FFI Forsvarets forskningsinstitutt

22/02237

FFI-RAPPORT

Sourcing for Forsvarets IKT-virksomhet

– skisse til rammeverk

Ann-Kristin Elstad
Monica Endregard
Anders Mykkeltveit

Sourcing for Forsvarets IKT-virksomhet – skisse til rammeverk

Ann-Kristin Elstad
Monica Endregard
Anders Mykkeltveit

Forsvarets forskningsinstitutt (FFI) 12. desember 2022

Emneord
IKT
Sourcing
Krigens folkerett
Digital kompetanse
Forsvarlig sikkerhetsnivå

FFI-rapport
22/02237

Prosjektnummer
1643

Elektronisk ISBN
978-82-464-3446-9

Engelsk tittel
Sourcing within the Norwegian Armed Forces' ICT organisation – a framework

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

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Strategisk samarbeid har fått økt oppmerksomhet i de siste tre langtidsperiodene. Forsvarsdepartementet har etablert prinsippet *så sivilt som mulig og så militært som nødvendig* for at Forsvaret skal kunne nyttiggjøre seg av både ressurser og kompetanse som finnes i næringslivet i større grad enn i dag. Prinsippet legger også til rette for at strategiske partnere ivaretar oppgaver der de er ledende.

Sourcing er en strategisk beslutning om hvorvidt en tjeneste skal utføres med interne ressurser eller om hele eller deler av tjenesten skal leveres som et tjenestekjøp eller samarbeid med ekstern virksomhet. Sourcing innen Forsvarets bruk av informasjons- og kommunikasjonsteknologi (IKT) er en komplisert problemstilling og det finnes ikke noe rammeverk som kan benyttes. Formålet med denne rapporten er å identifisere faktorer som bør tas hensyn til ved vurdering av sourcing for Forsvarets IKT-virksomhet og foreslå en skisse til rammeverk.

Vårt rammeverk baserer seg på transaksjonskostnadsøkonomi og ressursbasert teori som er de dominerende perspektivene på sourcing i litteraturen. Forsvarets forskningsinstitutt (FFI) har nylig utviklet en modell for valg av sourcingstrategi for Forsvaret. Vi har tatt utgangspunkt i denne modellen og utvidet den ved å knytte inn både spesielle forhold rundt IKT generelt, og IKT i Forsvaret spesielt. Identifisering av faktorer som må tas hensyn til ved sourcing har vært sentralt i arbeidet med denne rapporten. Vårt rammeverk består av syv faktorer det er viktig å dokumentere i beslutningsgrunnlag:

- operativt fortrinn
- forsvarlig sikkerhetsnivå
- krigens folkerett
- transaksjonskostnader
- kompetansebehov
- begrenset rasjonalitet
- risiko for opportunisme

Ved utarbeidelse av underlag til sourcing må det utarbeides ulike handlingsalternativer, slik som å utføre en tjeneste internt og ulike grader av å utsette tjenesten til eksterne. For hver faktor foreslår vi noen spørsmål som bør besvares i et beslutningsunderlag sourcing. Spørsmålene må besvares ut i fra de ulike handlingsalternativene. Faktorene er ikke direkte sammenlignbare. Det vil si at det ikke er mulig å benytte en kvantitativ sammenligning av de ulike handlingsalternativene. Årsaken til dette er at vurdering av nytte og effekt for hvert enkelt av handlingsalternativene vil kunne fremstå vanskelig og at de ulike faktorene kan ha ulik grad av kritikalitet.

Vårt rammeverk kan benyttes som en del av et underlag for å vurdere sourcing innen Forsvarets IKT-virksomhet. Rammeverket inneholder noen utvalgte momenter men er ikke uttømmende. I tillegg til å vurdere faktorene i vårt rammeverk, må et underlag ta hensyn til sivil parts leveranseevne i hele krisespekteret herunder hvordan innrette beredskapsordninger og avtaler knyttet til arbeidsplikt for sivil parts personell.

Summary

The last three long-term defence plans have placed increased awareness on the collaboration between the Norwegian defence sector and strategic partners. The Ministry of Defence has established the principle of being *as civilian as possible and as military as necessary.* It implies utilizing private sector resources and expertise and entering strategic partnerships for tasks where private entities have competitive advantages.

