FFI Forsvarets forskningsinstitutt

22/01569

FFI-RAPPORT

Hvordan håndtere IKT i Forsvarets langtidsplanlegging

Bodil Hvesser Farsund
Aasmund Thuv
Bjørn Jervell Hansen

Hvordan håndtere IKT i Forsvarets langtidsplanlegging

Bodil Hvesser Farsund
Aasmund Thuv
Bjørn Jervell Hansen

Forsvarets forskningsinstitutt (FFI) 27. oktober 2022

Emneord
IKT
Langtidsplanlegging
Kapabilitet
Metoder

FFI-rapport
22/01569

Prosjektnummer
1501

Elektronisk ISBN
978-82-464-3424-7

Engelsk tittel
How to include operational ICT in Norwegian long-term defence planning

Godkjennere
Ronny Windvik, *forskningssjef*
Espen Skjelland, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Informasjons- og kommunikasjonsteknologi (IKT) er i dag mangelfullt representert i Forsvarets langtidsplanlegging. Dette gjelder både i FFIs metode for å støtte denne planleggingen og mer generelt. Dette har konsekvenser for muligheten til å gjøre hensiktsmessige investeringer i Forsvaret generelt og i IKT spesielt.

FFIs metode for å støtte Forsvarets langtidsplanlegging er scenario- og kapabilitetsbasert. Det vil si at den benytter scenarioer for å beskrive sikkerhetspolitiske utfordringer Forsvaret vil kunne møte i framtiden. Kapabiliteter brukes for å beskrive de evnene Forsvaret trenger for å møte disse utfordringene. FFI har god erfaring med å benytte denne metoden, men noen av egenskapene ved IKT gjør det vanskelig å integrere dette feltet direkte i metodikken. Blant annet er det vanskelig å måle hvordan IKT bidrar til operativ nytte og å vurdere risikoen knyttet til bruken. Vi argumenterer også for at dagens tilnærming med et fåtalls egne IKT-kapabiliteter ikke fungerer tilfredsstillende.

Derfor har vi ønsket å finne en tilnærming hvor man kan fortsette å benytte FFIs metode for å støtte Forsvarets langtidsplanlegging, men hvor IKT blir behandlet på en mer tilfredsstillende måte. Den grunnleggende ideen bygger på at IKT støtter opp under de forskjellige kapasitetene til strukturelementene i Forsvaret, både som en komponent i strukturelementene og som en integrator og støttefunksjon som sørger for at strukturelementer kan samhandle. Dette bør det tas hensyn til i langtidsplanleggingen. Vi foreslår at dette gjøres gjennom å analysere strukturelementene anvendelse av IKT basert på en grundig informasjonsinnsamling. Videre bør det analyseres hvordan IKT-systemene påvirker strukturelementenes kapasitet. I denne rapporten presenterer vi et forslag til en slik metode.

Vi har testet denne metoden i to caser. Erfaringene tilsier at selv om det kan være et omfattende arbeid å samle inn den nødvendige informasjonen, er det gjennomførbart, og det gir interessante resultater.

Summary

Information and communication technology (ICT) is insufficiently represented in long-term defence planning. This is the case both for FFIs method supporting such processes, and the processes themselves. As a result, the possibility of making appropriate investments in ICT for use in military operations and investments in the Armed Forces more generally is negatively affected.

The method FFI uses to support the Norwegian Armed Forces' long term defence planning utilizes a scenario and capability based approach. Scenarios are used to describe security challenges the Armed Forces may face in the future, while capabilities describe the abilities needed to meet them. FFI has used this method many times with good results, but some of the characteristics of ICT makes it difficult to integrate this field directly into the methodology. This includes the difficulty of measuring how ICT contributes to operational effectiveness and of assessing the risks associated with ICT use. We argue that today's approach, where a small set of ICT capabilities are defined, is not satisfactory for a number of reasons.

We have therefore developed an approach where ICT is integrated into the method in a more suitable way. Our starting point is the recognition that ICT enables capabilities to function, by being a component of force structure elements in their delivery of capabilities, and by being an integrator that enables force structure elements to interact and collaborate. This fact should be taken into account in long-term planning. We suggest that this may be done by gathering information and analyzing how force structure elements use ICT, followed by assessments of how this use affects the capacities of the force structure elements. In this report, we present a proof-of-concept method.

We have tested this method through two case studies. Our experiences indicate that while the work required to gather and analyze necessary information may be quite extensive, the method works and provides relevant results.

Innhold

Forord

Vi vil gjerne takke FFI-forskerne Jan Henry Pay, Vegard Bjonge, Aleksander Vatn Skaldebø, Ståle Ingarson Mellesdal, Rune Stensrud og Sigmund Valaker for god hjelp med å teste ut vår tilnærming og for å ha gitt bistand ved utvikling av casene.

Kjeller, 27. oktober 2022

Bodil H. Farsund
Aasmund Thuv
Bjørn J. Hansen

1 Innledning

Forsvaret er i dag svært avhengig av IKT[1] for å kunne gjennomføre militære fellesoperasjoner. Dette illustreres blant annet i Forsvarets IKT-strategi: «Informasjons- og kommunikasjonsteknologi (IKT) er en kritisk faktor for at Forsvaret skal kunne løse sine oppgaver i krig, krise og fred.»[2] Samtidig er denne teknologien i en rivende utvikling som blir drevet frem av sivile teknologiselskaper, og Forsvaret ønsker å utnytte de mulighetene dette bringer med seg. Dette vil øke avhengigheten ytterligere.

IKT er likevel ett av flere områder som per i dag ikke er tilstrekkelig representert i langtidsplanleggingen i Forsvaret, i den forstand at sammenhengen mellom IKT og operativ evne i svært liten grad er fanget opp. Langtidsplanlegging har som mål å identifisere hvilke evner Forsvaret bør ha på sikt, og dette kan blant annet brukes til å utlede hvilke konkrete strukturelementer som bør anskaffes. Slik langtidsplanleggingen gjennomføres i dag, er det imidlertid ikke rom for å gjøre strukturerte vurderinger rundt IKT som for eksempel kan gi grunnlag for å vurdere IKT-anskaffelser på tilsvarende måte som man i dag vurderer anskaffelse av strukturelementer. Dette hemmer Forsvarets muligheter til å gjøre vurderinger rundt operativ nytte, behov og kostnader tilsvarende det som gjøres for de tradisjonelle strukturelementene.

Med dette som bakgrunn, har én av de overordnede målsettingene med FFI-prosjekt *Forsvarets bruk av det digitale og elektromagnetiske rom* vært å sette Forsvaret og Forsvarsdepartementet (FD) bedre i stand til å gjøre helhetlige vurderinger av kapasiteter innen IKT både i forsvarsplanleggingen og i planleggingen av militære operasjoner. I denne rapporten er fokuset på IKT og langtidsplanlegging, men innholdet kan også være nyttig i andre sammenhenger.

Målgruppen for rapporten er derfor primært analytikere og beslutningstakere knyttet til langtidsplanleggingen i Forsvaret, det vil si de som utarbeider analyser for valg og prioritering av fremtidige kapabiliteter og strukturelementer.

Langtidsplanlegging i forsvarssektoren ledes av FD og støttes blant annet av FFIs prosjektserie *Støtte til FDs langtidsplanlegging* (SIMFOR). SIMFOR benytter en scenario- og kapabilitetsbasert metode, ofte omtalt som SIMFOR-metoden. Scenarioene beskriver mulige sikkerhetspolitiske utfordringer Norge kan møte, og kapabilitetene brukes for å beskrive hvilke evner Forsvaret må ha for å møte disse utfordringene. Vi har i vår tilnærming valgt å legge oss tett opp til SIMFORs metodikk for langtidsplanlegging, siden FFI har god erfaring med å benytte denne.

I denne rapporten argumenterer vi for at det ikke er fornuftig å håndtere IKT som egne kapabiliteter ved langtidsplanlegging, men at disse teknologiene heller bør forstås som en integrator og støttefunksjon for de mer tradisjonelle strukturelementene. Vi har videre utviklet og testet ut en metode for å se hvordan IKT-systemer påvirker de mer tradisjonelle struktur-

[1] Informasjons- og kommunikasjonsteknologi.
[2] Forsvarsstaben (2021); *Forsvarets IKT-strategi*. Side 5.

elementenes kapabiliteter[3]. Gjennom den utviklede metoden synliggjøres IKT-vurderinger vi mener er hensiktsmessige og gjennomførbare. Akkurat hva som gjøres som del av SIMFOR-metoden og hva som gjøres som underlagsstudier, er ikke videre vurdert.

Håndtering av IKT i militær langtidsplanlegging er et lite utforsket tema, og vi har ikke funnet litteratur om dette. Selv om Forsvaret har mange aktiviteter som omhandler planlegging og innføring av fremtidig IKT, faller disse utenfor vår definisjon av langtidsplanlegging.[4]

1.1 Begreper

Følgende begreper er sentrale i denne rapporten:

Informasjons- og kommunikasjonsteknologi (IKT)[5]
Samlebetegnelse for teknologi for innhenting, overføring, bearbeiding, lagring og presentasjon av informasjon.

IKT-system
Systemer som bruker IKT til innhenting, overføring, bearbeiding, lagring og/eller presentasjon av informasjon.

IKT-infrastruktur
IKT som sørger for at IKT-systemer kan kobles sammen og utveksle informasjon.

Med disse definisjonene kan grensesnittet mellom IKT-system og IKT-infrastruktur være noe uklar. Dette har ingen betydning for innholdet i denne rapporten.

IKT-anvendelse (forkortet «anvendelse»)
IKT-anvendelse sier noe om bruken av IKT-systemer. En anvendelse er knyttet til struktur-elementets bruk av et gitt system. Brukeren kan i denne sammenheng være en person som utfører oppgaver (for eksempel operativt personell), en plattform eller et system (for eksempel et fartøy som bruker et system for å overføre data).

Kapabilitet
En kapabilitet er evnen til å oppnå en ønsket effekt.[6] I langtidsplanlegging omfatter dette evne til å løse en bestemt oppgave eller oppnå et mål i en militær operasjon.[7]

[3] Metoden er testet ut på to caser gjengitt i Farsund, B.H. Thuv, Aa., Hansen, B. J. (2022); *Hvordan håndtere operativ IKT i Forsvarets langtidsplanlegging? – et innspill med testcaser;* FFI-rapport 22/01703 [BEGRENSET].
[4] Se for eksempel Regjeringen; *Fremtidige anskaffelser til forsvarssektoren (FAF) 2021-2028*; https://www.regjeringen.no/contentassets/09d83a5cbefd4fb68064e6ca871acccb/faf-2021-2028-norsk-versjon-__.pdf [sist besøkt 05.09.22].
[5] Store Norske Leksikon; https://snl.no/IKT [sist besøkt 08.08.22].
[6] Stensrud, R.; Rutledal, F.; Danjord, F.: Helesnes, J.-I.; Bjørnesgaard, T. (2007); *Metode for konseptutvikling*; FFI-rapport 2007/01722.
[7] Vatne, D.F.;Køber, P.K.; Guttelvik, M.S.; Arnfinnsson, B.; Rise, Ø.R. (2020); *Norwegian long-term defence analysis – a scenario- and capability-based approach*; FFI-rapport 20/02367.

Kapasitet
Kapasitet angir mengden av en kapabilitet. Mengden angis opp mot en referanseenhet, der referanseenheten er et strukturelement med den gitte kapabiliteten. Man måler derfor de andre strukturelementene som har denne kapabiliteten opp mot dette gitte strukturelementet.

Langtidsplanlegging
Forsvarsplanlegging er prosess som søker å sikre at en stat har et forsvar som klarer å utføre sine oppgaver og oppnå sine mål for hele spekteret av dets virksomhet.[8] Langtidsplanlegging er en planleggingsdisiplin innen forsvarsplanlegging som fokuserer på en lengre tidshorisont, typisk 10–30 år.[9]

Resiliens
Resiliens er evne til å tilpasse seg endrede betingelser og forberede seg på anslag, motstå disse og hurtig returnere til et tilstrekkelig funksjonsnivå.[10]

SIMFOR-metodikken
SIMFOR-metodikken er en scenario- og kapabilitetsbasert metodisk tilnærming til langtids-planlegging som FFI har utviklet med utgangspunkt i Natos arbeid med langtidsplanlegging.

SIMFOR-metoden
SIMFOR-metoden er en sentral del av SIMFOR-metodikken, og er en stegvis fremgangsmåte som belyser krav som kan stilles til en styrkestruktur, kapabilitetene en styrkestruktur har, og gapet mellom disse. Metoden kan brukes på større eller mindre deler av styrkestrukturen og på ulike abstraksjonsnivåer, men er typisk forbundet med sitt navn når hele Forsvarets styrke-struktur analyseres på overordnet nivå.

Strukturelement
Et strukturelement er en klart avgrenset del av en organisasjon bestående av personell, prosesser og systemer.[11]

1.2 Avgrensning

Dette arbeidet er en videreføring av innspill til metode for å håndtere IKT i Forsvarets langtidsplanlegging, hvor ett av to alternativer ble valgt for videre utvikling.[12]

[8] Fritt formulert etter Stojkovic og Dahl 2007: «Defence planning seeks to ensure that a nation has the necessary forces, assets, facilities and capabilities to fulfil its tasks throughout the full spectrum of its missions» (s. 7).
[9] Fritt formulert etter Stojkovic og Dahl 2007: "Long term defence planning is a specific planning discipline that is related to the relatively distant future…". (s. 7) "... assumed to have a time horizon of 10 years or more" (s. 10).
[10] «[A]bility to adapt to changing conditions and prepare for, withstand and rapidly recover from disruption». DHS Risk Lexicon 2010 Edition https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf [sist besøkt 08.08.22].
[11] Prinsix; https://www.fma.no/prinsix/maler/terminologi [sist besøkt 05.09.22]. Se også fotnote 21.
[12] Thuv Aa.; Farsund, B. H.; Hansen, B.J.; Enemo, G. (u.å); *Innspill til integrasjon av IKT i langtidsplanlegging;* under utarbeidelse.

I arbeidet med å utvikle denne første versjonen av metoden har det vært nødvendig å gjøre noen prioriteringer. For det første er det IKT-anvendelsen som har vært i fokus, og ikke det å vurdere resiliensen til IKT-systemene. Å vurdere IKT-systemenes resiliens er en omfattende problemstilling som blir sett videre på i FFI-prosjektet *Risiko og sikkerhet for kritiske digitale systemer og infrastrukturer.*

For det andre har vi konsentrert oss om konsekvensene av å degradere eksisterende IKT-systemer, fremfor å se på økt operativ evne på grunn av mer eller ny og bedre IKT. Når vi har sett på degradering av IKT, har vi fokusert på IKT-sikkerhetsegenskapen tilgjengelighet, mens integritet og konfidensialitet i liten grad har blitt behandlet.

Det finnes ulike typer IKT-systemer i Forsvaret. Vi har valgt å konsentrere oss om IKT-systemene som benyttes direkte av personell. Det vil si at vi for eksempel ikke har sett på IKT som er innebygget i materiell og/eller som opptrer mer autonomt.

1.3 Rapportens struktur

Vi starter rapporten med å gi en kort introduksjon til langtidsplanlegging og da med spesielt fokus på SIMFOR-metoden i kapittel 2. Deretter gir vi et overordnet bilde av IKT i kapittel 3, før vi beskriver utfordringene som er knyttet til å inkludere IKT i langtidsplanleggingen i kapittel 4. Hvordan IKT blir håndtert i SIMFOR-metodikken i dag blir beskrevet i kapittel 5, mens vår tilnærming blir beskrevet i kapittel 6. Rapporten avsluttes med noen erfaringer knyttet til tilnærmingen i kapittel 7 og en oppsummering med mulige veier videre i kapittel 8.

2 Introduksjon til langtidsplanlegging og SIMFOR-metoden

Hva som legges i begrepet *langtidsplanlegging* kan variere, men generelt er målet med militær langtidsplanlegging å sikre at nasjonen har tilstrekkelige styrker, utstyr, anlegg og kompetanse til å kunne utføre sine oppgaver i hele spekteret av mulige oppdrag.[13] Militær langtidsplanlegging er en tverrfaglig prosess som inkluderer mange ulike aktiviteter. Siden utvikling og investeringer i Forsvaret tar lang tid, er utfordringen å vite hva de fremtidige truslene, oppdragene og rammebetingelsene vil være. Eksempelvis må den planlagte styrkestrukturen være tilpasset de økonomiske midlene man har tilgjengelig. Når man planlegger langt frem i tid, ofte 10 til 30 år, vil det alltid være stor usikkerhet.

