ulike teknologiske bestanddelene av digital grunnmur og for helheten. I dette arbeidet er det avgjørende at det er tett koordinering mellom de ulike aktørene i IKT-virksomheten. Samtidig vil skyteknologi og KI utfordre inndelingen av digital grunnmur gjort i DRP, med IT-plattform, infrastruktur- og kommunikasjonstjenester, siden disse bestanddelene vil flyte mer over i hverandre ved overgang til slike nye teknologier.

I tillegg anbefaler vi at Forsvaret gjennomfører en systematisk kompetanseanalyse, for å avdekke hvilke IKT-kompetansebehov Forsvaret har, hvilke av disse som kan dekkes internt og eventuelt hvilke kompetansebehov som kan dekkes av eksterne samarbeidspartnere. Ved en tilnærming med eksterne samarbeidspartnere er det en rekke problemstillinger som må vurderes, som risiko for opportunisme, krigens folkerett og forsvarlig sikkerhetsnivå.

Forkortelser

ABE	Attributtbasert kryptering
C3	Consultation, Command and Control
CERT	Computer Emergency Response Team
DevSecOps	Development, Security, and Operations
DoD	Department of Defense
DRP	Digital reguleringsplan for forsvarssektoren
EBA	Eiendom, bygg og anlegg
Ekom	Elektroniske kommunikasjonstjenester
EMP	Elektromagnetisk puls
F24	Forsvarssektoren 2024
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
FKI	Forsvarets kommunikasjonsinfrastruktur
FMA	Forsvarsmateriell
FMR	Forsvarssjefens fagmilitære råd
FN	De forente nasjoner
GDPR	General Data Protection Regulation
GNF	Grunnleggende nasjonale funksjoner
HPM	High Power Microwave
IKT	Informasjons- og kommunikasjonsteknologi
IT	Informasjonsteknologi
K2	Kommando og kontroll
KI	Kunstig intelligens
KSF	Kritisk suksessfaktor
LTP	Langtidsplan for forsvarssektoren
MAST	Militær anvendelse av skytjenester
MilCERT	Military Computer Emergency Response Team – IKT responsmiljø
Nato	North Atlantic Treaty Organization
NBN	Nasjonalt BEGRENSET nett
NHN	Nasjonalt HEMMELIG nett
NIST	National Institute of Standards and Technology
NOU	Norges offentlige utredninger
PACE	Primary, Alternate, Contingency, Emergency
SIU	Sikker informasjonsutveksling
SOP	Standard eller stående operasjonsprosedyre
UK MoD	United Kingdom Ministry of Defence
VPN	Virtual Private Network
ZTA	Zero Trust Architecture

Referanser

Alberts, D. S. & Hayes, R. E. (2003). *Power to the edge: command, control in the information age*. CCRP Publication Series.

Alberts, D. S. & Hayes, R. E. (2005). *Campaigns of experimentation: pathways to innovation and transformation: code of best practice*. CCRP.

Alberts, D. S. & Hayes, R. E. (2007). *Planning: complex endeavors*. CCRP Publications.

Ali, M., Zhou, L., Miller, L. & Ieromonachou, P. (2016). User resistance in IT: A literature review. *International Journal of Information Management*, *36*(1), 35–43.

Allison, G. T. (1971). *Essence of Decisions: Explaining the Cuban Missile Crisis*. Little Brown.

Amoako-Gyampah, K. & Salam, A. F. (2004). An extension of the technology acceptance model in an ERP implementation environment. *Information & Management*, *41*(6), 731–745.

Andås, H. (2020). *Emerging technology trends for defence and security* (FFI-rapport 20/01050). Forsvarets forskningsinstitutt.

Anthony, R. N., Dearden, J. & Vancil, R. (1972). Key Economic Variables. I *Management Control Systems* (s. 147–156).

Ardichvili, A., Page, V. & Wentling, T. (2003). Motivation and Barriers to Participation in Virtual Knowledge-Sharing Communities of Practice. *Journal of Knowledge Management*, *7*(1), 64–77.

Arnfinnsson, B. & Kirkhorn, S. (2021). *Hvordan kan Forsvaret kutte utslipp av klimagasser? – en funksjonell studie* (FFI-rapport 21/01488). Forsvarets forskningsinstitutt.