Sourcing is a strategic decision on whether a service is to be performed using internal resources or all/part of the service is to be delivered as a purchased service or in collaboration with an external partner. Sourcing within the defence sector's use of Information Communication Technology (ICT) activities is complicated. The objectives of this report are to identify factors that should be considered in sourcing within the Norwegian Armed Forces' ICT organisation and suggest a framework for a structured sourcing process.

Our argumentation is based on transaction cost economics and resource-based theory. Our framework is based on the "Model for choosing a sourcing strategy" developed by the Norwegian Defence Research Establishment. We have expanded the model by including conditions that apply to ICT in general and ICT in the Norwegian Armed Forces in particular. Our recommended framework comprises seven factors that are important to assess and document in the sourcing decision making process:

- operational advantage
- appropriate level of security
- the law of armed conflict
- transaction costs
- competence
- bounded rationality
- risk of opportunism

In sourcing, alternative sourcing constellations have to be established, for example whether a service can be performed with internal resources or whether all or part of the service can be delivered as a purchased service or in collaboration with an external partner. For each factor in the framework, we propose a set of questions. The answers to these questions should be included in decision basis material regarding sourcing in an ICT context. The resulting assessments for the seven factors are not directly comparable. Hence, it is not possible to use a quantitative comparison of the various alternatives. Assessing the usefulness and effects of each sourcing alternative may appear difficult. In addition, various factors can have different weights and degrees of criticality.

The proposed framework can be utilised in assessments regarding sourcing. The framework presents while not exhaustive, selected key factors to consider when sourcing ICT activities. In addition to assessing the questions asked here, the civil party's ability to deliver in the entire crisis spectrum, including how to set up emergency arrangements and agreements related to work obligations for civil party personnel must be considered.

Innhold

Forord

I 2021 etablerte Forsvarssjefen (FSJ) IKT-avdelingen i Forsvarsstaben (FST J6). FST J6 støtter FSJ innen strategisk styring av Forsvarets informasjons- og kommunikasjonsteknologi (IKT)-virksomhet. Forsvarets forskningsinstitutt (FFI) støtter FST J6 med råd og kunnskapsutvikling gjennom FFIs forskningsprosjekt 1643 «IKT for morgendagens forsvar – støtte til FST J6». Ett prioritert område for J6 i 2022 har vært å etablere en sourcingstrategi for IKT-virksomheten. Bakgrunnen for denne rapporten er å gi innspill til FST J6 angående sourcingstrategi.

Vi vil rette en meget stor takk til høgskolelektor og hovedlærer i operasjonell rett Espen Persønn Flagstad ved Forsvarets høgskole, Stabsskolen, for grundige og utfyllende muntlige og skriftlige svar på spørsmål og innspill til vår tekst om krigens folkerett.

Vi vil videre takke FFI-forsker Olger Pedersen for et godt samarbeid og nyttige diskusjoner underveis i skriveprosessen. Takk også til FFI-forskerne Gunn Alice Birkemo og Kjell Olav Nystuen for gjennomlesing og nyttige innspill underveis i skriveprosessen.

Kjeller, 1. november 2022

Ann-Kristin Elstad
Monica Endregard
Anders Mykkeltveit

1 Innledning

I de siste tre langtidsplanperiodene har strategisk samarbeid fått økt oppmerksomhet (Pedersen, 2022). I gjeldende langtidsplan for forsvarssektoren (LTP) står det om Cyberforsvaret at «Strategisk samarbeid med NATO, allierte, næringslivet og andre statlige virksomheter skal intensiveres for å legge til rette for raskere implementering av nye teknologiske muligheter» (Forsvarsdepartementet 2020, s. 108). I denne rapporten ser vi på en av disse fire typene strategiske samarbeid, nemlig samarbeid med næringslivet – da det er her vi finner mest kompetanse på IKT, og det er her hvor det synes enklest å etablere et leverandørforhold for Forsvarets IKT-virksomhet. Forsvarets IKT-virksomhet[1] er «[…] de personer og organisasjoner som produserer varer, tjenester eller utfører aktivitet innen utvikling, drift, vedlikehold og forvaltning av Forsvarets IKT; være seg Forsvarets og forsvarssektorens egne eller andre offentlige og private aktører» (Forsvarsstaben, 2021).