FFI har over mange år utviklet en metodikk som støtter Forsvarets og FDs langtidsplanlegging. Denne omtales ofte som «SIMFOR-metoden».[14] Metodikken er i utgangspunktet hentet fra analysemiljøer i Nato, som benytter liknende tilnærminger i Natos styrkeplanlegging[15]. Målet er å skape balanse over en lengre tidshorisont mellom oppgavene som militære styrker skal løse, sammensetningen til de militære styrkene, og kostnadene ved å ha slike militære styrker som kan operere på et gitt ambisjonsnivå. FFI har tilpasset metodikken til norske forhold og Norges forsvar, blant annet med tanke på at Norge har en mindre styrkestruktur og ser på trusselbildet fra et nasjonalt ståsted.

I essens forsøker metodikken å belyse tre sentrale forhold[16]:

1. Truslene som kan ramme Norge og som Forsvaret skal håndtere.

2. Ulike styrkestrukturer som Forsvaret kan benytte for å møte truslene.

3. Gapet mellom hva Forsvaret trenger og hva Forsvaret har, gitt punkt 1 og 2, og kostnader knyttet til ulike måter å tette dette gapet på.

Metodikken benytter en rekke teknikker for både å være mest mulig dekkende, og for å skape en klar rød tråd i resonnementene som etableres. Dette kapitlet går videre inn i metodikken og beskriver sentrale sider ved denne.

[13] Stojkovic, D.; Dahl, B. R. (2007); *Methodology for long term defence planning*; FFI-rapport 2007/00600.
[14] Navnet «SIMFOR» er knyttet til FFI-prosjektserien «Støtte til Forsvarsdepartementets langtidsplanlegging». I dagligtale skiller en ikke nødvendigvis mellom metode og metodikk slik vi gjør i denne rapporten.
[15] NATO Defence Planning Process; https://www.nato.int/cps/en/natohq/topics_49202.htm [sist besøkt 12.08.22]
[16] Vatne, D.F.;Køber, P.K.; Guttelvik, M.S.; Arnfinnsson, B.; Rise, Ø.R. (2020); Norwegian long-term defence analysis – a scenario- and capability-based approach; FFI-rapport 20/02367.

2.1 Sentrale komponenter

Sentralt i SIMFOR-metodikken står anvendelsen av scenarioer, oppgaver, kapabiliteter og strukturelementer. Disse er beskrevet nærmere under.

Scenarioer

Det er vanskelig å forutse om Norge vil bli angrepet eller på annen måte påvirket i den perioden man planlegger for, og hvordan dette eventuelt vil utarte seg. På grunn av denne usikkerheten har FFI fokus på å planlegge en fleksibel struktur som skal ha evnen til å løse et bredt spekter av utfordringer. Ved hjelp av morfologisk analyse[17] prøver SIMFOR-metodikken å spenne ut utfallsrommet av hvilke sikkerhetspolitiske utfordringer som kan ramme Norge. Dette utfallsrommet deles deretter inn i ulike scenarioklasser.

Med utgangspunkt i en scenarioklasse, brukes scenarioer for å konkretisere mer spesifikke situasjoner som kan oppstå. SIMFOR-metodikken kan trekke på en portefølje av detaljerte scenarioer utviklet med utgangspunkt i scenarioklassene, som beskriver ulike trusler som Norges styrkestruktur skal kunne møte.

Oppgaver

Når norske styrker skal stoppe, eller på andre måter håndtere, en trusselaktør i et scenario, må en beskrive på en strukturert måte hva styrkene skal gjøre. Dette blir gjort gjennom oppgave-beskrivelser. For et scenario vil identifisering og dekomponering av oppdrag og oppgaver synliggjøre hva norske styrker må kunne utføre i møte med en trusselaktør. Oppgavene holdes på et overordnet nivå, og alle scenarioer i en scenarioklasse vil typisk ha samme oppgave-dekomponering.[18]

Kapabiliteter

For å kunne vurdere om en gitt styrkestruktur kan møte og håndtere truslene som angis i et scenario, er det nødvendig å kunne sammenlikne kravene som stilles til styrkestrukturen og hva styrkestrukturen kan bidra med. I SIMFOR-metodikken benyttes kapabiliteter som et bindeledd mellom krav og bidrag. En kapabilitet kan defineres som evnen til å oppnå en effekt, og en kan fra et analyseperspektiv legge til grunn at militære styrker bruker kapabiliteter i deres oppgave-løsning. En oppgave får dermed et sett med kapabiliteter knyttet til seg, som kan brukes til kravsetting.

Hver kapabilitet er forholdsvis abstrakt, men målsatt med en referanseenhet. På denne måten er det mulig å vurdere kapasitet (hvor mye) i tillegg til kapabilitet (av hva). Kapabiliteter som ikke

[17] Se for eksempel Johansen, I.; *Scenarioklasser i Forsvarsstudie 2007: En morfologisk analyse av sikkerhetspolitiske utfordringer mot Norge*,FFI-rapport 2006/02664, og *Scenarioklasser for forsvarsplanlegging – revisjon av FFIs scenariogrunnlag*,FFI-rapport 21/01788.
[18] Se Hennum, A.F.; Glærum, S. (2007) *Metode for langtidsplanlegging – støtte til FS 07*; FFI-rapport 2007/02174; s. 13;.

kan måles i tilstrekkelig grad, blir ikke håndtert på en tilfredsstillende måte i SIMFOR-metodikken. Årsaken er at det blir vanskelig å finne ut om man har det man trenger av denne kapabiliteten. En liste over kapabiliteter for norske forhold med tilhørende beskrivelser er over tid blitt utviklet ved FFI, og listen vedlikeholdes jevnlig.[19] Kapabilitetene er i størst mulig grad beskrevet uavhengig av de faktiske styrkene og plattformene som Forsvaret har, slik at analysene kan være uavhengig av den eksisterende styrkestrukturen. Den kan derfor brukes til å identifisere mangler i denne.

Strukturelementer

Et strukturelement er en klart avgrenset del av en organisasjon bestående av personell, prosesser og systemer.[20] Eksempler på dette er Telemarkbataljonen, KNM Otto Sverdrup og 332-skvadronen.[21] Det er strukturelementene som faktisk anvendes i militære operasjoner for å oppnå gitte målsettinger, og det er strukturelementene som kostnadsberegnes. I SIMFOR-metodikken er strukturelementer både bestanddelene av en styrkestruktur, og referanseenheter for kapabilitetene. Dersom to strukturelementer har samme kapabilitet, vil dette synliggjøres ved at begge strukturelementene har tilordnet et forholdstall for kapabiliteten opp mot den bestemte referanseenheten. Hvilket strukturelement som fungerer som referanseenhet, kan sies å være noe tilfeldig.

Et strukturelement får dermed én eller flere evner (kapabiliteter) knyttet til seg med en viss kapasitet, angitt som forholdstall mot en referanseenhet. Dersom en styrkestruktur viser seg å ha flere strukturelementer med samme kapabilitet og tilstrekkelig kapasitet, vil et kapabilitetskrav fra et scenario i teorien kunne bli oppfylt enten ved å bruke det ene eller det andre struktur-elementet. Dette leder til et optimeringsproblem, om hvor og hvordan ulike strukturelementer best kan benyttes, med tanke på blant annet kostnader.

2.2 Logisk flyt

SIMFOR-metodikken presenteres gjerne som en metode bestående av et sett med analytiske steg angitt i en rekkefølge. Metoden deles gjerne i tre deler, hvor første del går på utledning av

[19] Køber, P.K.; Bjonge, V. (2021); *(U) Kapabiliteter, strukturelementer og kravsetting i langtidsplanleggingen ved FFI – oppdatert 2021*; FFI-eksternnotat 21/02205, [KONFIDENSIELT].
[20] Ref. https://www.fma.no/prinsix/maler/terminologi. Videre: «Strukturelementet utfører en identifiserbar del av verdikjeden (etterretning, kampstyrke, ildstøtte, logistikk) og kan brytes ned i et hierarki og bestå av underordnede strukturelementer. I realiteten snakker vi da om byggeklosser av organisasjonselementer (artillerienhet, luftvernenhet, fregatt, kampflyenhet) …». Tidlige beskrivelser av SIMFOR-metodikken presiserer forskjellen mellom generiske enheter (f.eks. mekanisert infanteribataljon, FN-fregatt, kampfly) og faktiske strukturelementer (KNM Otto Sverdrup, Telemarkbataljonen osv). Se Hennum, A. C. og Glærum, S. (2007) *Metode for langtidsplanlegging – støtte til FS 07*; FFI-rapport 2007/02174; s. 20.
[21] Hennum, A.F. og Glærum, S. (2007); *Metode for langtidsplanlegging – støtte til FS 07*; FFI-rapport 2007/02174; s. 20.

krav, den andre på kapabilitetsanalyse av styrkestrukturen, og den tredje på en gapsanalyse eller en mer generell syntese.[22] Disse tre delene består av flere steg.

Del 1 – Utledning av krav

Målet med denne delen er å ende opp med en liste over kapabilitetskrav som representerer hvor mye en norsk styrke trenger av forskjellige kapabiliteter for å kunne håndtere det som anses for å være dimensjonerende nasjonale trusselscenarioer. Kapabilitetskravene utledes gjennom å se på hvilke oppgaver som må løses i et eller flere scenarioer, og vurdere hvor mye som må være på plass av de forskjellige kapabilitetene for at oppgavene skal kunne løses på en tilfredsstillende måte.

Del 2 – Kapabilitetsanalyse av styrkestrukturen

Del 2 starter med at det bestemmes hva slags styrkestruktur som skal analyseres, for eksempel en nåværende struktur, en fremtidig struktur basert på eksisterende planer, eller en alternativ fremtidig struktur. Om nødvendig brytes strukturen ned i strukturelementer, og hvert strukturelement beskrives med dets kapabiliteter og kapasiteter opp mot de relevante referanseenhetene. Videre utledes krav som ikke følger direkte av scenarioet, men heller av strukturelementenes behov for ulike former for støttevirksomhet (eksempelvis beskyttelse, logistikk), for senere bruk i metoden. Deretter summeres kapabilitetene for hele styrkestrukturen slik at et helhetsbilde blir tilgjengelig. Samtidighetsproblematikk er en del av dette bildet.

Del 3 – Syntese og gapsanalyse

I del 3 tas resultatene fra de to foregående delene som utgangspunkt for å utlede kapabilitetsgap.

Den totale mengden krav som skal vurderes er summen av kapabilitetskrav fra del 1, og behov for støttevirksomhet fra del 2, på tvers av alle scenarioer. Alle krav skal imidlertid ikke nødvendigvis oppfylles samtidig. Det mest krevende settet med krav som styrkestrukturen skal oppfylle, vil enten være fra ett scenario som anses som mest utfordrende, eller en kombinasjon av krav fra utvalgte scenarioer hvor det er en ambisjon om at styrkestrukturen skal kunne håndtere disse samtidig. Dette kravsettet anses å være dimensjonerende for styrkestrukturen.

For en gitt kapabilitet vil ulike typer gap kunne oppstå:

- Dersom behovet for en kapabilitet ikke kan oppfylles av styrkestrukturen, har man et *styrkestrukturgap*. Dette kan skyldes at styrkestrukturen ikke har kapabiliteten i det hele tatt, eller har for lite kapasitet tilgjengelig. Manglende kapasitet kan skyldes at strukturen i utgangspunktet ikke har tilstrekkelig kapasitet, eller at de relevante strukturelementene benyttes til å løse andre, mer prioriterte oppgaver.

[22] Se for eksempel Glærum et al. (2008); *FFIs støtte til Forsvarssjefens Forsvarsstudie 2007*; FFI-rapport 2008/00606; s. 15, figur 3.1, og Vatne et al. (2020); *Norwegian long-term defence analysis – a scenario- and capability-based approach;* FFI-rapport 20/02367; s. 10, figur 1.1.

- Dersom forhold knyttet til tid og rom i et scenario tas med i betraktningene, kan mulige *klartidsgap* identifiseres. En kapabilitet kan i teorien være tilgjengelig, men geografisk forflytning og forberedelser for å gjøre strukturelementet klar til innsats medfører at det tar tid før kapabiliteten kan anvendes.

Det totale gapet for en kapabilitet er summen av styrkestrukturgap og klartidsgap. Dette kan beregnes individuelt for de ulike fasene i et scenario, sammenlagt for et scenario eller totalt for alle scenarioer. Videre kan kritikalitetsgraden på gapene vurderes samt overskytende kapasitet (redundans).

2.3 Den større sammenhengen

SIMFOR-metodikken brukes primært som et verktøy for å understøtte utarbeidelsen av langtidsplanen for forsvarssektoren (LTP). Denne planen er en fireårsplan som er styrende for utviklingen i forsvarssektoren.[23] Veien frem til en LTP går vanligvis via flere steg.[24] Forsvarssjefen utarbeider et militærfaglig råd til regjeringen, som etter behandling og beslutning legger frem en stortingsproposisjon. Denne behandles i Utenriks- og forsvarskomiteen, som kommer med sin innstilling før det endelige resultatet blir vedtatt av Stortinget.[25] Den vedtatte langtidsplanen er grunnlaget for mer detaljerte planer som strukturutviklingsplan (SUP), som operasjonaliserer ambisjoner, mål og krav og beskriver en planmessig utvikling av styrkestrukturen.[26] SIMFOR-metodikken vil typisk benyttes for å informere og understøtte Forsvarssjefens militærfaglige råd under utarbeidelsen.

SIMFOR-metodikken kan også benyttes på mer avgrensede problemstillinger knyttet til fremtidsscenarioer, styrkestrukturen og utvikling av Forsvaret. Dette inkluderer blant annet funksjonelle studier, hvor store deler av metodikken benyttes på en avgrenset del av styrkestrukturen og med et høyere detaljnivå. Det kan også inkludere analyser hvor ulike veivalg studeres i mer detalj. Slike analyser og arbeider kan fungere som underlag for de større SIMFOR-analysene.

2.4 Kjente usikkerhetsmomenter

Det er flere kjente usikkerhetsmomenter i SIMFOR-metodikken. Det er derfor viktig å være klar over hvor og hvorfor usikkerhet oppstår, og hva usikkerheten består av. Dette gjør det mulig å vurdere om usikkerheten er akseptabel slik den er, eller om en bør legge ned mer innsats for å

[23] Regjeringen; *Ny langtidsplan for forsvarssektoren (2021–2024).* https://www.regjeringen.no/no/tema/forsvar/ltp/LTP/id2611090/ [sist besøkt 29.06.22].
[24] Kämpe, M.K.M.*(2021); Langtidsplanen for Forsvaret – hva er det?* Folk og Forsvar. https://folkogforsvar.no/langtidsplanen-for-forsvaret-hva-er-det/ [sist besøkt 29.06.22].
[25] Ibid.
[26] Forsvarets Materiellanskaffelser; Forsvarsstrukturplanlegging, PRINSIX. ,https://www.fma.no/prinsix/Prosjektmodell/forsvarsstrukturplanlegging [sist besøkt 29.06.22].

forsøke å redusere den, dersom dette er mulig. I metodebeskrivelsen er en del usikkerhetsmomenter identifisert knyttet til analyse og setting av krav, som beskrevet i Vatne et al. (2021). Noen av disse mener vi er spesielt relevante for IKT.

Det første gjelder forståelsen for aktørenes mulige handlemåter i et scenario. Teknologiutviklingen og nye typer irregulære, ukonvensjonelle midler og nye måter å tenke på, muliggjør tidligere uforutsette handlemåter. Slike handlemåter gir både oss og de fiendtlige aktørene potensielt både nye muligheter og nye sårbarheter. Dette gjør det vanskelig å forutse hva trusselaktørene vil gjøre, og hvordan vi best vil kunne respondere.

Det vil også være usikkerhet vedrørende flere forhold knyttet til kapabilitetsvurderingene, hvor noen ligger litt i bakgrunnen av metodikken. Dette inkluderer definisjonene av selve kapabilitetene (har vi rett nivå og grad av detaljer?), kvantifisering av ytelse (klarer vi å sette gode tall på referanseenheter og strukturelementenes bidrag?), og kvantifisering av behov (fanger vi opp effektiviteten til styrkene korrekt, tapsrater, begrensninger som følge av geografi, vedlikehold, utholdenhet, og så videre?). Som vi kommer inn på i kapittel 4, kan dette være spesielt vanskelig for IKT.

I tillegg pekes det på at kvantifisering av enkelte kapabiliteter er særdeles utfordrende, som for eksempel for kommando og kontroll (K2) og cybertrusler. Gitt at cyberdomenet i prinsippet er uavhengighet av geografi, kan flere trusselaktører være aktive. Generalisering av trusler og kapabiliteter i cyberdomenet kan være meget vanskelig, gitt at cyberkapabiliteter tilpasses anvendelsen i en gitt militær operasjon. Sivil og militær infrastruktur overlapper, slik at sårbarheter kan ligge på utsiden av militær kontroll og Forsvarets ansvar. Et annet eksempel som nevnes er at det er vanskelig å vite når det kommer nyvinninger med store konsekvenser innen EK, for eksempel som radar i andre verdenskrig. Dette vil påvirke utnyttelsen av IKT-systemene.