Arnfinnsson, B. & Tønsberg, E. K. (2023). *Nullutslippsforsvaret – en mulighetsstudie av klima-vennlig teknologi for Forsvaret* (FFI-rapport 23/01418). Forsvarets forskningsinstitutt.

Atkinson, S. R. & Moffat, J. (2005). *The agile organization: From informal networks to complex effects and agility*. DoD CCRP publication series.

Axelos. (2011). *Management of Portfolios (MoP®), The Stationary Office*.

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

Barth, C. & Koch, S. (2019). Critical success factors in ERP upgrade projects. *Industrial Management & Data Systems*, *119*(3), 656–675.

Beadle, A., Diesen, S., Nyhamar, T. & Bostad, E. K. (2019). *Globale trender mot 2040 – et oppdatert fremtidsbilde* (FFI-rapport 19/00045). Forsvarets forskningsinstitutt.

Bentstuen, O. I. (2022). *Trender innen IKT – relatert til militærmakt*. Forsvarets forsknings-institutt. FFI-rapport 22/00544.

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

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

Bjørnstad, A. L. & Lichacz, F. M. J. (2013). Organizational flexibility from a network organizational perspective: A study of central predictors and moderating factors in military contexts. *Leadership and Organizational Development Journal*.

Bloebaum, T. H., Bentstuen, O. I., Birutis, B., Hansen, B. J., Hauge, M. & Mancini, F. (under arbeid). *Kampnær IKT*. Forsvarets forskningsinstitutt.

Bratbergsengen, K. (2021). *Digital infrastruktur*. Store norske leksikon på snl.no. Hentet 5.9.2023 fra https://snl.no/digital_infrastruktur.

Bukkestein, I., Volden, G. H. & Andersen, B. H. (2021). *Styring av prosjektporteføljer i offentlig sektor* (Concept-rapport nr. 65). Ex ante akademisk forlag.

Bush, T., Vanebo, J. O. & Dehlin, E. (2010). *Organisasjon og organisering*. Universitetesforlaget.
Cameron, K. (1978). Measuring organizational effectiveness in institutions of higher education. *Administrative Science Quarterly*, *23*, 604–632.
Cooper, C. G. (2023). *Internasjonal humanitærrett i Store norske leksikon på snl.no.* https://snl.no/internasjonal_humanit%C3%A6rrett.
Cortellazzo, L., Bruni, E. & Zampieri, R. (2019). The Role of Leadership in a Digitalized World: A Review. *Frontiers in Psychology*, *10*(1938).
Cyberforsvaret. (2020). *Nasjonalt konsept for kommunikasjon- og informasjonssystemer (CIS)* (BEGRENSET). Cyberforsvaret.
Cyberforsvaret. (2022). *Konsept for defensive cyberoperasjoner* (Datert 1.7.2022. Signert Sjef Cyberforsvaret). Cyberforsvaret.
Cyert, R. & March, J. G. (1963). *The Behavioral Theory of the Firm*. Prentice-Hall.
Cyert, R. & March, J. G. (1992). *A behavioral theory of the firm*. Blackwell.
Das, T. K. & Teng, B. S. (1999). Cognitive biases and strategic decision processes: An integrative perspective. *Journal of Management Studies*, *36*(6), 757–778.
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, M. C., Challenger, R., Jayewardene, D. N. W. & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics*, *45*(2, Part A), 171–180.
Department of Defense. (2020). *DOD Data Strategy*. Departement of Defense. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.
DeSanctis, G. & Poole, M. S. (1997). Transitions in teamwork in new organizational forms. *Advances in group processes*, *14*, 157–176.
Diesen, S. (2020, 20.12.2020). *Når endringer blir en trussel*. Stratagem. Hentet 2.11.2023 fra https://www.stratagem.no/nar-endringer-blir-en-trussel/.
Diesen, S. (2022). *Fra teknologi til strategi og operasjoner – teknologiutviklingens påvirkning på militære styrker og bruken av militærmakt* (FFI-rapport 22/01682). Forsvarets forskningsinstitutt.
Digitaliseringsdirektoratet. (u.d.). *Kva er informasjonsforvaltning?* Digitaliseringsdirektoratet. Hentet 8.11.2023 fra https://www.digdir.no/informasjonsforvaltning/kva-er-informasjonsforvaltning/2116.
Digitaliseringsrådet. (2018). *Digitaliseringsrådets anbefalingsbrev til Direktoratet for e-helse: Felles digital grunnmur*. https://www.digdir.no/digitaliseringsradet/direktoratet-e-helse-felles-digital-grunnmur/1803.
Direktoratet for forvaltning og økonomistyring. (2022). *Strategisk kompetansemålbilde*. Direktoratet for forvaltning og økonomistyring. https://arbeidsgiver.dfo.no/strategisk-hr/strategisk-kompetanseutvikling/strategisk-kompetansemalbilde.
Elstad, A. K., Endregard, M. & Mykkeltveit, A. (2022). *Sourcing for forsvarssektorens IKT-virksomhet – skisse til rammeverk* (FFI-rapport 22/02237). Forsvarets forsknings-institutt.
Elstad, A. K., Fuglseth, A. M. & Grønhaug, K. (2009). CSFs for Implementation of ERP Systems: A Literature Review and Critique. I J. Krogstie (Red.), *Norsk konferanse for organisasjoner bruk av informasjonsteknologi (NOKOBIT)* (s. 147–158). Tapir akademiske forlag.