I Meld. St. 17 (2020–2021) «Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar» fremgår det at strategiske partnerskap mellom forsvarssektoren og næringslivet kan bidra til å sikre langsiktig tilgang til materiell, tjenester og kompetanse – samt å forbedre forsvarssektorens evne til å løse oppgaver ut fra prinsippet *så sivilt som mulig og så militært som nødvendig* (Forsvarsdepartementet, 2021c). Et sentralt mål for forsvarssektoren med en slik tilnærming er å sørge for at Forsvaret nyttiggjør seg sivil teknologi og kompetanse samt oppnår stordriftsfordeler. Dette gjøres ved å dra nytte av både ressurser og kompetanse som allerede finnes i næringslivet – samt at strategiske partnere ivaretar oppgaver der de er ledende (Forsvarsdepartementet, 2021c).

Moderne informasjons- og kommunikasjonsteknologi (IKT)-løsninger er «nødvendig for å understøtte operativ evne og for effektiv gjennomføring av virksomheten i forsvarssektoren». (Forsvarsdepartementet, 2020 s. 136). Samtidig peker flere dokumenter på problemer med å utnytte IKT maksimalt i Forsvaret (se, f.eks. Forsvarsdepartementet, 2019; Riksrevisjonen, 2022; Svendsen-utvalget, 2020). I IKT-strategien for forsvarssektoren er det identifisert en rekke utfordringer med å utnytte IKT i sektoren (Forsvarsdepartementet, 2019), og ett av tiltakene er å tydeliggjøre sourcingstrategien. Bakgrunn for tiltaket er at sektoren «mangler en plan for utnyttelse av eksterne tjenesteleveranser» innen IKT (Forsvarsdepartementet, 2019).

1.1 Formål og problemstilling

Formålet med denne rapporten er å identifisere faktorer som bør tas hensyn til ved vurdering av sourcing for Forsvarets IKT-virksomhet og foreslå en skisse til rammeverk. Sourcing er en strategisk beslutning om hvorvidt en tjeneste kan utføres med interne ressurser eller om hele eller deler av tjenesten kan leveres som et tjenestekjøp eller samarbeid med ekstern virksomhet.

[1] Se også kapittel 2.1 om bruk av IKT i Forsvaret og kapittel 2.2 IKT-virksomheten i Forsvaret og sektoren for øvrig.

Problemstillingen har blitt aktualisert blant annet gjennom virksomhetsprogrammet «Militær anvendelse av skytjenester (MAST)» der forsvarssektoren er i ferd med å anskaffe en strategisk partner for IKT-leveranser (Forsvarsmateriell, 2022). *Strategisk partnerskap* eksisterer når to eller flere uavhengige organisasjoner samarbeider i utvikling, produksjon eller salg av produkter og tjenester (Barney, 2002). En *strategisk partner* kan derfor forstås som en organisasjon Forsvarets IKT-virksomhet har inngått strategisk partnerskap med (se ellers kapittel 2.4).

Rapporten bygger på et forskningsarbeid fra FFI om valg av sourcingstrategi i Forsvaret (Pedersen, 2022), heretter forkortet modell for valg av sourcingstrategi. I det nevnte forskningsarbeidet bidrar FFI til å øke kompetanse og bevissthet rundt valg av sourcingstrategi i Forsvaret, i tillegg til et metodisk bidrag til valg av sourcingstrategi basert på en omfattende litteraturstudie. Forskningsarbeidet danner også grunnlaget for videre studier av sourcingstrategier i Forsvaret og forsvarssektoren. I vår studie tar vi derfor utgangspunkt i tidligere FFI-forskning og tilpasser tilnærmingen med momenter som etter vårt syn er viktige for sourcing innen IKT-virksomheten.