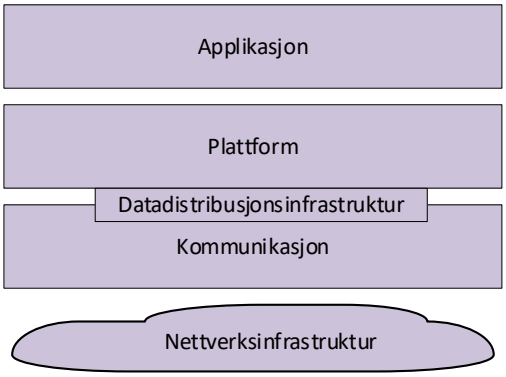
3 Hva er IKT?

IKT er et vidt begrep som kan tolkes på ulike måter. Store norske leksikon beskriver IKT som en «samlebetegnelse for teknologi for innhenting, overføring, bearbeiding, lagring og presentasjon av informasjon»[27]. Begrepet IKT-systemer brukes tilsvarende om ulike systemer som benyttes til dette. I Forsvarets fellesoperative doktrine (FFOD) brukes det beslektede begrepet *kommunikasjons- og informasjonssystemer* (CIS, Communications and Information Systems) som et fellesbegrep som omfatter materiell, metoder, prosedyrer og personell som er organisert for å oppnå informasjonsutveksling og -håndtering.[28]

IKT kan være et vanskelig fagfelt å forstå, og moderne IKT-systemer er ofte svært komplekse. I dette kapittelet beskrives kort hvordan IKT-systemer er bygd opp, og kompleksiteten som typisk karakteriserer slike systemer. I tillegg beskrives trender relatert til den teknologiske utviklingen, og Forsvarets anvendelse av IKT.

3.1 Hvordan IKT-systemer er bygd opp

Mange tenker på IKT som det fysiske utstyret og/eller applikasjonen som brukeren interagerer med, det vil si maskinvaren eller skjermen som brukeren forholder seg til, og den applikasjonen man bruker. Men dagens IKT er kompleks, og det er mye bakenforliggende teknologi som må fungere for at applikasjoner skal kunne brukes som tiltenkt. En måte å beskrive oppbyggingen av IKT på som er brukt tidligere ved FFI er vist i figur 3.1.



Figur 3.1 Enkel modell over funksjonalitet i et IKT-system. [29]

Sett fra brukeren leverer det øverste nivået applikasjonene som brukeren trenger. Dette kan være alt fra enkel telefoni til komplekse beslutningsstøtteverktøy. Plattformene består av maskinvaren

[27] Store norske leksikon; https://snl.no/informasjons-_og_kommunikasjonsteknologi#:~:text=Informasjons%2D%20og%20kommunikasjonsteknologi%2C%20samlebetegnelse%20for,lagring%20og%20presentasjon%20av%20informasjon. [sist besøkt 11.03.22].
[28] Forsvarets fellesoperative doktrine (2019), s. 228.
[29] Nystuen, K.O.; Farsund, B.H (2009)*; (U)Operativ evne og behovet for sikkerhetsegenskaper I INI – Metode og resultater*; FFI-rapport 2009/00646 [BEGRENSET].

og programvaren som skal til for å levere funksjonalitet til applikasjonene. Dersom plattformen består av flere datamaskiner i et større system, vil en ofte ha et datadistribusjonslag med overføring av informasjon internt innenfor plattformen. Kommunikasjonsnivået er den funksjonaliteten som hver plattform har tilgjengelig for å formidle informasjon mellom to eller flere brukere internt på plattformen, mens nettverksinfrastrukturen beskriver måten informasjonen formidles på i nettverket mellom lokasjoner uavhengig av plattform.

C3-taksonomien[30] er et annet eksempel på beskrivelse av den funksjonelle oppbygningen av IKT. Andre kjente modeller som retter seg mer mot kommunikasjonsdelen av IKT, er OSI-modellen[31] og DoD-modellen[32].

Det er imidlertid vanskelig å lage gode modeller av IKT-systemer. Dagens IKT-systemer og -infrastrukturer er svært komplekse, samtidig som de inngår i stadig lengre og mer komplekse verdikjeder.[33] Beskrivelsene er derfor en sterk forenkling av virkeligheten og bør sees på som en måte å strukturere og beskrive funksjonalitet på ulike lag som må eller kan inkluderes for at IKT-systemet skal fungere som tiltenkt.

3.2 Kompleksiteten i dagens IKT-systemer

Det er flere aspekter som er viktige for å forstå kompleksiteten knyttet til et IKT-system eller en IKT-infrastruktur. Disse aspektene er ikke uavhengig av hverandre og kan være delvis overlappende. Noen egenskaper ved systemene og infrastrukturene vil derfor passe inn i flere av aspektene. En måte å strukturere dette på, inspirert av arbeider gjort av Nancy Leveson[34] og Charles Perrow[35], er som følger[36]:

- Samspillkompleksitet beskriver ulike avhengigheter mellom og innad i de tekniske systemene:
    - Interne avhengigheter som kan betraktes som et sett med aktiviteter mellom elementer eller funksjoner i et system eller en infrastruktur.

[30] Consultation, Command and Control Board (C3B); C3 Taxonomy Baseline 5.0; 30. August 2021.
[31] Open System Interconnection model, se for eksempel https://www.networkworld.com/article/3239677/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html. [sist besøkt 08.07.22].
[32] Department of Defence model, se for eksempel https://petri.com/introduction-to-the-dod-tcpip-model/#:~:text=The%20TCP%2FIP%20model%2C%20sometimes,into%20the%20modern%20day%20Internet. [sist besøkt 08.04.2022].
[33] Telenor (2020); *Når nettene blir lange*; https://www.telenor.no/om/digital-sikkerhet/2020/artikler/nettene-blir-lange.jsp [sist besøkt 08.04.2022].
[34] Leveson, N. G. (2011): *Engineering a safer world*, The MIT Press.
[35] Perrow, C. (1984): *Normal Accidents: living with high-risk technologies*, Basic Books.
[36] Fasund, B. H.; Søndrol, T.; Nystuen, K. O.; Hornfelt, L. Sellevåg; S. R., Pham, V. (2022); *Utviklingen av nye IoT-baserte infratrukturer i samfunnet – utfordringer for nasjonal sikkerhet*; FFI-rapport 22/00631.

- Eksterne avhengigheter til andre (komplekse) systemer eller infrastrukturer, der man er avhengig av ressurser eller tjenester fra disse andre systemene eller infrastrukturene.

- Eksterne avhengigheter mellom systemer og infrastrukturer, fordi de trenger data fra hverandre.

- En form for eksterne avhengigheter mellom systemer eller infrastrukturer fordi de bruker samme maskinvare og/eller programvare. Et angrep som rettes mot ett av disse systemene eller infrastrukturene vil kunne ramme flere fordi de har de samme sårbarhetene.

- Koplingskompleksitet beskriver i hvilken grad koblingene mellom tekniske systemer og organisatoriske elementer er tidskritiske. Desto flere slike tidskritiske koblinger, desto høyere vil koblingskompleksiteten være.

- Verdikompleksitet beskriver hvordan et teknisk system eller et organisatorisk element bidrar oppover i verdikjeden. Verdi kan for eksempel være å medvirke til at et ledelseselement har et oppdatert og tilstrekkelig detaljert situasjonsbilde, eller at en styrke kan få kommunisert sin logistikkstatus. Hvis det er lett å holde oversikt over hvilke verdier infrastrukturen bidrar til, vil verdikompleksiteten være lav. Har man derimot liten oversikt over dette, fordi infrastrukturen for eksempel blir brukt av mange aktører, både indirekte og direkte, vil verdikompleksiteten være høy.

- Organisatorisk kompleksitet sier noe om hvordan avhengighetene er mellom de involverte organisasjonene, og mellom de involverte organisasjonene og de tekniske systemene. Det kan være mange involverte aktører for å levere en tjeneste. Det kan være private virksomheter, offentlige instanser og utenlandske virksomheter, og ofte en kombinasjon av disse. Det er i dag mange eksempler på at virksomheter splittes opp og/eller at deler av virksomheten tjenesteutsettes.

- Dynamisk kompleksitet beskriver hvordan tekniske systemer, organisatoriske elementer og koblinger endrer seg over tid. Disse endringene kan være knyttet til alt fra hvor ofte det skjer programvareoppdateringer, hvor ofte den fysiske infrastrukturen endres, hvor ofte det skjer endringer i hva infrastrukturen brukes til, til hvor ofte det skjer organisatoriske endringer, eksempelvis gjennom oppkjøp.

Utviklingen av IKT-systemer og -infrastrukturer, spesielt sivile, går mot at systemene og infrastrukturene blir stadig mer komplekse.[37]

[37] Telenor (2020); *Når nettene blir lange*; https://www.telenor.no/om/digital-sikkerhet/2020/artikler/nettene-blir-lange.jsp [sist besøkt 08.04.2022].

3.3 Trender knyttet til teknologiutviklingen

Det skjer i dag en enorm utvikling innen IKT-området. Utviklingen er så rask at den ofte omtales som den fjerde industrielle revolusjon[38]. Det er viktig at Forsvaret utnytter mulighetene som denne utviklingen gir.[39]

Det er mange måter å beskrive disse trendene på, og dette er gjort i rikt monn i litteraturen, se for eksempel arbeid fra Gartner[40] og NATO STO[41]. En måte vi kan sammenfatte trendene på er:

- Fremskritt innen kunstig intelligens (*AI – Artificial Intelligence*) og håndtering av stordata, sammen med stadig økende tilgang på data, gjør det nå mulig i større grad enn før å digitalisere og automatisere også avanserte analyser og andre prosesser som hittil har vært forbeholdt mennesker og manuell behandling. Et eksempel er hvordan dette i det sivile er tatt i bruk i beslutningsstøtte for medisinsk diagnose basert på bildegjenkjenning.[42]

- Den sivile utviklingen innen mikroprosessorer gir god tilgang på små, kraftige fleksible enheter som også kan brukes på taktisk nivå.[43] Tilgang til både data og prosesseringskraft gjennom skytjenester og kapable nettverk forsterker denne trenden.

- Mengden av enheter som gjøres autonome, det vil si at de er i stand til å utføre oppgavene sine uten menneskelig inngripen, øker stadig.[44] De mest etablerte løsningene er allerede i militær bruk i form av UAV-er/smådroner.[45]

- Teknologiene bak utvidet virkelighet (*augmented reality*) har vært under utvikling lenge (siden 1990-tallet), men har så langt ikke funnet sitt endelige gjennombrudd i ordinær bruk. Utviklingen har imidlertid pågått jevnt og trutt, og det forventes at teknologiene i løpet av de neste fem årene er modne for mer utstrakt bruk, også militært.[46]

- Utbygging av 5G innebærer mye mer enn kun bedre mobiltelefoni. 5G innebærer også at brukeren skal kunne utnytte et stort antall forskjellige tilknytningsformer for å holde seg «online». Felles styringssystemer for kommunikasjonsinfrastrukturer sammen med

[38] Se for eksempel: World Ecnomic Forum, *Fourth Industrial Revolution*, https://www.weforum.org/focus/fourth-industrial-revolution [sist besøkt 27.06.22].
[39] Bentstuen, O.I. (2022); *Trender innen IKT – relatert til militærmakt*; FFI-rapport 22/00544.
[40] Gartner (2022): *Top Strategic Technology Trends 2022.*
[41] NATO STO (2020): *Science & Technology Trends 2020 – 2040.*
[42] Oren, O.; Gersh, B.J.; Bhatt, D.L. (2020): *Artificial intelligence In medical imaging: switching from radiographic pathological data to clinically meaningful endpoints*; The Lancet.
[43] Tortonesi et al. (2016): *Leveraging Internet of Things within the military network environment—Challenges and solutions*; IEEE 3rd World Forum on Internet of Things (WF-IoT); s. 111–116.
[44] Philip (2019): *Autonomous Devices Are Here. Are You Ready? https://www.bridge-global.com/blog/autonomous-devices-are-here-are-you-ready/* [Sist besøkt 04.07.22].
[45] Bender (2016): This chart shows just how massive America's drone fleet is; https://www.businessinsider.com/chart-of-us-drone-fleet-2016-3 [Sist besøkt 04.07.22].
[46] Spiegel (2021): *The Fundamentals of AR and VR – and how the Military Is Using Them*; https://www.designnews.com/automation/fundamentals-ar-and-vr-and-how-military-using-them [Sist besøkt 04.07.22].

ny 5G-radio og massive satellittsystemer vil tilby kommunikasjonstjenester uavhengig av lokasjon.[47]

3.4 IKT som integrator i Forsvaret

Tidligere var det vanlig å betrakte IKT kun som et støttesystem[48], det vil si noe som ble brukt til å støtte opp om de andre strukturelementene, på linje med for eksempel drivstoff- og mat-forsyningssystemer. Det vil si at IKT-systemer sørger for at strukturelementene i Forsvaret fungerer hver for seg. IKT-systemer brukes fremdeles som støttesystem, men utviklingen går nå mot at IKT i stadig større grad inngår som en integrator. Da fungerer strukturelementene ikke bare hver for seg, men sammen. Det vil si at båndene mellom IKT-systemene og den militære virksomheten ofte er så tette og sammenvevde, at det blir mer korrekt å omtale IKT som integrert med militær virksomhet fremfor kun støttende og dermed separat. IKT blir for eksempel brukt ved opparbeidelse av situasjonsbilde, i beslutningsprosessen, ved ordregiving, klargjøring av materiell, utførelse av militære operasjoner og rapportering.

Det er ikke bare de brukernære IKT-systemene som kan betraktes som integrator i Forsvaret. Det er også mye IKT som er integrert i de ulike plattformene, samt bakenforliggende IKT-systemer som er nødvendige.

[47] Bentstuen (2019): *Trender som påvirker Forsvarets kommunikasjonsinfrastruktur;* FFI-fakta.
[48] Støttesystem: Alle anlegg, materiell, programvare, tjenester og personellressurser utenom selve materiellsystemet som er nødvendig for operativ bruk og støtte av materiellsystemet, slik at det kan betraktes som en selvforsynt enhet i sitt tiltenkte brukermiljø (Forsvarets Prinsix Terminologi; https://www.fma.no/prinsix/maler/terminologi [Sist besøkt 18.03.22]).

4 Utfordringer ved inkludering av IKT i langtidsplanlegging

De tradisjonelle strukturelementene i Forsvaret som ubåter, luftvern og overvåkningsfly, har man hatt i mange årtier. Dette har gjort det mulig å opparbeide mye erfaring med hvordan ulike vurderinger best kan gjøres, for eksempel vurdering av operativ nytte og risiko. Selv om også disse strukturelementene har gjennomgått en teknologisk utvikling har hovedfunksjonaliteten ligget fast. Basert på dette er det derfor mulig å si noe om behovet for disse strukturelementene ved ulike handlemåter i ulike scenarioer.

Selv om IKT også har blitt brukt lenge, er det svært vanskelig å avgrense IKT til å være ett eller et mindre sett med klart definerte og avgrensede strukturelementer som kan behandles som dette i en analyse. Dette skyldes blant annet den tette integrasjonen av IKT i de tradisjonelle strukturelementene og egenskaper ved IKT som gir høy kompleksitet.[49] Disse egenskapene gjør det vanskelig å gjøre slike vurderinger for IKT, og dermed inkludere disse teknologiene i Forsvarets langtidsplanlegging. I det følgende blir noen av disse utfordringene beskrevet.

4.1 Hvilket tidsperspektiv skal benyttes?

Vanligvis ser man 10–30 år frem i tid ved langtidsplanlegging. Dette er håndterbart for strukturelementer med lange levetider som kampfly, stridsvogner og skip. På grunn av den raske teknologiutviklingen vil det være vanskelig å kunne si noe detaljert om IKT så langt frem i tid, selv om en del grunnleggende behov for IKT trolig vil være mer konstante. Usikkerheten knyttet til hvordan dette teknologiområdet vil utvikle seg er for stor. Her er det også den sivile industrien og den sivile anvendelsen som er drivende. Dette gjør det spesielt vanskelig å si noe om retningen innen militær IKT. Det vil derfor være nødvendig å vektlegge kortere tidsperspektiver når man planlegger innen IKT-området.

4.2 Hvilken IKT fokuserer vi på?

IKT er mer abstrakt enn de fleste strukturelementer, og kan være en svært kompleks materie å analysere. Dette krever en bevisst holdning til hva man velger å legge i begreper og hvordan man avgrenser og konkretiserer dem i tråd med målsettingene for arbeidet. Det er en generell utfordring å finne egnede måter å gjøre dette på.