Elstad, A. K., Langvik, G., Reitan, B. K. & Gran, C. J. (2016). *Sammensatte læringssystemer - Hvordan kan man legge til rette for læring og kunnskapsdeling på nett?* (FFI-notat 16/01816). Forsvarets forskningsinstitutt.

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

Endregard, M. (2019). Totalforsvaret i et sivilt perspektiv. I P. M. Norheim-Martinsen (Red.), *Det nye totalforsvaret*. Gyldendal Norsk Forlag.

Endregard, M. (2020). Totalforsvaret – samfunnet i væpnet konflikt IA. K. Larsen & G. L. Dyndal (Red.), *Strategisk ledelse i krise og krig. Det norske systemet* (s. 406–419). Universitetsforslaget.

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

Endregard, M. & Rongved, G. F. (2022). Fremtidens totalforsvar – gjensidighet eller gjenstridighet? I G. F. Rongved & P. M. Norheim-Martinsen (Red.), *Totalforsvaret i praksis*. Gyldendal Norsk Forlag.

Etterretningstjenesten. (2023). *Fokus 2023*. Etterretningstjenesten. https://www.etterretningstjenesten.no/publikasjoner/fokus/innhold.

Fardal, H. & Elstad, A. K. (2020). Decision-making in crisis management of a serious digital incident: A garbage can approach. *Journal of Emergency Management*, *18*(6), 489–498.

Fauske, M. F. (2023). *Hvordan påvirker automatisering av arbeidsoppgaver kompetansebehovet i Forsvaret?* (FFI-rapport 23/00995). Forsvarets forskningsinstitutt.

Fauske, M. F. & Strand, K. R. (2022). *Kompetansebehov i Forsvaret knyttet til fremtidige teknologier – intervjuer med FFIs teknologimiljøer* (FFI-rapport 22/01192). Forsvarets forskningsinstitutt.

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

Flathagen, J., Elstad, A. K., Endregard, M., Farsund, B., Bentstuen, O. I., Lund, K., Mykkeltveit, A. & Bloebaum, T. H. (2023). *Forsvarets IKT – utvalgte anbefalinger* (FFI-rapport 23/00409). 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.

FN-sambandet. (2023a, 28.6.2023). *Bærekraftig utvikling*. Hentet 7.11.2023 fra https://www.fn.no/tema/fattigdom/baerekraftig-utvikling.

FN-sambandet. (2023b, 18.9.2023). *FNs bærekraftsmål*. Hentet 7.10.2023 fra https://www.fn.no/om-fn/fns-baerekraftsmaal. For engelsk versjon se https://www.un.org/sustainabledevelopment/sustainable-development-goals/.

Forsvaret. (2019). *Forsvarets fellesoperative doktrine (FFOD) 2019* (Ikrafttredelse 1.12.2019). Forsvarsstaben.

Forsvaret. (2022). *Konsept for defensive cyberoperasjoner* (Datert 1.7.2022).

Forsvaret. (2023a, 30.8.2023). *Forsvarssektoren 2024*. https://www.forsvaret.no/soldater-og-ansatte/modernisering-og-effektivisering-i-forsvarssektoren/forsvarssektoren-2024

Forsvaret. (2023b). *Trygghet i usikre tider – Forsvarssjefens fagmilitære råd 2023*.