Det er flere forhold å ta hensyn til. Det første er å definere hva vi mener med IKT, det vil si å bestemme hvilke teknologier vi ønsker å ha med i våre analyser. Noen tilfeldige eksempler på

[49] Det er ikke helt umulig å definere utvalgte «IKT-strukturelementer», slik som det i praksis gjøres i dagens langtidsplanlegging. Men disse har en rekke ulemper og svakheter (se kapittel 5.1 og 5.2). Vår tilnærming bruker ikke slike strukturelementer.

forskjellig IKT er IoT[50], SCADA/ICS[51], OT[52], kommunikasjonsinfrastruktur, kjernenett, integrert IKT og *embedded devices*. Det neste problemet er hvordan vi klassifiserer, kategoriserer eller videre bryter ned den teknologien vi velger å fokusere på. Det er ikke intuitivt hva som vil være den beste kategoriseringen, og dette vil være avhengig av hensikten med arbeidet. En modell som ofte benyttes i Forsvaret er C3-taksonomien.[53]

Det må imidlertid også gjøres andre avgrensninger, og her er det flere aspekter å ta hensyn til. Det første går ut på hvor det er hensiktsmessig å sette grenser når IKT-systemer er sammenkoblede og har avhengigheter mellom seg. Spørsmålet er viktig når man for eksempel skal vurdere operative konsekvenser av et angrep på et IKT-system, og implikasjonene av at følgekonsekvenser kan forplante seg fra et system til et annet. Hvor langt i slike kjeder man skal følge etter eller spore opp mulige følgekonsekvenser må avgjøres. Dette er et svært relevant spørsmål når man for eksempel analyserer endringer i IKT-systemer for å få innsikt i hvordan dette påvirker den operative evnen.

Et annet aspekt er mer relatert til Forsvarets virksomhet og bruken av IKT. Skal vi se på all IKT som Forsvaret bruker, eller forsøker vi å avgrense til kun IKT som brukes i militære operasjoner? Her er det rollen til IKT-systemene som står i fokus. Er det for eksempel hensiktsmessig å inkludere kontormaskinene til ansatte i FD når vi studerer IKT-systemenes understøttelse av en militær operasjon?

I begge disse aspektene knyttet til avgrensninger av IKT dukker også spørsmålet om inkludering av tjenester og systemer som er utenfor Forsvarets direkte eie opp, eksempelvis innleide tjenester og leide linjer i form av overføringskapasitet. Dette er også et aspekt som krever at man gjør noen bevisste valg.

Noe av årsaken til at det er vanskelig å lage en oversikt over de IKT-systemene som er i bruk i Forsvaret i dag, er utfordringene med å definere, klassifisere og avgrense disse IKT-systemene. Dette er også et problem i langtidsplanleggingen, da det er nødvendig å vurdere hvilke IKT-systemer man skal ha med i analysen, og hvordan disse henger sammen.

4.3 Hva er fordelene ved å bruke IKT?

Mye av utfordringen knyttet til å integrere IKT i langtidsplanleggingen i Forsvaret, ligger i å finne gode og dekkende måter å fange opp hvordan IKT-systemer gir økt operativ evne. Grunnen til at vi investerer i og tar i bruk IKT, ligger intuitivt i at IKT-systemer hjelper oss med å gjøre det vi skal, og at fravær av slike systemer gjør jobben vår vanskeligere, og i enkelte tilfeller helt umulig. Men å måle eller beskrive hvordan denne nytten oppstår, og hvordan og i hvilken grad den hjelper oss med å gjøre våre oppgaver mer effektivt, er vanskelig.

[50] Internet of Things
[51] Supervisory control and data acquisition / Industrial Control Systems
[52] Operational technology
[53] Consultation, Command and Control Board (C3B); C3 Taxonomy Baseline 5.0; 30. August 2021.

Hvis man ser på IKT-systemer som personellet bruker direkte i en operasjon, så kan en argumentere for at anvendelsen er nært koblet til OODA-løkka[54], da IKT kan gi oss bedre og flere sensorer (*Observe*), bedre muligheter til å distribuere og tolke data (*Orient*), mulighet til å ta bedre beslutninger, for eksempel ved bruk av kunstig intelligens (*Decide*) og flere handlingsmuligheter (*Act*). IKT kan dermed gi oss OODA-løkker som både er raskere og gir høyere måloppnåelse. Begge deler gir bedre operativ evne. Det kan imidlertid være vanskelig å vurdere en eventuell økt måloppnåelse.

Den økte operative evnen en investering i IKT eventuelt gir, vil være avhengig av i hvilken grad personellet på alle nivåer i organisasjonen klarer å utnytte potensialet som ligger i teknologien. Her er kunnskap, opplæring og trening av personellet viktig. I tillegg kan nye IKT-systemer muliggjøre helt nye handlemåter. Her kan det oppstå ulineære sammenhenger, det vil si at den operative evnen kan øke betraktelig hvis IKT-systemene muliggjør helt nye og fordelaktige handlemåter.

Til sammen gjør dette det utfordrende å vurdere den operative nytten til ulike IKT-alternativer, også dersom man ønsker å vurdere disse opp mot hverandre.

4.4 Hva er risikoen ved å bruke IKT?

Å gjøre seg avhengig av IKT kan medføre en stor risiko, både når det gjelder utilsiktede hendelser og tilsiktede uønskede handlinger.

Den mest vanlige måten å vurdere risiko for utilsiktede hendelser på er å vurdere risikoen som produktet av sannsynligheten for slike hendelser og konsekvensen av disse, slik som blant annet beskrevet i NS 5814[55]. For å kunne si noe om sannsynlighet bør man ha en viss historikk over et tilsvarende system over en viss tid, bygd opp og brukt på samme måte og i samme omgivelser. Dette er utfordrende siden moderne IKT-systemer er komplekse og i stadig endring, og siden det er vanskelig i fredstid å få et bilde på realistisk bruk i for eksempel konflikt og krig. Bruken vil variere fra operasjon til operasjon og fra situasjon til situasjon, og det vil derfor være utfordrende å ha oversikt over hva systemene faktisk brukes til. Dette gjør det vanskelig å forstå hvilke konsekvenser en degradering av IKT-systemene vil få. I tillegg kan feil forplante seg videre til nye systemer, siden IKT-systemer har mange avhengigheter. På denne måten kan en hendelse eskalere. Dette kan skje på måter det kan være vanskelig å forutsi på forhånd. Her kan det oppstå ulineære sammenhenger.

Det som imidlertid er mest relevant for IKT-systemer i en konflikt er risikoen for tilsiktede uønskede handlinger. For slike handlinger er det vanlig å bruke risikotrekanten beskrevet i NS 5832[56], hvor risikoen vurderes ut fra faktorene verdi, sårbarhet og trussel. Verdivurderingen er nært knyttet opp mot konsekvenser, og vil ha de samme utfordringene som konsekvens-

[54] OODA: Observe Orient Decide Act, se for eksempel Richards, C. (2020); Boyd's OODA loop; Necesse, vol 5, nr 1.
[55] Norsk Standard 5814 (2008); *Krav til risikovurdering.*
[56] Norsk Standard 5832 (2014); *Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse.*

vurderingene over. I tillegg er det vanskelig å ha oversikt over systemene som brukes, og hvilke sårbarheter disse har. Dette er mye på grunn av kompleksitet og usikkerhet. I tillegg overlapper sivil og militær digital infrastruktur, noe som gir sårbarheter utenfor Forsvarets kontroll.

Trusselbildet knyttet til IKT er det også vanskelig å ha grep om,[57] og dette kan dessuten endres raskt. Evnen til å utføre Cyber- og EK-angrep varierer hos ulike trusselaktører, samtidig som det kan være vanskelig å forutsi hva slags verktøykasse motstanderen sitter med på forhånd, for eksempel i hvilken grad det er gjort forberedelser i våre nettverk.

Alt i alt vil en slik risikovurdering inneholde mye usikkerhet. Det er imidlertid viktig å beskrive denne usikkerheten som bidrar til økt risiko.

I langtidsplanleggingen er det viktig å kunne vurdere ulike strukturalternativer for IKT opp mot hverandre. Disse vurderingene bør inkludere betraktninger rundt risikoen ved de ulike alternativene.

4.5 Hva er IKT-behovet og hvordan dekkes dette?

Det kan være vanskelig å vurdere hva behovet for IKT vil være i et scenario. Som regel kreves det veldig detaljerte scenarioer for å kunne si noe om dette.

I tillegg kan det være vanskelig å vurdere hva ny teknologi kan bidra med. Utviklingen går som tidligere nevnt svært fort. Moderne teknologi som skytjenester, 5G, stordata og AI gir så mange nye muligheter at det er vanskelig å bedømme rekkevidden av hva dette egentlig kan løse, og hvordan det kan utnyttes på en best mulig måte.[58] Som nevnt tidligere kan IKT noen ganger bidra til at man kan gjøre oppgavene på helt nye måter. Dette kan det være vanskelig å se for operativt personell når de er opplært til å utføre sine oppgaver på bestemte måter.

Det kan også være utfordrende å utvikle helhetlige og gode strukturalternativer som skal dekke et behov. Dette er det flere årsaker til. Det kan være vanskelig å vurdere det totale mulighetsrommet som ny teknologi gir. Samtidig er det ofte mange mulige måter å realisere behovet på. Hvilke former for kommunikasjon man skal bruke, hvor servere skal ligge samt hvorvidt man skal leie, inngå partnerskap eller at Forsvaret skal sørge for dette selv er alle avveiinger som må gjøres. I tillegg bør hvert enkelt behov sees i sammenheng med andre IKT-behov som Forsvaret har, og også med tanke på hvordan IKT-området vil utvikle seg fremover. Det er en fordel å velge løsninger som gjør det enkelt for Forsvaret å følge utviklingen videre.

[57] Se for eksempel Farsund, B.H.; Enemo, G (2018); *En morfologisk analyse av tilsiktede uønskede handlinger rettet mot Forsvarets informasjonsinfrastruktur*; FFI-rapport 18/00466.[58] Se for eksempel Voldhaug, J.E.; Hansen, B.J.; Lund, K.; Mykkeltveit, A.; Rytir, M.; Bentstuen, O.I. (2021); *Hvordan kan ny IKT gjøre Forsvaret bedre?*; FFI-rapport 21/01819.

[58] Se for eksempel Voldhaug, J.E.; Hansen, B.J.; Lund, K.; Mykkeltveit, A.; Rytir, M.; Bentstuen, O.I. (2021); *Hvordan kan ny IKT gjøre Forsvaret bedre?*; FFI-rapport 21/01819.

4.6 Hva koster IKT?

Det er forskjell på å beregne kostnaden av IKT som allerede er innført i en organisasjon, og kostnadene relatert til nye IKT-systemer som potensielt skal innføres. Utfordringene med å beregne kostnader på IKT som allerede er i bruk i Forsvaret, er beskrevet i en tidligere studie ved FFI.[59]

Innkjøp av IKT-systemer er kompliserte prosesser. Systemene er ofte ikke ferdig utviklet når de bestilles, ei heller når de tas i bruk. I dag er det vanlig at funksjonaliteten utvikles kontinuerlig. Dette gjør det vanskelig å kostnadsberegne slike systemer, men også å vite hva slags funksjonalitet man faktisk ender opp med.

Det er flere eksempler på at statlige IKT-investeringer ikke har gått som planlagt, hverken når det gjelder funksjonaliteten til produktet eller kostnadene.[60,61] Det kan også være svært kostbart å komme seg ut av slike kontrakter og alternativet er ofte å starte helt på nytt med andre leverandører. I praksis blir man derfor ofte låst til leverandøren.

[59] Arnfinnsson, B; Elman, E; Eriksen, S. H. (2020); *Hvor mye bruker forsvassektoren på IKT?;* FFI-rapport 20/00806 [BEGRENSET].

[60] I 2020 valgte politidirektoratet å stanse prosjektet «Omnia» etter store forsinkelser og en kostnadssprekk i millionklassen, selv om systemet ikke var klart til bruk. Jakobsen, H. Ø (2020).; *Slik ble politiets «supervåpen» en 100-millioners fiasko;* Morgenbladet nr. 47 årgang 202.

[61] Helse Sør-Øst sitt nye felles laboratoriedatasystem for medisinsk biokjemi, mikrobiologi, patologi og blodbank ble tatt i bruk i 2015, og i dag varsler leger fremdeles om et tungrodd system med så mange feil og mangler at pasienter kan ende opp med å få uriktige diagnoser. Systemet har kostet en milliard kroner, og dette er minst 200 millioner mer enn planlagt. Einan, T. S.; Drønen, O. (2022); *Slår alarm: Nytt datasystem kan gi pasienter feil diagnose*; Morgenbladet nr 13, årgang 203.

5 IKT i dagens langtidsplanlegging

I nåværende versjon av SIMFOR-metodikken er IKT delvis integrert ved at fem IKT-kapabiliteter med referanseenheter er definert. De behandles på lik linje med alle andre definerte kapabiliteter, inklusive utledning av behov ved vurderinger av rød trussel og blå respons i valgt scenario. IKT-kapabilitetene omhandler elektronisk kommunikasjon, og det identifiserte kommunikasjonsbehovet i et gitt scenario er grunnlaget for kravene til kapabilitetene.

5.1 Representasjon ved IKT-kapabiliteter

De fem IKT-kapabilitetene[62] er:

- *Støtte-felles-kommunikasjon, operasjonelt*. Omfatter evne til å opprettholde sikker og robust kommunikasjon 1) innbyrdes mellom mobile brukere og 2) mellom stasjonære og mobile brukere, i eller nært knyttet til, operasjonsområdet under et lavt til moderat trusselnivå. Evnen omfatter kapasitetskrevende tjenester og tjenester med strenge krav til ytelse. Referanseenhet: «UAV med 100 km dekningsradius».

- *Støtte-felles-kommunikasjon, operasjonelt, høy trussel*. Omfatter evne til å opprettholde sikker og robust kommunikasjon 1) innbyrdes mellom mobile brukere og 2) mellom stasjonære og mobile brukere i eller nært knyttet til operasjonsområdet under et høyt trusselnivå, det vil si med økt risiko for oppdagelse og tjenestenekt. Dette inkluderer kommunikasjon til enheter på dypet. Evnen omfatter kapasitetskrevende tjenester og tjenester med strenge krav til ytelse. Referanseenhet: «UAV med 100 km dekningsradius, EPM[63]-bølgeform, LPD[64]-bølgeform».

- *Støtte-felles-kommunikasjon-sivilt*. Omfatter evne til å etablere kommunikasjon mellom militære og sivile brukere, i eller nært knyttet til, operasjonsområdet under et lavt til moderat trusselnivå. Referanseenhet: «dagens nødnett TETRA».

- *Støtte-felles-kommunikasjon-strategisk*. Omfatter evne til å opprettholde sikker og robust kommunikasjon mellom stasjonære brukere eller datasentre spredt utover hele landet og under et lavt til moderat trusselnivå. Evnen omfatter både overføring av store datamengder på kort tid og kapasitetskrevende tjenester. Referanseenhet: «dagens permanente stasjonære FKI[65] (kjernenett + aksessnett)».

- *Støtte-felles-kommunikasjon-strategisk, høy trussel*. Omfatter evne til å opprettholde sikker og robust kommunikasjon mellom stasjonære brukere eller datasentre spredt utover hele landet under et høyt trusselnivå, det vil si ved økt risiko for tjenestenekt.

[62] Køber, P. K.; Arnfinnsson, B. (2020); (U) Kapabiliteter, strukturelementer og kravsetting i langtidsplanleggingen ved FFI – oppdatert 2019; FFI-notat 20/00145; [KONFIDENSIELT].
[63] Electronic Protection Measures.
[64] Low Probability of Detection.
[65] Forsvarets kommunikasjonsinfrastruktur.

Evnen omfatter både overføring av store datamengder på kort tid og kapasitetskrevende tjenester. Referanseenhet: «geostasjonær satellittkommunikasjon (SATKOM) med EPM-bølgeform».

Ved å sette krav til disse kapabilitetene i et gitt scenario vil noe av behovet for den type IKT som er angitt gjennom referanseenhetene bli synliggjort.

5.2 Ulemper og svakheter

Denne tilnærmingen har imidlertid flere ulemper og svakheter. For det første synliggjør den ikke behovet som oppstår som en konsekvens av at de andre kapabilitetene og struktur-elementene Forsvaret benytter er avhengige av IKT for å operere som tiltenkt. Dette er et indirekte IKT-behov, som ikke blir belyst med mindre analytikerne tilfeldigvis har ekstra kunnskap om dette. IKT-kapabilitetene er sidestilte med de andre kapabilitetene, og behandles dermed i prinsippet uavhengig av disse i en analyse. Dette gjør at de samlede, reelle behovene for eksempelvis FKI er større enn det som fremkommer gjennom kravet for den tilhørende kapabiliteten (i dette tilfellet «støtte-felles-kommunikasjon-strategisk»).