Forsvaret, Forsvarsbygg, Forsvarsmateriell & Forsvarets forskningsinstitutt. (2022). *Forsvarssektorens klima- og miljøstrategi.* https://www.forsvarsbygg.no/contentassets/c710de8776b7427f9a6756f6c41dc869/forsvarssektorensklima-ogmiljostrategi_kortversjon.pdf.

Forsvarsdepartementet (2016). *Prop. 1 S (2015–2016) for budsjettåret 2016 – Utgiftskapitler: 1700–1795 Inntektskapitler: 4700–4799*.
Forsvarsdepartementet. (2017a). *P8043 Konseptuell løsning (KL) for taktisk ledelsessystem for landdomene* (BEGRENSET).
Forsvarsdepartementet. (2017b). *Prop. 153 L (2016–2017). Lov om nasjonal sikkerhet (sikkerhetsloven)*. Forsvarsdepartementet.
Forsvarsdepartementet. (2019a). *IKT-strategi for forsvarssektoren – Hoveddokument* (Godkjent av Forsvarsministeren 27.3.2019). www.regjeringen.no/.
Forsvarsdepartementet. (2019b). *P8100 Konseptuell løsning for kommunikasjon til kampplattformer* (BEGRENSET).
Forsvarsdepartementet. (2020a). *Evne til forsvar – vilje til beredskap. Langtidsplan for forsvarssektoren* (Prop. 14 S (2020–2021)). www.regjeringen.no.
Forsvarsdepartementet. (2020b). *Tildelingsbrev for Forsvaret 2021*.
Forsvarsdepartementet. (2022). *Prop. 134 L (2021–2022). Endringer i forsvarsloven (utvidet adgang til å inngå kontrakt om tjenesteplikt mv.)*. www.regjeringen.no.
Forsvarsdepartementet. (2023a). *Prop. 1 S (2023–2024). For budsjettåret 2024 – Utgiftskapitler: 1700–1791 Inntektskapitler: 4700–4799.* www.regjeringen.no.
Forsvarsdepartementet. (2023b). *Strategi for kunstig intelligens i forsvarssektoren*. www.regjeringen.no.
Forsvarsdepartementet & Justis- og beredskapsdepartementet. (2018). *Støtte og samarbeid. En beskrivelse av totalforsvaret i dag*. www.regjeringen.no.
Forsvarsmateriell. (2021, 20.2.2023). *MAST*. Forsvarsmateriell. Hentet 7.11.2023 fra https://www.fma.no/anskaffelser/virksomhetsprogrammet-mast .
Forsvarsmateriell & Forsvaret. (2019). *Effektrealiseringsplan for program Mime, v. 1.0, juni 2019.*
Forsvarssjefen. (2013). *Manual i krigens folkerett*. Forsvaret.
Forsvarsstaben. (2018). *Digitaliseringsstrategi for Forsvaret*. Forsvarsstaben.
Forsvarsstaben. (2021). *Forsvarets IKT-strategi. Økt operativ effekt gjennom robust IKT i kontinuerlig utvikling – IKT for morgendagens forsvar*. Forsvarsstaben.
Forsvarsstaben. (2023). *Digital reguleringsplan (DRP) for forsvarssektoren* (Ikrafttredelse 15.2.2023. BEGRENSET). Forsvarsstaben.
Forsvarsstaben. (u.d.). S*amarbeidsrommet «IKT-styring i forsvarssektoren» på FISBasis BEGRENSET*.
Forvarsmateriell & Forsvaret. (2019). *Virksomhetsbeskrivelse for program Mime, v. 1.0, juni 2019*.
Friedman, A. L. & Miles, S. (2002). Developing stakeholder theory. *Journal of Management Studies*, *39*(1), 1–21.
Fuglseth, A. M. (1989). *Beslutningsstøtte: metode for diagnose av lederes informasjons- og situasjonsoppfatninger* [Doctoral thesis, Norwegian School of Economics and Business Administration]. Bergen.
Geertz, C. (1983). *Local knowledge: further essays in interpretive anthropology*. Basic.
Ghauri, P. N. & Grønhaug, K. (2005). *Research methods in business studies: a practical guide*. Financial Times Prentice Hall.
Goyal, V., Pandey, O., Sahai, A. & Waters, B. (2006). *Attribute-based encryption for fine-grained access control of encrypted data*. Proceedings of the 13th ACM conference on Computer and communications security, Alexandria, Virginia, USA.
Granlund, C., Lausund, K. B., Lausund, R., Klepper, K. B., Pedersen, M. N. & Voie, Ø. A. (2022). *Konsekvenser av klimaendringer og klimatilpasninger for Forsvaret fram mot*

2040 – rapport til Forsvarskommisjonen (FFI-rapport 22/02438). Forsvarets forskningsinstitutt.
Hatum, A. & Pettigrew, A. M. (2006). Determinants of organizational flexibility: a study in an emerging economy. *British Journal of Management*, *17*, 115–137.
Hislop, D. (2013). *Knowledge Management in Organizations: a critical introduction*. Oxford University Press.
Hofstad, K. (2017). *Sporbarhet i Store norske leksikon*. Hentet 23.4.2021 fra https://snl.no/sporbarhet.
IBM. (u.d.). *Software-Defined Data Centers*. https://www.ibm.com/topics/software-defined-data-center.
Ilie, V. & Turel, O. (2020). Manipulating user resistance to large-scale information systems through influence tactics. *Information & Management*, *57*(3), 103178.
IONOS. (2023, 22.3.2023). *Software Defined Data Center (SDDC)*. https://www.ionos.com/digitalguide/server/know-how/software-defined-data-center.
Jacobsen, D. I. & Thorsvik, J. (2007). *Hvordan organisasjoner fungerer* (3. utgave. utg.). Fagbokforlaget Vigmostad og Bjørke.
Johannessen, A., Tufte, P. A. & Kristoffersen, L. (2004). *Introduksjon til samfunnsvitenskapelig metode*. Abstrakt forlag.
Johnson, R. B. (1997). Examining the Validity Structure of Qualitative Research. *Education*, *118*(2), 282–292.
Jones, G. R. & Hill, C. W. L. (2013). *Theory of strategic management*. Cengage Learning.
Justis- og beredskapsdepartementet. (2021). *Høring om endringer i sikkerhetsloven (eierskap mv.)*. www.regjeringen.no.
Kiran, J. H. (2022). *Våpenvirkninger og beskyttelse – fortifikatoriske tiltak som del av helheten* (FFI-rapport 22/00427).
Kotter, J. P. (2007). Leading change – Why transformation efforts fail. *Harvard Business Review*, *85*(1), 96–103.
Kubernetes. (u.d.). *Production-Grade Container Orchestration*. Hentet 11.4.2022 fra https://kubernetes.io/.
Lai, L. (2011). Kompetansemobilisering og egenmotivasjon. *Magma*, *3*, 50–55.
Lai, L. (2013). *Strategisk kompetanseledelse* (3. utgave. utg.). Fagbokforlaget.
Laskey, K., Estefan, J. A., McCabe, F. G. & Thornton, D. (2009). *Reference architecture foundation for service oriented architecture version 1.0*.
Laureani, A. & Antony, J. (2018). Leadership – a critical success factor for the effective implementation of Lean Six Sigma. *Total Quality Management & Business Excellence*, *29*(5-6), 502–523.
Leavitt, H. J. (1965). Applied Organizational Change in Industry: Structural, Technological and Humanistic Approaches. I J. March (Red.), *Handbook of Organizations* (s. 1144–1170). Rand Mc Nally & Co.
Lewin, K. (1952). Group Decision and Social Change. I Newcomb & Hartley (Red.), *Readings in Social Psychology* (s. 459–473). Henry Holt and Company.
Lillestøl, J. (1994). *Kvalitet: ideer og metoder – offensiv kvalitetsutvikling*. Fagbokforlaget.
Lund, K., Johnsen, F. T. & Bergh, A. (2021). *Bruk av Skytjenester i Forsvaret – muligheter og utfordringer* (FFI-rapport 21/00136). Forsvarets forskningsinstitutt.
Lysne, O. (2020). *Risikostyring i digitale verdikjeder. Rapport fra en arbeidsgruppe ledet av professor Olav Lysne*. Direktoratet for samfunnssikkerhet og beredskap. https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf.