For det andre er det en svakhet at IKT-behovet er større enn det som fanges opp gjennom disse IKT-kapabilitetene. Dette gjelder spesielt med tanke på plattformer og applikasjoner. Behov for IKT utenom behovet for de gitte typene elektronisk kommunikasjon blir i dag ikke synliggjort i det hele tatt.

For det tredje er flere av referanseenhetene enten uklare på hva som måles, eller ikke målbare. Hva er for eksempel én, to eller tre «dagens nødnett TETRA»? En slik referanseenhet er ikke velfungerende med tanke på å kunne angi mengden av noe. Snakker man for eksempel om å øke geografisk utbredelse, eller datakapasiteten, hvis vi øker antallet? Paradoksalt skjuler denne uklarheten at ulempen om manglende synliggjøring av indirekte IKT-behov eksisterer: dersom det eneste kravet som kan settes for eksempel er «ett stykk FKI», og vi har én FKI, så vil aldri spørsmålet om hva slags behov de andre strukturelementene har for FKI dukke opp. Problemer knyttet til målbarhet blir spesielt vanskelige med applikasjoner og plattformer. Hva skal måles med tanke på ytelsen til et K2-system?

Strengt tatt burde kapabilitetene også kunne kobles opp mot operativ evne. Som vi var inne på i kapittel 4.3, er dette en utfordring for IKT.

Å definere flere uavhengige IKT-kapabiliteter i jakten på bedre dekning av IKT i SIMFOR-metodikken, ville i teorien kunne løse utfordringen knyttet til å adressere mer av IKT-behovet enn bare det som går på elektronisk kommunikasjon. Det er imidlertid uklart hvor mange IKT-kapabiliteter som ville vært nødvendig, om en tilstrekkelig dekningsgrad i det hele tatt hadde vært mulig på denne måten, og hvordan en skulle kunne vurdere at tilstrekkelig dekningsgrad faktisk var oppnådd. Gitt dette og de andre ulempene, især manglende synliggjøring av indirekte IKT-behov, ansees det lite hensiktsmessig å utvikle denne tilnærmingen videre på det nivået man trenger ved langtidsplanlegging.

6 Vår metode for å inkludere IKT i langtidsplanleggingen

Dagens integrasjon av IKT i SIMFOR-metodikken er innrettet slik at Forsvarets IKT-behov i begrenset grad kommer til syne i analysene. Operativ nytte og risiko knyttet til IKT er i stor grad utelatt og overlatt til fageksperter å diskutere på eget initiativ. Unntaket er de fem IKT-kapabilitetene, som dekker deler av behovet for elektronisk kommunikasjon. I realiteten er behovet for elektronisk kommunikasjon større enn det som synliggjøres på denne måten, og det er behov for andre typer IKT som ikke blir fanget opp.

Hensikten med metoden vi har utviklet er å få et bedre grep på IKT-behovet som ikke er synliggjort i dag. Fremfor å etablere og legge til flere IKT-kapabiliteter, har vi utviklet en løsning som lar oss studere hvor viktig IKT er for et tradisjonelt strukturelement uten å definere «IKT-strukturelementer». Etter vår vurdering åpner dette opp for bedre vurderinger rundt operativ nytte, behov og risiko ved bruk av IKT. Samtidig er det viktig å slå fast at når kompleksiteten på IKT-systemene er høy og IKT-anvendelsen omfattende, er det generelt meget utfordrende å gjøre slike vurderinger. Også på utsiden av langtidsplanleggingen er dette kjente problemstillinger som ikke er tilfredsstillende løst. Metoden løser ikke disse utfordringene på en automatisk måte, men skaper en struktur som kan være til støtte for analytikere.

I vår metode avgrenser vi oss til å se på strukturelementenes anvendelse av IKT, og hvordan endringer i anvendte IKT-systemer påvirker strukturelementenes kapasiteter positivt eller negativt. Dette gjør det mulig å vurdere konsekvensene for strukturelementet ved angrep på dets IKT-systemer, samt studere hvordan behov for flere kapabiliteter eller mer kapasitet potensielt kan realiseres ved å investere i mer og/eller nye og bedre IKT-systemer.

I dette kapitlet går vi først igjennom ulike anvendelser et strukturelement kan ha av IKT, og hvordan anvendelsen av IKT kan brukes i vurderinger av kapasiteter. Deretter viser vi hvordan disse vurderingene kan knyttes til SIMFOR-metodikken og andre liknende metodikker. Videre beskriver vi hvordan vår metode dekker noen av utfordringene vi beskrev i kapittel 4, samt hvilke andre fordeler og ulemper denne metoden har. Til slutt beskriver vi hvordan disse vurderingene gjøres i praksis.

6.1 Et strukturelements ulike anvendelser av IKT

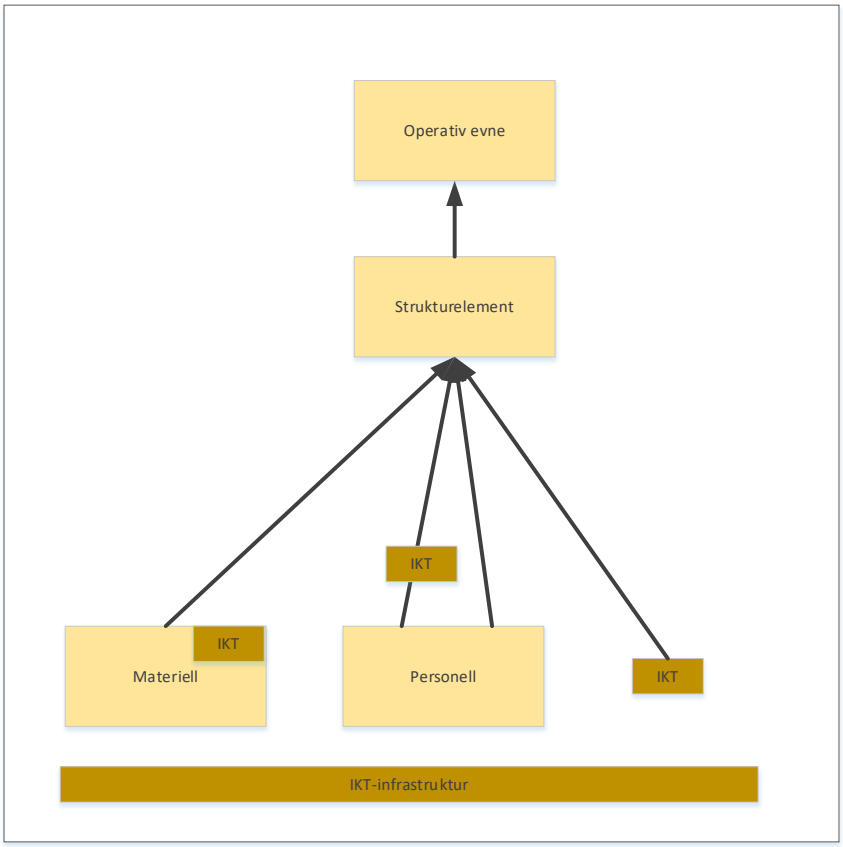
I vårt arbeid har vi fokusert på IKT-anvendelser for å forstå hvor viktig IKT er. Vi har som utgangspunkt at et strukturelement vil anvende IKT-systemer på ulike måter i sitt virke, og at denne anvendelsen bidrar til strukturelementets kapasiteter. Vi utnytter her IKT-systemenes egenskap av å være en integrator eller støttefunksjon for strukturelementene, og at degradering av IKT-systemene generelt vil ha som konsekvens at kapasiteten senkes og tilføring av mer og/eller ny og bedre IKT at kapasiteten økes. Dette hjelper oss med å kunne si noe om den operative evnen IKT bidrar til, både med tanke på positiv og negativ endring.

Som beskrevet i kapittel 4.2, er avgrensing av IKT en eksersis i seg selv som må tilpasses analyseformålet. Her mener vi analysene i prinsippet bør inkludere de IKT-systemene som understøtter eller er integrert i et strukturelement når strukturelementet skal levere kapasiteter inn i en operasjon. Hvilke IKT-systemer dette omfatter vil variere fra strukturelement til strukturelement, og det vil være utfordrende å identifisere og kategorisere IKT-systemene i forkant på en god måte for alle strukturelementene. For å komme videre har vi i vår metode valgt å gjøre en prinsipiell grovinndeling av IKT-systemene et strukturelement kan anvende. Denne inndelingen lar oss trekke noen grenser mellom IKT-systemene vi velger å analysere, og dem vi utelater i våre analyser. Inndelingen må sees på som en forenkling og bør raffineres ved videre bruk av metoden. Det er også mulig å bruke andre inndelinger. Inndelingen er som følger, se figur 6.1:

- Et strukturelement kan bestå av ulike former for forsvarsmateriell som kjøretøy, farkoster, våpensystemer og lignende. Her vil det ofte være innebygget IKT, for eksempel IKT-systemer som stabiliserer kjøretøy eller beregner skytedata til kanoner. Enkelte av disse systemene opererer helt uten interaksjon med personellet, mens andre har noen former for interaksjon for å gi kommandoer eller sette valgmuligheter. Vi inkluderer også her IKT som gjør at ulike komponenter av strukturelementet får kommunisert seg imellom, for eksempel i et luftvernsystem. En fellesnevner er at forsvarsmateriellet er laget for å ha operatører og at IKT-systemene er en integrert del av materiellet ved innkjøp (angitt til venstre i figuren).

- Et strukturelement består også som regel av personell. Disse bruker ofte mer personlig IKT-utstyr for å utføre enkelte av sine oppgaver. Her tenker vi på IKT-systemer i form av mer standardisert utstyr som PC-er med applikasjoner og mobiltelefoner. Denne formen for IKT kan for eksempel brukes til å vise informasjon i forbindelse med planlegging, å gi ordre eller rapportere. Vi inkluderer også her IKT-systemer som personellet direkte interagerer med for å kommunisere internt i strukturelementet eller med andre strukturelementer, for eksempel radioer (angitt i midten av figuren).

- Et strukturelement kan også bestå av enheter som opptrer mer selvgående. Her regner vi semi-autonome og fullstendig autonome enheter som roboter og UAV-er. Dette er enheter som på et tidspunkt opererer, herunder forflytter seg og tar beslutninger, med lite eller helt uten menneskelig interaksjon. Muligheten for å kommunisere med enheten og å gi ytterligere kommandoer underveis kan være tilstede i varierende grad (angitt til høyre i figuren).



Figur 6.1 Ulike måter et strukturelement kan anvende IKT på.

I tillegg til disse tre kategoriene definerer vi også IKT-systemer som brukes av ovennevnte IKT-systemer, herunder kommunikasjonssystemer og -infrastruktur som muliggjør kommunikasjon ut av et strukturelement. Dette er IKT-systemer som ikke direkte brukes av personell eller materiell, men som indirekte blir anvendt når personellet eller materiellet bruker IKT-systemene.[66]

6.2 Etablering av en argumentasjonskjede fra et strukturelements anvendelse av IKT til dets kapasiteter

Hvordan den egentlige årsakskjeden ser ut, fra et strukturelements anvendelse av IKT til operativ effekt, kan være meget vanskelig å finne ut av. Kombinasjonen av kompleksitet, potensielt høy dynamikk og mangel på et komplett teoretisk fundament som kan trekke tråden

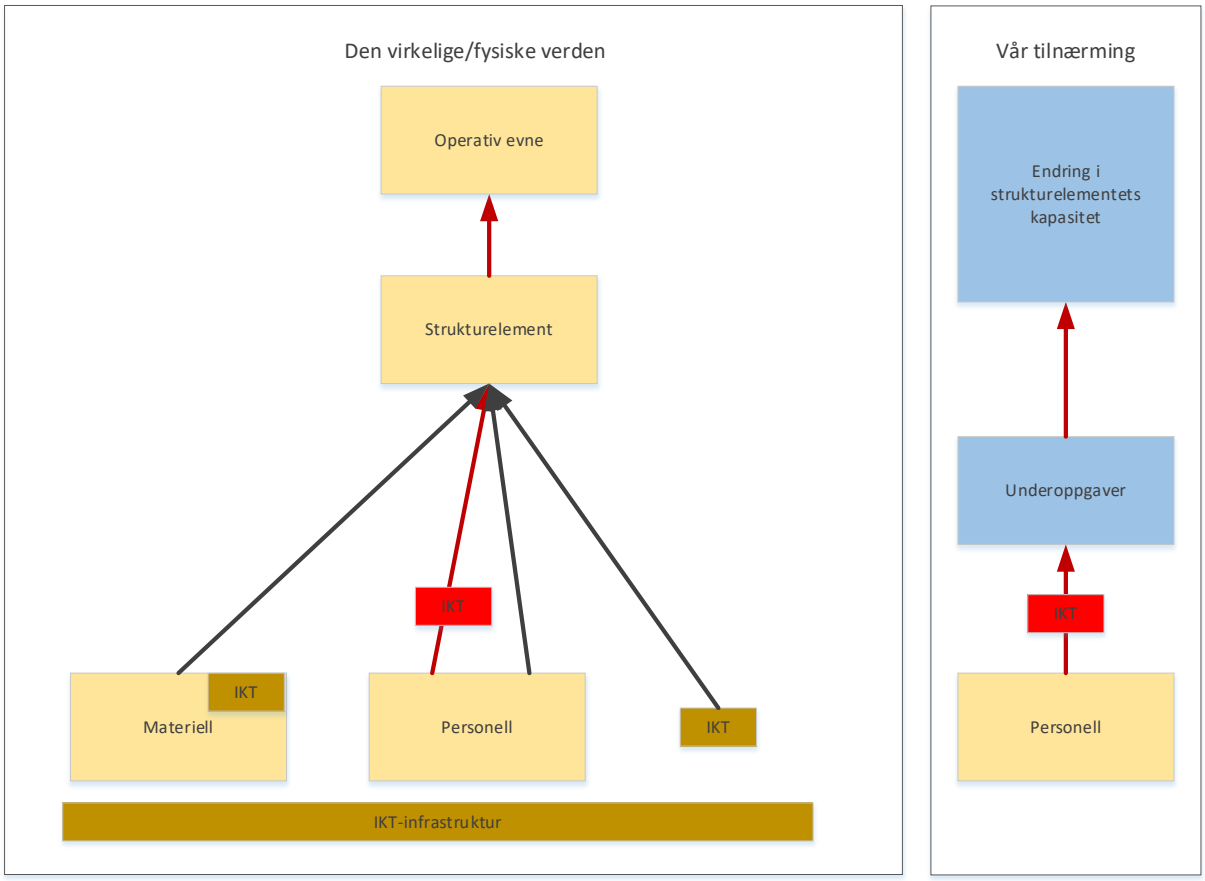
[66] I denne rapporten benytter vi inndelingen som vist i figur 6.1. Det er også mulig å bruke andre inndelinger, for eksempel IKT som er integrert i strukturelementet og som er nødvendig for at strukturelementet skal fungere i seg selv, IKT som muliggjør at et strukturelement kan kommunisere med andre strukturelementer og IKT som muliggjør at personer i et strukturelement kan kommunisere med personer i andre strukturelementer.

fra start til slutt, gjør at alle forsøk på å etablere en årsakskjede vil ha store forenklinger, slik vi ser det. Derfor har vi lagt oss på en mer pragmatisk linje.

Vi har identifisert tre bestanddeler, som bidrar til å gi en struktur på en argumentasjonskjede som leder fra IKT til kapasitet. Disse bestanddelene er personellroller, IKT-systemer og underoppgaver[67]. Vi har tatt utgangspunkt i den midtre IKT-typen i figur 6.1 – IKT-systemer som brukes av personellet i et strukturelement – og lagt til grunn at IKT-systemene brukes for å løse oppgaver internt i strukturelementet for å muliggjøre leveranse av kapasitetene. Vi kan da først velge et strukturelement og en av dens kapabiliteter for analyse, og deretter spisse informasjonsinnsamlingen til å identifisere underoppgaver som bidrar til leveransen av kapabiliteten, personellet som gjør dem og IKT-systemene de bruker. Det er på ingen måte en ny tanke i seg selv å slå fast at personell bruker IKT-systemer til å løse oppgaver, men vi har ikke sett dette gjort tidligere som et ledd i å integrere IKT i langtidsplanleggingen slik vi forsøker her.

Vi får da til slutt en kjede fra personellroller, deretter til IKT, så til underoppgave, og tilslutt til et strukturelements kapasitet. Dette er illustrert i figur 6.2.

[67] Vi bruker «underoppgaver» for å skille disse fra «oppgaver», da sistnevnte begrep allerede har en særegen betydning i SIMFOR-metodikken.