Lyytinen, K. & Newman, M. (2008). Explaining information systems change: a punctuated socio-technical change model. *European Journal of Information Systems*, *17*(6), 589–613.
MacKenzie, R. (2008). From networks to hierarchies: The construction of subcontracting regime in the Irish telecommunications industry. *Organization Studies*, *29*(6), 867–886.
March, J. (1994). *Primer on Decision Making: How Decisions Happen*. Simon and Schuster.
McDermott, R. (1999). Why Information Technology Inspired But Cannot Deliver Knowledge Management. *California Management Review*, *41*(4), 103–117.
Meld. St. 10 (2021–2022). *Prioriterte endringer, status og tiltak i forsvarssektoren*. Forsvarsdepartementet. www.regjeringen.no
Meld. St. 28 (2020−2021). *Vår felles digitale grunnmur − Mobil-, brebånds- og internett-tjenester*. Kommunal- og moderniseringsdepartementet. www.regjeringen.no
Meld. St. 40 (2020–2021). *Mål med mening – Norges handlingsplan for å nå bærekraftsmålene innen 2030*. Kommunal- og moderniseringsdepartementet. www.regjeringen.no
Microsoft. (u.d.-a). Hva er Azure*?* Microsoft. Hentet 15.01.2024 fra https://azure.microsoft.com/nb-no/resources/cloud-computing-dictionary/what-is-azure.
Microsoft. (u.d.-b). What is DevSecOps? Microsoft. Hentet 22.01.2024 fra https://www.microsoft.com/en-us/security/business/security-101/what-is-devsecops.
Miles, M. B. & Huberman, A. M. (1994). *Qualitative data analysis: an expanded sourcebook*. Sage.
Ministry of Defence. (2021). *Data Strategy for Defence*. Ministry of Defence. https://www.gov.uk/government/publications/data-strategy-for-defence.
Mykkeltveit, A. & Fongen, A. (2020). *Moderne løsninger for management av sammensatte kommunikasjonsinfrastrukturer* (FFI-rapport 20/01320). Forsvarets forskningsinstitutt.
Münch, C., Marx, E., Benz, L., Hartmann, E. & Matzner, M. (2022). Capabilities of digital servitization: Evidence from the socio-technical systems theory. *Technological Forecasting and Social Change*, *176*, 121361.
Mørk, B. E., Hoholm, T., Maaninen-Olsson, E. & Aanestad, M. (2012). Changing practice through boundary organizing: A case from medical R&D. *Human Relations*, *65*(2), 263–288.
Nasjonal kommunikasjonsmyndighet. (2019). *EkomROS 2019: Den digitale grunnmuren*. www.nkom.no/.
Nasjonal kommunikasjonsmyndighet. (2023). *Risiko 2023: Økt uforutsigbarhet krever høyere beredskap*. Nasjonal sikkerhetsmyndighet. www.nsm.no.
Nasjonal sikkerhetsmyndighet. (2020a). *Grunnprinsipper for IKT-sikkerhet 2.0*. www.nsm.no.
Nasjonal sikkerhetsmyndighet. (2020b). *Muligheter for en moderne IT-plattform* (VIRT-1902-NO).
Nasjonal sikkerhetsmyndighet. (2021). *Risiko 2021 − helhetlig sikring mot sammensatte trusler*. www.nsm.no.
National Institute of Standards and Technology (NIST). (2020, 10.8.2020). *Zero Trust Architecture*. National Institute of Standards and Technology (NIST). Hentet 7.11.2023 fra https://www.nist.gov/publications/zero-trust-architecture.
Nato. (2021). *Consultation, Command and Control board (C3B). C3 Taxonomy Baseline 5.0. Note by the Secretary* (AC/322-WP(2021)0017, C3 Taxonomy Baseline 5.0, 13 Aug 21.). https://www.nato.int/nato_static_fl2014/assets/pdf/2021/10/pdf/210830-C3-taxonomy-baseline.pdf.
Nato. (2022). *Federated Mission Networking*. Hentet 14.11.2022 fra https://www.act.nato.int/activities/fmn.