Figur 6.2 Illustrasjon som viser hvordan ulike former for IKT bidrar til strukturelementets operative evne, samt hvilken IKT vi har valgt og hvordan vi i vår tilnærming prøver å fange dette.

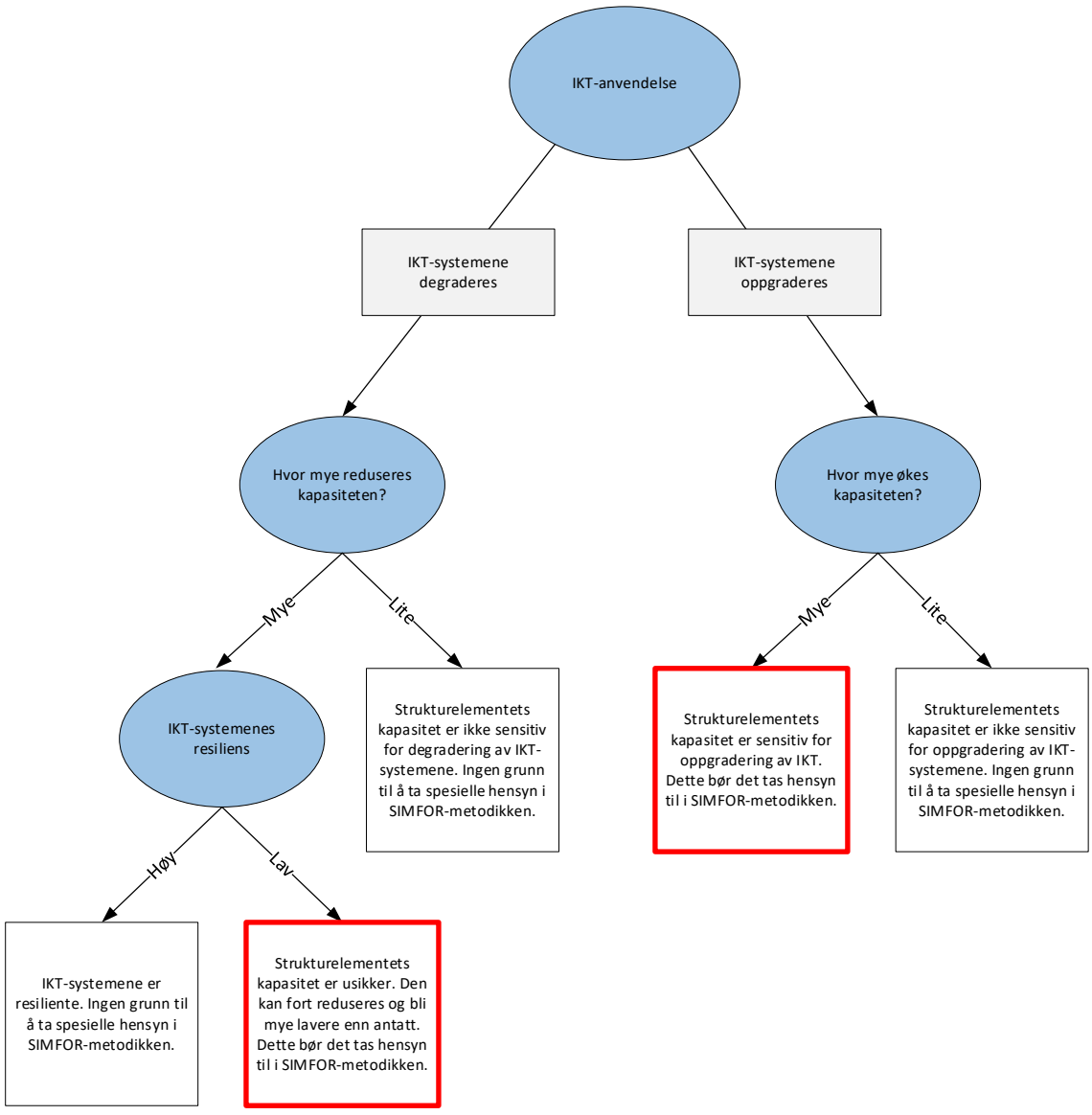
Denne kjeden har vært grunnlaget for å utvikle et mer praktisk håndverk med hjelpeverktøy for informasjonsinnsamling og analyse, som beskrevet i kapittel 6.6.

Her er det også verdt å merke seg at ulike strukturelementer med samme kapabilitet ikke nødvendigvis bruker de samme IKT-systemene. Dette kan skyldes både at kapabiliteten baseres på forskjellige oppgaver i de forskjellige strukturelementene, og at samme oppgaver utføres med forskjellige IKT-systemer.

6.3 Hvordan IKT-anvendelsen kan knyttes til SIMFOR-metodikken

Ved å kartlegge IKT-anvendelsen har man et utgangspunkt for hvordan man videre kan gjøre vurderinger knyttet til hvor sensitivt strukturelementet er med tanke på endringer i de understøttende og integrerte IKT-systemene som vist i delkapittel 6.2. En overordnet oversikt over

hvordan IKT-anvendelsen og vurderinger knyttet til kapasitetsendringer og IKT-systemenes resiliens kan knyttes til SIMFOR-metodikken er vist i figur 6.3.



Figur 6.3 Enkel prinsippskisse av hvordan IKT-anvendelsen og resultatet av vurderinger av kapasitetsendringer samt resiliens bør inkluderes i SIMFOR-metodikken.

Dersom degradering av IKT-systemene ikke medfører at strukturelementets kapasitet endrer seg mye, trenger man ikke inkludere vurderinger knyttet til IKT når man behandler strukturelementet i SIMFOR-metodikken.

Hvis strukturelementets kapasitet derimot reduseres mye, er det viktig å undersøke i hvilken grad disse IKT-systemene er resiliente. Resiliens kan defineres som evne til å tilpasse seg endrede betingelser og forberede seg på anslag, motstå disse og hurtig returnere til et tilstrekkelig funksjonsnivå.[68] Dersom IKT-systemene er resiliente, vil det være vanskelig for en motstander å degradere disse systemene. Resiliensen til IKT-systemene vil derfor være en viktig faktor knyttet til i hvilken grad et strukturelement klarer å levere sine kapasiteter, gitt at strukturelementet er sårbart for degradering av IKT-systemene og disse blir utsatt for trusler. Vurderinger knyttet til IKT-resiliens gjøres dog uavhengig av trusselsituasjonen, og den kan gjøres separat fra vurderinger knyttet til IKT-anvendelse.

Dersom IKT-systemene har høy resiliens, er det ikke nødvendig å inkludere vurderinger knyttet til IKT når dette strukturelementet og denne kapabiliteten behandles i SIMFOR-metodikken. Hvis derimot strukturelementets kapasitet reduseres mye ved degradering av IKT-systemene og i tillegg disse IKT-systemene er lite resiliente, bør IKT-vurderinger tas med i analysen. Da er strukturelementets kapasitet usikker, siden et angrep på IKT-systemene fort kan redusere kapasiteten mye. For eksempel bør det da vurderes om det bør investeres i mer resiliente IKT-systemer eller om kapabiliteten bør dekkes med strukturelementer som ikke har denne sårbarheten.

Når man vurderer kapasitetsendringer ved degradering av IKT-systemene, bør man vurdere degradering knyttet til konfidensialitet, integritet og tilgjengelighet.

Tilsvarende undersøkes det i hvilken grad kapasiteten kan økes dersom IKT-systemene oppgraderes. Denne oppgraderingen kan bestå av at det investeres i mer av IKT-systemer man allerede har og/eller at det investeres i nye og bedre IKT-systemer. Ved disse vurderingene bør man se på om oppgraderingen av IKT-systemene kan muliggjøre nye handlemåter med potensielt nye underoppgaver og personellroller.[69]

Dersom man finner at oppgradering av IKT-systemene øker kapasiteten lite, kan man utelate vurderinger av oppgradering av IKT-systemer knyttet til dette strukturelementet og denne kapabiliteten inn i SIMFOR-metodikken. Hvis derimot strukturelementets kapasitet øker mye, bør vurderinger knyttet til investeringer i IKT tas med inn i SIMFOR-metodikken. For eksempel bør det vurderes om det kan være kosteffektivt å investere i IKT-systemer fremfor flere strukturelementer dersom man trenger mer av denne kapabiliteten.

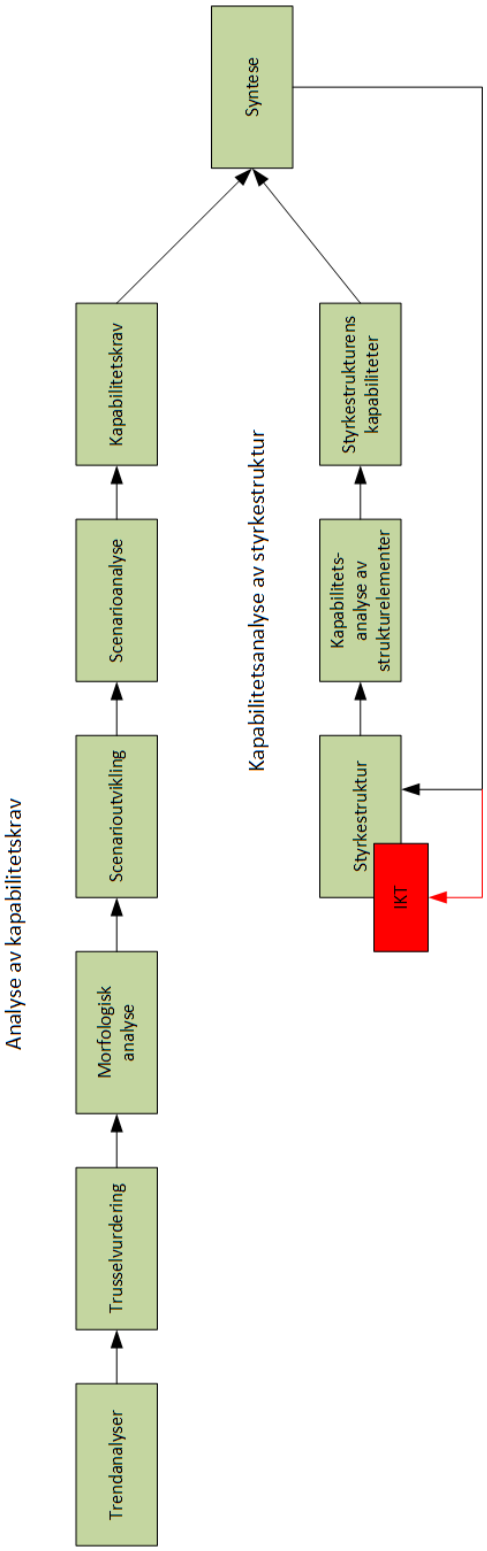
[68] «[A]bility to adapt to changing conditions and prepare for, withstand and rapidly recover from disruption»; DHS Risk Lexicon, 2010 Edition; https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

[69] Et eksempel på en spillbasert metode for dette finnes i Siedler, R. E.; Hansen, B. J.; Farsund, B. H.; Diesen, S.; *(U) Det blå IKT-spillet – en beskrivelse av muligheter ved ny IKT under Begrenset angrep;* FFI-rapport 22/00897 [KONFIDENSIELT].

Hva som defineres som «mye» og «lite» kapasitetsendringer og «høy» og «lav» resiliens er dog et skjønnsspørsmål analytikeren må vurdere.

I henhold til vår metode er IKT-vurderingenes plass i SIMFOR-metodikken knyttet til styrke-strukturen. Dette gjelder i prinsippet alle de tre måtene et strukturelement kan anvende IKT på. Vi visualiserer dette ved å legge til IKT som en ekstra faktor i SIMFOR-metodikken, tett knyttet til styrkestrukturen, se figur 6.4.

I tillegg til at inkludering av IKT-anvendelsen og vurderinger knyttet til kapasitetsendringer og resiliens kan gi mer helhetlige svar ved bruk av SIMFOR-metodikken som angitt over, så kan også vurderinger av kapasitetsendringer brukes for å stadfeste IKT-behovet i et gitt scenario. Identifiserte endringer, i IKT-systemer og IKT-infrastruktur som påvirker kapasitet slik at krav ikke kan oppfylles, sier også noe om hva IKT-systemer og -infrastruktur må kunne yte. Vår metode kan dermed bidra til å stadfeste IKT-behovet i et gitt scenario. Behovet kan videre benyttes som et referansepunkt som andre IKT-styringsløp kan sjekkes opp mot. Dette blir da et møtepunkt mellom SIMFOR-metodikken og andre prosesser som påvirker hva vi har av IKT og hva den yter, som ulike planleggings- og styringsprosesser for utvikling av IKT-porteføljen.



Figur 6.4 Oversikt over hvilke analyser og vurderinger som utføres i SIMFOR-metodikken og hvor vurderinger knyttet til IKT-systemene bør gjøres.

6.4 Metodens håndtering av identifiserte utfordringer

Metoden håndterer de seks identifiserte utfordringene med inkludering av IKT i langtids-planleggingen beskrevet i kapittel 4 på ulikt vis:

1. Hvilket tidsperspektiv skal benyttes? I metoden fokuseres det på IKT som er i bruk i dag for å forstå IKT-anvendelse og konsekvensene av degradering for eksisterende kapasiteter. Men en slik vurdering bør i prinsippet også gjøres for eventuelle planlagte IKT-systemer. Ved vurderinger knyttet til oppgradering av IKT-systemene vil man også kunne gjøre vurderinger knyttet til fremtidige IKT-systemer, men i praksis vil dette ikke være like langt frem i tid som ved andre strukturelementer.

2. Hvilken IKT fokuserer vi på? Metoden i seg selv kan dekke all IKT. Vi har i vår metodeutvikling gjort en avgrensing til IKT-systemer som personellet interagerer med, med rom for eventuell videre kartlegging av avhengigheter nedover til andre under-liggende IKT-systemer. IKT-systemene som dekkes er dermed i utgangspunktet de IKT-systemene som personellet selv identifiserer, ikke en tydelig forhåndsdefinert kategori av IKT.

3. Hva er fordelene ved å bruke IKT? Vi omgår i stor grad problemstillingene knyttet til å etablere og benytte en teoretisk fundert modell over fordelene ved å anvende IKT. Vi tar utgangspunkt i dagens anvendelse og ser på denne som en baselinje. Vi diskuterer så med eksperter hva som skjer med strukturelementenes kapasitet hvis IKT-systemene degraderes eller oppgraderes. På denne måten får vi synliggjort nytten av IKT.

4. Hva er risikoen ved å bruke IKT? Risiko fanges delvis opp gjennom konsekvenser for kapasitet dersom IKT degraderes. Resiliens er i prinsippet en del av metoden og vil være grunnlag for å kunne gjøre ytterligere vurderinger av risiko og usikkerheten knyttet til denne. Sannsynlighet og trusler blir derimot ikke håndtert.

5. Hva er IKT-behovet og hvordan dekkes dette? Metoden søker kun å fange opp IKT-behov gjennom dagens IKT-anvendelser, og fageksperters vurderinger knyttet til justeringer av disse. Metoden fungerer i utgangspunktet uten scenarioer, men er åpen for å trekke dette inn dersom det blir synlig i en analyse at kapasitetsendringene en får ved oppgraderinger og/eller degraderinger i IKT-systemene er sensitive for scenario- og vignettkonteksten.

6. Hva koster IKT? Vi har ikke fokusert på kostnad i vår metodeutvikling, men kostnader kan belyses sammen med at en ser på oppgradering av IKT og mer resilient IKT. De involverte IKT-systemene kan være startpunktet for en avgrenset studie av kostnader med for eksempel undersøkelse av relevante budsjetter og liknende.

6.5 Andre fordeler og ulemper med metoden

I motsetning til dagens inkludering av IKT i SIMFOR-metoden med IKT-kapabiliteter, gjør vår metode det mulig å belyse strukturelementenes anvendelse av IKT-systemer og hvordan dette påvirker kapasitetene. På grunn av metodens innretning blir flere av utfordringene knyttet til inkludering av IKT i langtidsplanlegging omgått, herunder etablering av teoretiske årsakskjeder for operativ effekt, noe som forenkler arbeidet som må gjøres. Selv om metoden kan anses som omfattende, så skalerer i prinsippet metoden relativt godt dersom flere strukturelementer og kapabiliteter skal studeres.

Samtidig har metoden enkelte ulemper. Den beror på informasjonsinnsamling og vurderinger av både fageksperter, operativt personell og analytikerne som gjennomfører metoden, og dersom feilaktig eller ukomplett informasjon og vurderinger legges til grunn blir resultatet av metoden deretter. Kvaliteten på eksisterende beskrivelser av strukturelementer og kapabiliteter påvirker hvor mye arbeid som må gjøres for å etablere gode vurderinger. Dersom IKT-systemenes påvirkning på kapasiteter viser seg å være meget kontekstavhengig, det vil si at kapasitets-endringene er situasjonssensitive, og flere scenarioer og vignetter bør utforskes, så vil antall vurderinger som bør gjennomføres fort bli for mange og kreve for mye ressurser. IKT-ens potensiale til å oppnå økt effektivitet ved å endre handlemåter eller personellets arbeidsflyt er ikke adressert. Et ønske om økt nøyaktighet i vurderingene ved å ta hensyn til flere detaljer og gjennomføre dypere undersøkelser kan også føre til at metoden blir for omfattende i praksis. Til sist er den negative konsekvensen av at enkelte problemstillinger er omgått (jf. kapittel 6.4) at disse forblir uløst.