Nätt, T.H.(223) Virtualisering – IT i Store norske leksikon på snl.no. Hentet 11.1.2024 fra https://snl.no/virtualisering_-_IT.
NOU 2023: 14. *Forsvarskommisjonen av 2021 Forsvar for fred og frihet*. Forsvarsdepartementet. www.regjeringen.no.
NOU 2023: 17. *Totalberedskapskommisjonen. Nå er det alvor – Rustet for en usikker fremtid*. www.regjeringen.no.
Nyeng, F. (2004). *Vitenskapsteori for økonomer*. Abstrakt forl.
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.
Paroutis, S. & Al Saleh, A. (2009). Determinants of Knowledge Sharing Using Web 2.0 Technologies. *Journal of Knowledge Management*, *13*(4), 52–63.
Presterud, A. O., Lien, B. & Voldhaug, J. A. (2022). *Porteføljestyring i forsvarssektoren – Status i leveranseoppfølgingen* (FFI-rapport 22/01167. Unntatt offentlighet). 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.
Prop. 1 S (2023-2024). *For budsjettåret 2024*. Forsvarsdepartementet. www.regjeringen.no
Regjeringen. (2019). *Hva er personvern?* Kommunal- og distriktsdepartementet. www.regjeringen.no.
Regjeringen. (2022). *Hovedavtalen i staten* (Avtalen er inngått mellom Kommunal- og distriktsdepartementet (KDD) og hovedsammenslutningene LO Stat, YS Stat, Unio og Akademikerne). www.regjeringen.no.
Riksrevisjonen. (2022). *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner* (Ugradert versjon av Dokument 3:3 (2022−2023)). www.riksrevisjonen.no.
Rockart, J. F. (1979). Chief executives define their own data needs. *Harvard Business Review*, *57*(2), 81–93.
Roth, K. & Farahmand, K. A. (2023). Socio-Technical Study of Industry 4.0 and SMEs: Recent Insights from the Upper Midwest. *Sustainability 15*.
Schein, E. H. (2004). *Organizational culture and leadership* (4th. ed.). John Wiley & Sons, Inc.
Schnackenberg, A. K. & Tomlinson, E. C. (2016). Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships. *Journal of Management*, *42*(7), 1784–1810.
Simon, H. A. (1957). *Models of man*. John Wiley.
Simon, H. A. (1964). On the concept of Organizational Goal. *Administrative Science Quarterly*, *9*(1), 1–22.
Skjelland, E., Arnfinnsson, B., Birkemo, G. A., Bråthen, K., Glærum, S., Graarud, E., Hakvåg, U., Klepper, K. B., Kvalvik, S., Larsen, M. V., Mayer, M. J., Minos-Stensrud, M., Monsen, I. H. L., Mørkved, T., Nordvang, E. U., Presterud, A. O., Sellevåg, S. R., Sendstad, C., Sivathas, K., Strand, K. R., Thuv, A. & Voldhaug, J. A. (2023). *Forsvarsanalysen 2023* (FFI-rapport 23/00659). 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. A. (2022). *Forsvarsanalysen 2022* (FFI-rapport 22/00659). Forsvarets forskningsinstitutt.

Snider, B., da Silveira, G. J. C. & Balakrishnan, J. (2009). ERP implementation at SMEs: analysis of five Canadian cases. *International Journal of Operations & Production Management*, *29*(1), 4–29.
Sony, M. & Naik, S. (2020). Industry 4.0 integration with socio-technical systems theory: A systematic review and proposed theoretical model. *Technology in Society*, *61*, 101248.
Stacey, R. D. (2007). *Strategic Management and Organisational Dynamics: The Challenge of Complexity* (5. utg.). Prentice Hall.
Store norske leksikon (2005-2007). Applikasjon i Store norske leksikon på snl.no. Hentet 11.1.2024 fra https://snl.no/applikasjon.
Strand, M. (2023). *Hvor redd er kryptologene for kvantedatamaskiner?* Forsvarets forskningsinstitutt. Hentet 7.11.2023 fra https://www.ffi.no/aktuelt/blogg/hvor-redd-er-kryptologene-for-kvantedatamaskiner.
Svendsen-utvalget. (2020). *Økt evne til å kombinere menneske og teknologi – Veier mot et høyteknologisk forsvar* (Svendsen-utvalget, 24.6.2020). www.regjeringen.no.
The White House. (2021). *Executive Order on Improving the Nation's Cybersecurity*. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.
Usoro, A., Sharratt, M., Tsui, E. & Shekar, S. (2007). Trust as an Antecedent to Knowledge Sharing in Virtual Communities of Practice. *Knowledge Management Research and Practice*, *2007*(5), 199–212.
Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N. & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, *122*, 889–901.
Volberda, H. W. (1998). *Building the flexible firm: How to remain competitive*. Oxford University Press.
Voldhaug, J. A., 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.
Wenger, E. (1998). *Communities of practice: learning, meaning, and identity*. Cambridge University Press.
Wenger, E. & Snyder, W. M. (2000). Communities of Practice: The Organizational Frontier. *Harvard Business Review*, *January-February*, 139–145.
Wixom, B. H. & Todd, P. A. (2005). A Theoretical Integration of User Satisfaction and Technology Acceptance. *Information Systems Research*, *16*(1), 85–102.
Zikmund, W. G. (2003). *Business research methods*. Thomson/South-Western.

Liste over lover, forskrifter og konvensjoner

Arbeidsmiljøloven. (2005). *Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)* (LOV-2005-06-17-62).
Beredskapsloven. (1950). *Lov om særlige rådgjerder under krig, krigsfare og liknende forhold (beredskapsloven)* (LOV-1950-12-15-7).
Endringslov til sikkerhetsloven. (2023). *Lov om endringer i sikkerhetsloven (eierskapskontroll og lovens virkeområde)* (LOV-2023-06-20-77).
Forskrift om behandling av personopplysninger. (2018). *Forskrift om behandling av personopplysninger,* (FOR-2018-06-15-876).
Forsvarsloven. (2016). *Lov om verneplikt og tjeneste i Forsvaret m.m. (forsvarsloven)* (LOV-2016-08-12-77).

Genève-konvensjonene. *Genève-konvensjonen om behandling av krigsfanger, med vedlegg (Konvensjon III). Ratifisert 3.8.1951. Ikrafttredelsesdato: 3.2.1952.*
Grunnloven. (1814). *Kongerike Norges Grunnlov* (LOV-1814-05-17).
Menneskerettsloven. (1999). *Lov om styrking av menneskerettighetenes stilling i norsk rett*.
Personopplysningsloven. (2018). *Lov om behandling av personopplysninger (personopplysningsloven)* (LOV-2018-06-15-38).
Sikkerhetsloven. (2018). *Lov om nasjonal sikkerhet (sikkerhetsloven)* (LOV-2018-06-01-24).
Vernepliktsforskriften. (2017). *Forskrift om verneplikt og heimevernstjeneste (vernepliktsforskriften)* (FOR-2017-06-16-779).
Virksomhetsikkerhetsforskriften. (2018). *Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften)* (FOR-2018-12-20-2053).

Om FFI

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

FFIs formål

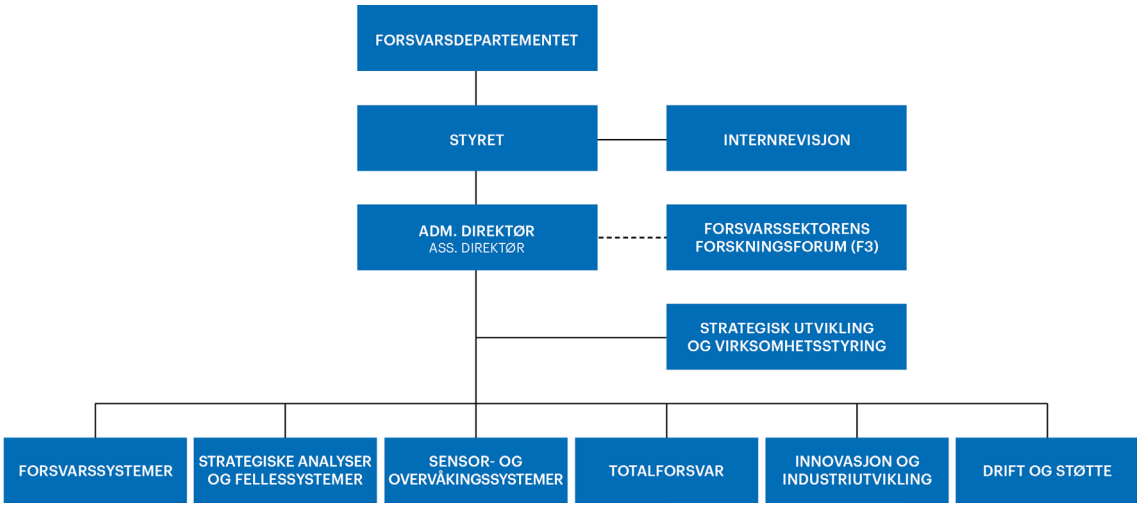
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som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