6.6 Det praktiske håndverket

Det praktiske håndverket i metoden som driver informasjonsinnsamlingen og analysen består av seks steg. Da degradering av IKT har vært i fokus i utviklingsarbeidet, ikke oppgradering, reflekterer de siste to stegene i metoden dette. Det antas at de første fire stegene også vil kunne understøtte analyser rettet mot oppgradering av IKT. Resiliens dekkes ikke av metoden, men resultater fra egne resiliensanalyser kan kombineres med resultater fra kapasitetsvurderinger. Dette er skrevet inn som et ekstra syvende steg til slutt.

Stegene i metoden er:

1. Valg av strukturelement og kapabiliteter som ønskes analysert.

2. Innsamling av informasjon om hvilke IKT-systemer som er involvert, hvilke personell som bruker IKT-systemene og hvilke oppgaver som personellet utfører for å realisere kapabilitetene.

3. Analyse av innsamlet informasjon, inklusive sammenfatning og presentasjon av informasjon i strukturerte diagrammer.

4. Ytterligere informasjonsinnsamling og analyse av IKT-systemenes oppbygging og avhengighet av andre IKT-systemer og IKT-infrastruktur, dersom ønskelig.

5. Innsamling av informasjon om hvordan endringer i IKT-systemenes sikkerhets-egenskaper påvirker kapasitetene.

6. Sammenfattende analyse av IKT-systemenes innvirkning på strukturelementets kapasitet(er).

7. Ekstra steg: Sammenstilling av resultater fra kapasitetsvurderinger og resiliensanalyser.

Merk at selv om denne metoden fremstilles som en fossefallsmetode, hvor stegene tas én etter én i stigende rekkefølge, så vil det i praksis være rom for å hoppe mellom enkelte av stegene og jobbe iterativt for å få etablert et tilstrekkelig detaljert og dekkende informasjonsgrunnlag. Likevel vil det kunne være hensiktsmessig å etablere en relativt komplett oversikt over IKT-systemer, personellroller og underoppgaver som kvalitetssikres før kapasitet og kapasitets-endringer adresseres. All informasjon som samles inn ved intervjuer eller workshoper, bør kvalitetssikres av deltakerne etter at analytikerne har strukturert informasjonen.

Metoden kan benyttes både med og uten en eksplisitt scenariokontekst med taktiske vignetter. Behovet for å definere slike forhold vil være et resultat av hvor sensitive vurderingene er for endringer i disse. Selv om ingen kontekst er definert for en gitt analyse, bør analytikerne forsøke å fange opp eventuelle forutsetninger og gjøre vurderinger av sensitiviteten underveis. Dersom indikasjoner tyder på at sensitiviteten er høy, kan dette kreve etablering av en mer eksplisitt kontekst. Forhold som kan inngå her er scenario med trussel, blå handlemåte, blått oppdrag og blått operasjonskonsept på ulike nivåer.

Dersom det inngår i analysen å gjøre endringer i disse forholdene, vil man i praksis måtte kjøre deler av metoden flere ganger. Enkelte ganger vil dette være hensiktsmessig, for eksempel hvis man ønsker mer dybdekunnskap om IKT-anvendelsen og kritikaliteten ved denne på tvers av ulike situasjoner.

Hvert av stegene i metoden utdypes videre i det følgende:

6.6.1 Steg 1 – Valg av strukturelementer og kapabiliteter som ønskes analysert

Ett eller flere strukturelementer, og én eller flere kapabiliteter tilhørende hvert strukturelement velges for analyse. Gitt de store forskjellene som vanligvis finnes mellom IKT-anvendelsen til ulike strukturelementer, anbefales det å gjøre separate analyser for hvert strukturelement dersom flere er valgt.

Dersom flere kapabiliteter for et gitt strukturelement er valgt, bør det vurderes løpende om det er behov for separate analyser for hver kapabilitet. Hvor like IKT-anvendelsene for kapabili-tetene er, inklusive om kritikaliteten er lik, bestemmer dette.

6.6.2 Steg 2 – Innsamling av informasjon om hvilke IKT-systemer som er involvert, hvilke personell som bruker IKT-systemene og hvilke oppgaver som personellet utfører for å realisere kapabilitetene

Innsamling av informasjon om hvilke IKT-systemer som er involvert i de valgte kapabilitetene på det valgte strukturelementet kan gjøres på flere måter. Informasjon som analytikerne kan finne fra skrevne produkter som tidligere analyser og teknisk informasjon om strukturelementet kan være et godt startpunkt. Den viktigste informasjonskilden vil, etter vårt syn, dog være å intervjue eksperter og personellet som er en del av strukturelementet som benytter IKT-systemene.

Informasjon om personellroller og underoppgaver kan i prinsippet søkes gjennom skriftlig materiale der dette er dokumentert, men eksperter og personellet selv fremstår også her som den viktigste informasjonskilden.

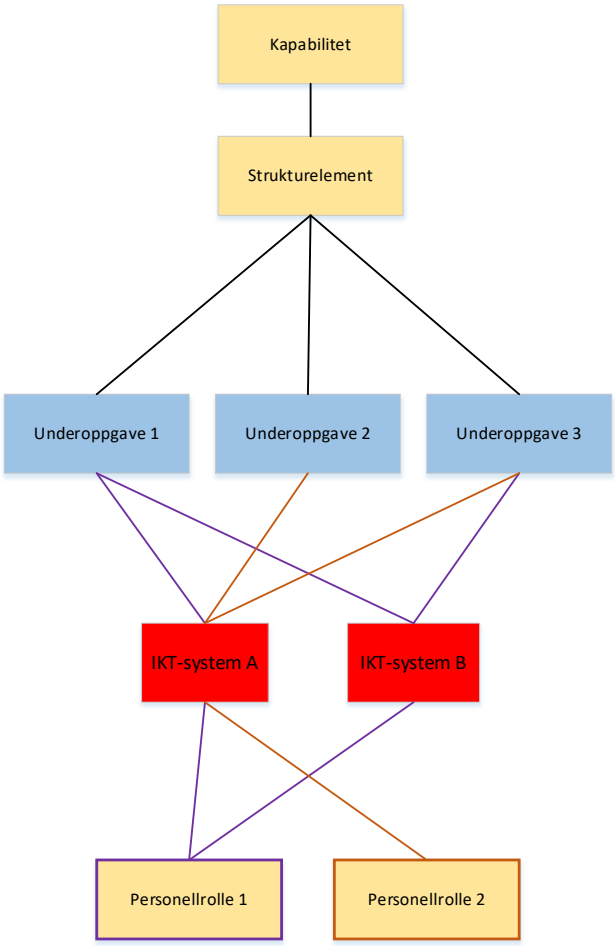
Følgende spørsmål er et utgangspunkt for å hente inn nødvendig informasjon. Rekkefølgen på spørsmålene kan variere, da analytikeren kan ha ulike strategier for å samle inn informasjonen. I listen under legges det til grunn at analytikeren ønsker å identifisere involverte personer i strukturelementet først, for så finne mer ut om oppgavene de utfører og IKT-systemene de bruker for å løse dem.

1. For de valgte kapabilitetene, hva er strukturelementets kapasiteter?
2. Hvem bidrar til å opprettholde kapasiteten? Dette kan være personer, både «innenfor» selve strukturelementet og utenfor, samt operatører og annet personell som bruker IKT-systemene.
3. Hvilke oppgaver utfører/løser de som enkeltindivider eller gruppe?
4. Hvilke IKT-systemer benytter de i sin oppgaveløsning?
5. Hva er helheten og samspillet mellom disse menneskene og deres oppgaver? Er de f.eks. avhengig av at andre gjør sine oppgaver for å kunne gjøre sine egne?
6. Har de alternative løsninger som kan benyttes for å gjennomføre oppgaver, dersom noe skjer med IKT-systemene?

Den innsamlede informasjonen skrives ned på en egnet måte. Det er viktig å opprettholde de logiske linkene mellom svar på de ulike spørsmålene, For eksempel hvilke IKT-systemer som brukes av hvilke personer for å utføre hvilke oppgaver. Ved intervjuer eller workshoper kan det være nyttig å gjøre løpende nedskriving elektronisk med felles visning slik at alle deltakerne ser nedskrivingen og kan gjøre korrigereringer og presiseringer på selve data-materialet underveis. Dette hever kvaliteten på innsamlet informasjon og gjør kvalitets-sikring lettere.

6.6.3 Steg 3 – Analyse av innsamlet informasjon, inklusive sammenfatning og presentasjon av informasjon i strukturerte diagrammer

Den innsamlede informasjonen bearbeides og struktureres for at analytikerne skal kunne danne seg et helhetsbilde. Dette inkluderer å etablere en sporbar oversikt over hvilke personer og deres oppgaver som bidrar til å opprettholde hvilke kapasiteter, og hvilken IKT som kan brukes for å støtte personene i deres oppgaver. En egen mal for diagrammer er utarbeidet for dette formål, se figur 6.5.



Figur 6.5 Strukturen på diagrammene til bruk under informasjonsinnsamlingen.

6.6.4 Steg 4 – Ytterligere informasjonsinnsamling og analyse av IKT-systemenes oppbygging og avhengighet av andre IKT-systemer og IKT-infrastruktur, dersom ønskelig

Når listen over involverte IKT-systemer er klar, analyseres IKT-systemenes oppbygging og koblinger til andre IKT-systemer og underliggende IKT-infrastruktur. Dette gjøres for å inkludere IKT-systemer og IKT-infrastruktur som ikke personellet direkte interagerer med, men

som de identifiserte IKT-systemene selv benytter. Endringer i disse kan også påvirke strukturelementenes kapasiteter, men da gjennom lengre årsakskjeder. Dersom det finnes oversikter eller annen kjent informasjon om IKT-systemenes oppbygging og koblinger til andre IKT-systemer og underliggende IKT-infrastruktur, bør disse benyttes.[70]

6.6.5 Steg 5 – Innsamling av informasjon om hvordan endringer i IKT-systemenes sikkerhetsegenskaper påvirker kapasitetene

Etter hvert som grunnlagsinformasjonen er strukturert, samler analytikerne inn vurderinger knyttet til konsekvensene for kapasitetene ved endringer i IKT-systemenes sikkerhetsegenskaper. Disse vurderingene gjøres i første rekke av personellet som bruker IKT-systemene og utfører oppgaver som støtter kapasitetene, men de kan også være gjort av andre eksperter.

Med andre ord:

> Hva er personellets formening om konsekvensene for kapasitet, dersom IKT-systemene de bruker degraderes på ulikt vis, alternative løsninger må tas i bruk, eller om IKT-systemene forbedres?

Med degradering eller forbedring av IKT-systemer menes endringer i sikkerhetsegenskapene konfidensialitet, integritet og tilgjengelighet.

Her ber vi ikke operativt personell gjøre dype vurderinger, men besvare etter beste evne under intervju eller workshop. Vurderingene kan være basert på personellets egne erfaringer eller meninger, eller inkludere eventuelle relevante studier dersom personellet kjenner til dette.

6.6.6 Steg 6 – Sammenfattende analyse av IKT-systemenes innvirkning på strukturelementets kapasitet(er)

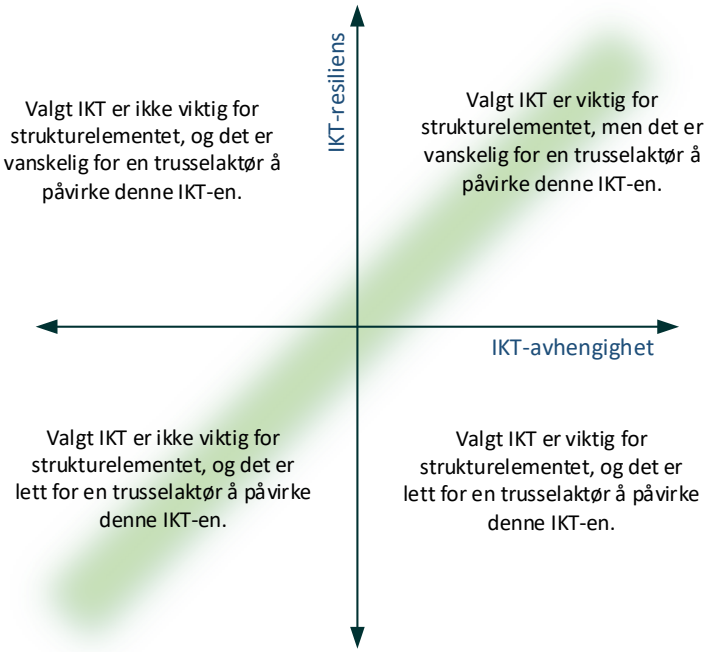
Avhengig av hvilken og hvor mye informasjon som er samlet inn, kan det gjøres en samlet vurdering om IKT-systemenes innvirkning på strukturelementets kapasiteter basert på alle tilgjengelige kilder. Dette kan inkludere både hvordan ny eller forbedret IKT kan ha en positiv innvirkning og hvordan degradert IKT kan ha en negativ innvirkning. Fageksperter eller personell som tidligere har vært involvert i analysene, eller andre individer med relevant kompetanse, kan benyttes for å kvalitetssikre resultatene.

6.6.7 Ekstra steg 7: Sammenstilling av resultater fra kapasitetsvurderinger og resiliensanalyser

Kunnskap om IKT-anvendelse og kapasitetsvurderinger kan settes sammen med vurderinger om resiliens for å belyse om IKT-anvendelsene og deres kritikalitet, og resiliens, er balansert. Dette kan gjøre det mulig å identifisere både over- og underinvesteringer i resiliens, og hvor en

[70] Her kan det potensielt hentes informasjon fra arkitekturarbeidet som utføres ved Forsvarsmateriell. Se også notat av Brose, M.A. og Bentstuen, O.I. (under utarbeidelse).

eventuelt bør sette inn tiltak. Ideen om å kombinere innsikt på denne måten er i prinsippet gyldig uavhengig av hvordan en har fått generert innsikt om hvor viktig IKT er, og dens resiliens, se figur 6.6.



Figur 6.6 Startpunktet for å lage en eller flere IKT-profiler for et strukturelement.

I figur 6.6 er resiliens (y-aksen) krysset med IKT-avhengighet (x-aksen). IKT-avhengighet er her et uttrykk for hvor kritisk anvendelsen av IKT er. For at en slik figur skal være nyttig er det viktig å presisere i forkant hvilken IKT figuren er ment å omfatte, samt hvordan IKT-en gir utslag på strukturelementets virke. Slike figurer kan ansees å være IKT-profiler for et strukturelement.

Kvadrantene er definert som:

- Høy IKT-avhengighet, høy resiliens ved valgt IKT: Valgt IKT er viktig for strukturelementet, men det er vanskelig for en trusselaktør å påvirke IKT-en. Her er det samsvar mellom graden av IKT-avhengighet og resiliensnivået – den viktige IKT-en (og dennes avhengigheter) er resilient.

- Lav IKT-avhengighet, høy resiliens ved valgt IKT: Valgt IKT er ikke viktig for strukturelementet, og det er vanskelig for en trusselaktør å påvirke IKT-en. Her er det ikke samsvar mellom graden av IKT-avhengighet og resiliensnivået. Her kan f.eks. ressurser reprioriteres.

- Lav IKT-avhengighet, lav resiliens ved valgt IKT: Valgt IKT er ikke viktig for strukturelementet, og det er lett for en trusselaktør å påvirke IKT-en. Her er det samsvar mellom graden av IKT-avhengighet og resiliensnivået.

- Høy IKT-avhengighet, lav resiliens ved valgt IKT: Valgt IKT er viktig for strukturelementet, og det er lett for en trusselaktør å påvirke IKT-en. Her er det ikke samsvar mellom graden av IKT-avhengighet og resiliensnivået. Enten bør resiliensen økes eller avhengigheten senkes, for eksempel ved å endre operasjonskonsept.

Da et strukturelement potensielt kan benyttes i ulike situasjoner, og ha forskjellige oppdrag og operere etter ulike operasjonskonsepter, så vil også IKT-avhengigheten og således IKT-profilene for strukturelementet kunne variere. Dersom en IKT-profil er forholdsvis lik over mange av disse parameterne så er IKT-profilen stabil. Dersom den varierer mye, er IKT-profilen ustabil. Høy variasjon i en IKT-profil kan medføre at det er nødvendig å utforske flere kombinasjoner av ulike parametere for å forstå hvordan viktigheten av IKT-systemene kan variere.

7 Erfaringer med metoden

Som et ledd i utviklingen av metoden presentert i kapittel 6 gjennomførte vi to caser der vi tok for oss to ulike strukturelementer og brukte interne eksperter ved FFI ved informasjons-innsamlingen og analysen som beskrevet i kapittel 6.6. Casene vi valgte omhandlet OP-lag og F-35. Siden detaljene i informasjonen og analysene omhandler virkelige strukturelementer, har vi valgt å gi ut en egen gradert versjon av denne rapporten hvor dette er inkludert.[71] Her vil vi gå gjennom de mer generelle erfaringene vi gjorde oss etter å ha gjennomført disse casene. Casene ble gjennomført i flere omganger, noe som gjorde at vi kunne bruke erfaringer underveis til å videreutvikle metoden.

Først og fremst erfarte vi at stegene i kapittel 6.6 ga oss informasjon som satte oss i stand til å gjøre de analysene vi var ute etter. Vi måtte dog gjennom noen forsøk før vi endte opp med en strukturering og visualisering av informasjonen som gjorde informasjonsinnsamlingen og kvalitetskontrollen med de interne ekspertene effektiv.

De to casene ble valgt slik at de var ganske forskjellige i omfang, og det viste seg at spesielt det mest omfattende caset var tids- og ressurskrevende til tross for at vi bare tok for oss én av flere kapabiliteter. Dette peker mot at en full gjennomføring av metoden for alle strukturelementer og deres kapabiliteter vil være et omfattende arbeid. Samtidig var det indikasjoner på at flere IKT-anvendelser var like på tvers av flere kapabiliteter. Hvor ofte man trenger å gjennomføre slike analyser vil imidlertid avhenge av om noen faktorer i analysen har blitt endret. Videre bør det være mulig å etablere informasjonsdatabaser (for eksempel som NORAR, men med sterkere konsistenssjekk) for å bygge og vedlikeholde informasjonsgrunnlag som så kan nyttiggjøres i analyser. Dette burde kunne gjøre innsamlingsarbeidet mindre ressurskrevende. I tillegg tror vi at man etter hvert vil se at ulike former for IKT-anvendelse ikke bare vil gjenta seg innenfor samme strukturelement, men også på tvers mellom ulike strukturelementer.

Formålet med å gjennomføre casene var først og fremst å teste og videreutvikle metoden, og gjennomføringen var ikke planlagt med tanke på å identifisere faktisk IKT-anvendelse og kapasitetsendringer for strukturelementene vi valgte. Vi klarte imidlertid å gjennomføre analyser som etablerte en koherent sammenheng mellom IKT og kapasitet, noe som tyder på at metoden kan bidra med slike resultater. Med tanke på hvordan prosessen ble gjennomført, og spesielt det at vi ikke innhentet informasjon hos operativt personell tilknyttet de aktuelle strukturelementene, anser vi imidlertid at de konkrete analyseresultatene må gjennom ytterligere kvalitetssikring før de kan anses for å være av verdi.

[71] Farsund, B.H.;Thuv, Aa.; Hansen, B. J.(2022); *Hvordan håndtere operativ IKT i Forsvarets langtidsplanlegging – inkludert to testcaser;* FFI-rapport 22/01703 [BEGRENSET].

8 Oppsummering og veien videre

IKT er en kritisk faktor for at Forsvaret skal kunne løse sine oppgaver, men inngår i liten grad som et selvstendig tema i langtidsplanleggingen som ligger til grunn for framtidig forsvars-struktur. Dette gjør at IKT ikke blir behandlet og vurdert på lik linje med andre struktur-elementer, og dette har konsekvenser for muligheten til å gjøre hensiktsmessige investeringer i Forsvaret generelt og i IKT spesielt.

Denne utfordringen er blant temaene det har vært arbeidet med i FFI-prosjektet «Forsvarets bruk av det digitale og elektromagnetiske rom». Resultatet av dette arbeidet er en foreslått metode for å inkludere IKT i langtidsplanlegging på en strukturert og etterprøvbar måte.

Den grunnleggende ideen bygger på at IKT støtter opp under de forskjellige kapasitetene til strukturelementene i Forsvaret, både som en komponent i strukturelementene og som en støttefunksjon og integrator som sørger for at strukturelementer kan samhandle. Dette bør det tas hensyn til i langtidsplanleggingen. Vi foreslår at dette undersøkes gjennom å analysere strukturelementenes IKT-anvendelse basert på en grundig informasjonsinnsamling. Denne rapporten inneholder et forslag til en metode for å gjennomføre en slik informasjonsinnsamling med tilhørende analyse, samt hvordan man kan tilrettelegge for kapasitetsvurderinger.

Vi har testet denne metoden i to caser. Erfaringen er at metoden synliggjør IKT-anvendelsen på en god måte, samt at den er en realistisk måte å angripe denne problemstillingen på.

Integrert i langtidsplanlegging legger vår tilnærming opp til en analyse med tilhørende informasjonsinnsamling for alle relevante strukturelementer og deres kapabiliteter. Dette kan synes som en omfattende og omstendelig måte å angripe problemet på, men dette er den beste måten vi har funnet. Med tanke på kompleksiteten moderne IKT-systemer og -infrastrukturer innehar, hvor viktig IKT er for Forsvaret og det faktum at IKT nå er allesteds-nærværende i hele Forsvaret vil det bli omfattende. Det er også verdt å merke seg at resultatene fra en slik analyse også kan brukes til å forstå sammenhengen mellom IKT og operativ nytte, og med det være med på å kvantifisere hvilken nytte Forsvaret har av IKT også innen andre områder enn langtids-planlegging. Konsekvensene som blir synliggjort ved degradering av IKT-systemene, vil eksempelvis kunne være nyttige ved planlegging av militære operasjoner.

Veien videre for et slikt arbeid er først og fremst mer testing. Både for å undersøke nærmere om metoden lar seg gjennomføre fullt ut, og for å undersøke aspekter ved metoden som ikke ble inkludert i denne omgang. For det første bør casene som er skissert gjennomføres også med eksterne eksperter for å se om det er realistisk å fange den ønskede informasjonen slik at analysene lar seg gjennomføre. Det bør også gjennomføres grundigere analyser for å se hvor realistisk det er å utlede faktiske endringer i kapasitet for strukturelementene på grunnlag av deres bruk av IKT. Videre bør analysene som er skissert utvides til å inkludere IKT-systemenes resiliens. Et annet aspekt som ikke er berørt i dette arbeidet, og som bør forfølges videre, er hvorvidt og i hvilken grad forbedring i IKT kan medføre økning i kapasitet. Det var i dette arbeidet heller ikke rom for å se på effekten av indirekte avhengighet av IKT, altså at IKT-

systemene som strukturelementene er avhengig av igjen er avhengig av andre IKT-systemer. Dette bør også inkluderes i videre testing av metoden. Dersom videre testing av metoden skulle vise seg å være vellykket, er det mulig å gå i gang med et mer omfattende arbeid for å kartlegge flere strukturelementers anvendelse av IKT.

Alt i alt mener vi at den foreslåtte tilnærmingen er en hensiktsmessig måte å ta hensyn til IKT på i en langtidsplanleggingsprosess, men at det fortsatt gjenstår mye arbeid for å kunne fullføre hele prosessen.

Referanser

Arnfinnsson, B; Elman, E; Eriksen, S. H. (2020); *Hvor mye bruker forsvarssektoren på IKT?;* FFI-rapport 20/00806 [BEGRENSET].

Bender (2016); *This chart shows just how massive America's drone fleet is*; https://www.businessinsider.com/chart-of-us-drone-fleet-2016-3 [Sist besøkt 04.07.22].

Bentstuen, O.I. (2019): *Trender som påvirker Forsvarets kommunikasjonsinfrastruktur;* FFI-fakta.

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

Consultation, Command and Control Board (C3B); C3 Taxonomy Baseline 5.0; 30. August 2021.

DHS Risk Lexicon, 2010 Edition; https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf. [sist besøkt 08.08.22].

Einan, T. S.; Drønen, O. (2022); *Slår alarm: Nytt datasystem kan gi pasienter feil diagnose*; Morgenbladet nr. 13, årgang 203.

Farsund, B.H.; Enemo, G. (2018); *En morfologisk analyse av tilsiktede uønskede handlinger rettet mot Forsvarets informasjonsinfrastruktur*; FFI-rapport 18/00466.

Farsund, B. H.; Søndrol, T.; Nystuen, K. O.; Hornfelt, L. Sellevåg; S. R.; Pham, V. (2022); *Utviklingen av nye IoT-baserte infratrukturer i samfunnet – utfordringer for nasjonal sikkerhet*; FFI-rapport 22/00631.

Farsund, B.H.; Thuv, Aa.; Hansen, B. J. (2022); *Hvordan håndtere operativ IKT i Forsvarets langtidsplanlegging – inkludert to testcaser;* FFI-rapport 22/01703 [BEGRENSET].

Forsvaret (2019); *Forsvarets fellesoperative doktrine*.

Forsvarets Matriellanskaffelser*; Forsvarsstrukturplanlegging*, PRINSIX. https://www.fma.no/prinsix/Prosjektmodell/forsvarsstrukturplanlegging [sist besøkt 29.06.22].

Forsvarsstaben (2021); *Forsvarets IKT-strategi*.

Gartner (2022); *Top Strategic Technology Trends 2022.*

Glærum, S., Berg-Knutsen, E., Gulichsen, S., johansen, I., Steder, F.B. (2008); *FFIs støtte til Forsvarssjefens Forsvarsstudie 2007;* FFI-rapport 2008/00606.

Hennum, A.C.; Glærum, S. (2007); *Metode for langtidsplanlegging – støtte til FS 07*; FFI-rapport 2007/02174.

Jakobsen, H. Ø. (2021); *Slik ble politiets «supervåpen» en 100-millioners fiasko;* Morgenbladet nr. 47. årgang 202.

Johansen, I. (2006); *Scenarioklasser i Forsvarsstudie 2007: En morfologisk analyse av sikkerhetspolitiske utfordringer mot Norge*; FFI-rapport 2006/02664.

Johansen, I. (2021); *Scenarioklasser for forsvarsplanlegging – revisjon av FFIs scenario-grunnlag*; FFI-rapport 21/01788.

Kämpe, M.K.M. (2021); *Langtidsplanen for Forsvaret – hva er det?* Folk og Forsvar. https://folkogforsvar.no/langtidsplanen-for-forsvaret-hva-er-det [sist besøkt 29.06.22].

Køber, P.K.; Arnfinnsson, B. (2020); *(U) Kapabiliteter, strukturelementer og kravsetting i langtidsplanleggingen ved FFI – oppdatert 2019*; FFI-notat 20/00145 [KONFIDENSIELT].

Køber, P.K.; Bjonge, V. (2021); *(U) Kapabiliteter, strukturelementer og kravsetting i langtidsplanleggingen ved FFI – oppdatert 2021*; FFI-eksternnotat 21/02205 [KONFIDENSIELT].

Leveson, N. G. (2011); *Engineering a safer world*; The MIT Press.

NATO STO (2020); *Science & Technology Trends 2020–2040.*

NATO Defence Planning Process; https://www.nato.int/cps/en/natohq/topics_49202.htm [sist besøkt 12.08.22].

Norsk Standard 5814 (2008); *Krav til risikovurdering.*

Norsk Standard 5832 (2014); *Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikrings-risikoanalyse.*

Nystuen, K.O.; Farsund, B.H (2009); *(U) Operativ evne og behovet for sikkerhetsegenskaper i INI – Metode og resultater*; FFI-rapport 2009/00646 [BEGRENSET].

Oren, O.; Gersh, B.J.; Bhatt, D.L. (2020); *Artificial intelligence in medical imaging: switching from radiographic pathological data to clinically meaningful endpoints*; The Lancet.

Perrow, C. (1984); *Normal Accidents: living with high-risk technologies*; Basic Books.

Philip (2019); *Autonomous Devices Are Here. Are You Ready? https://www.bridge-global.com/blog/autonomous-devices-are-here-are-you-ready/* [Sist besøkt 04.07.22].

Prinsix; https://www.fma.no/prinsix/maler/terminologi [sist besøkt 05.09.22].

Regjeringen; *Fremtidige anskaffelser til forsvarssektoren (FAF) 2021—2028*; https://www.regjeringen.no/contentassets/09d83a5cbefd4fb68064e6ca871acccb/faf-2021-2028-norsk-versjon-__.pdf [sist besøkt 05.09.22].

Regjeringen; *Ny langtidsplan for forsvarssektoren (2021—2024)* https://www.regjeringen.no/no/tema/forsvar/ltp/LTP/id2611090 [sist besøkt 29.06.22].

Richards, C. (2020); Boyd's OODA loop; Necesse, vol. 5, nr. 1.

Siedler, R. E.; Hansen, B. J.; Farsund, B. H.; Diesen, S. (2022); *(U) Det blå IKT-spillet – en beskrivelse av muligheter ved ny IKT under Begrenset angrep;* FFI-rapport 22/00897 [KONFIDENSIELT].

Spiegel (2021); *The Fundamentals of AR and VR – and how the Military Is Using Them*; https://www.designnews.com/automation/fundamentals-ar-and-vr-and-how-military-using-them [Sist besøkt 04.07.22].

Stensrud, R.; Rutledal, F.; Danjord, F.: Helesnes, J.-I.; Bjørnesgaard, T. (2007); *Metode for konseptutvikling*; FFI-rapport 2007/01722.

Stojkovic, D.; Dahl, B. R.(2007); *Methodology for long term defence planning*; FFI-rapport 2007/00600.

Store Norske Leksikon; https://snl.no/IKT [sist besøkt 08.08.22].

Telenor (2020); *Når nettene blir lange*; https://www.telenor.no/om/digital-sikkerhet/2020/artikler/nettene-blir-lange.jsp [sist besøkt 08.04.2022].

Thuv, Aa.; Farsund, B. H.; Hansen, B.J.; Enemo, G. (u.å); *Innspill til integrasjon av IKT i langtidsplanlegging;* under utarbeidelse.

Tortonesi, M.; Morelli, A.; Govoni, M.; Michaelis, J.; Suri, N.; Stefanelli, C.; Russell, S. (2016): *Leveraging Internet of Things within the military network environment—Challenges and solutions*; IEEE 3rd World Forum on Internet of Things (WF-IoT); s. 111-116.

Vatne, D.F; Køber, P.K.; Guttelvik, M.S.; Arnfinnsson, B.; Rise, Ø.R. (2020); *Norwegian long-term defence analysis – a scenario- and capability-based approach*; FFI-rapport 20/02367.

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

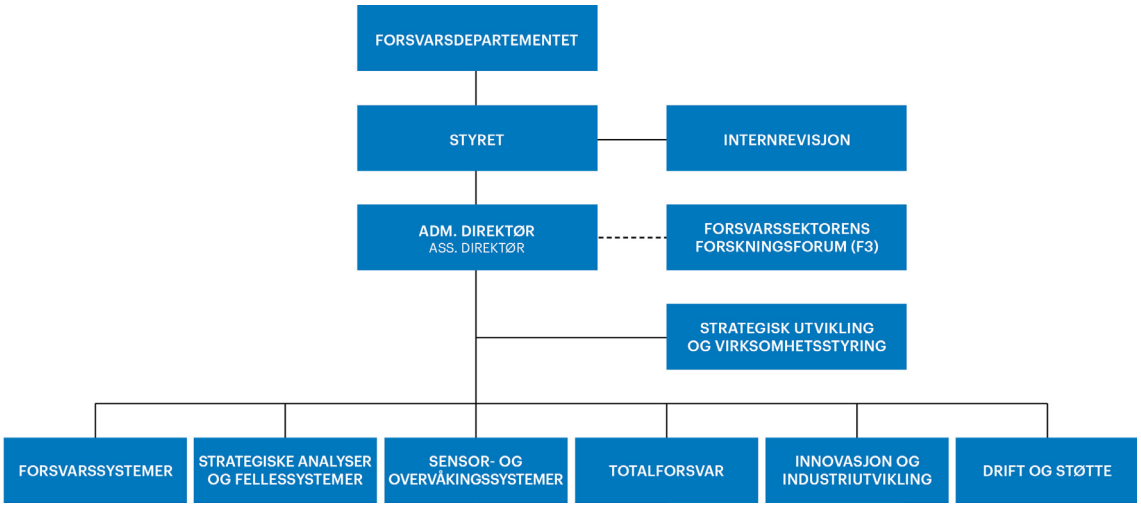
World Ecnomic Forum, *Fourth Industrial Revolution*; https://www.weforum.org/focus/fourth-industrial-revolution [sist besøkt 27.06.22].

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