Det ligger en rekke ikke-kontrollerbare variabler[2] til grunn for en avgjørelse om sourcing, for eksempel ivaretakelse av nasjonale sikkerhetsinteresser (jf. Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven) med forskrifter) og hensynet til krigens folkerett. Det ligger også et overordnet styringsprinsipp til grunn, som allerede nevnt: *så sivilt som mulig og så militært som nødvendig.* I tillegg går den teknologiske utviklingen i tydelig retning mot økt kompleksitet med mange aktører og et fragmentert systemansvar. Resultatet vil være en rekke beslutningsvariabler og ikke-kontrollerbare variabler som kan danne utgangspunkt for hva som er kritisk å ta hensyn til ved sourcing.

1.2 Bidrag, målgruppe og avgrensning

Rapporten bidrar med faglige innspill til IKT-avdelingen i Forsvarsstaben (FST J6) sitt arbeid ved vurdering av strategisk samarbeid for Forsvarets IKT-virksomhet og ved utvikling av en sourcingstrategi for denne virksomheten. Basert på modell for valg av sourcingstrategi foreslår vi syv faktorer som bør tas hensyn til ved sourcing innen IKT. For hver av faktorene foreslår vi spørsmål som bør stilles, analyser som må til for å svare ut disse spørsmålene samt at vi diskuterer hvilke konsekvenser de ulike svarene på spørsmålene har for sourcingstrategien. Vi foreslår ikke konkrete handlingsalternativer[3] eller en nedbryting av aktivitetene som inngår i Forsvarets IKT-virksomhet.

Vårt rammeverk kan benyttes som en del av et underlag for sourcing innen Forsvarets IKT. Rapporten presenterer noen utvalgte tema vi mener bør vurderes og spørsmål som bør besvares i

[2] Problemstillingen har en rekke variabler vi kaller ikke-kontrollerbare variabler, det vil si rammebetingelser og føringer som ligger til grunn og ikke kan endres.

[3] For en beslutning ligger det ulike løsningsforslag – såkalte handlingsalternativer til grunn. Et handlingsalternativ inneholder en begrunnelse og redegjørelse, inkludert fordeler og ulemper ved valg av alternativet. Dvs. at handlingsalternativene har ulike løsningsforslag for beslutningen. Ett handlingsalternativ kan være å sette ut all IKT-drift til ekstern partner, og et annet kan være å beholde all IKT-drift internt. I mellom disse ytterpunktene av handlingsalternativer finnes det en rekke ulike løsninger, hvor hver av løsningene angir et handlingsalternativ.

et beslutningsgrunnlag, men selve vurderingen av hvert enkelt av disse momentene må gjøres av beslutningstakere i sektoren, inkludert hvilke deler av IKT-porteføljen som må tas hånd om internt i sektoren og hva som potensielt kan settes ut til en strategisk partner fra næringslivet.

Målgruppen for rapporten er primært FST J6. I tillegg kan personell som jobber med beslutninger knyttet til problemstillingen, for eksempel i program MAST, ha nytte av rapporten.

2 Bakgrunn og begrepsavklaringer

Dette kapittelet tar for seg bakgrunn og sentrale begreper som benyttes i rapporten. Først gis en kort introduksjon til bruk av IKT i Forsvaret og til Forsvarets IKT-virksomhet. Deretter følger begrepsavklaringer knyttet til verdistrømmer og digitale verdikjeder. Videre diskuteres begrepene sourcing og samarbeidsformer samt begreper knyttet til strategisk samarbeid. Det presenteres to teoretiske grunnlag for sourcing. Det siste kapittelet handler om digital kompetanse.

2.1 Bruk av IKT i Forsvaret

IKT er «en samlebetegnelse for teknologi for innhenting, overføring, bearbeiding, lagring og presentasjon av informasjon» (Store norske leksikon, 2019). IKT-utviklingen går raskt, og IKT er innebygget i produkter, tjenester, forholdet til ulike interessenter og i arbeidsprosesser (Paré et al., 2020). IKT brukes i hele spennet av aktiviteter Forsvaret gjennomfører – fra tilretteleggende virksomhet til utførelse av kjernevirksomhet. Det vil si at Forsvaret benytter IKT i det daglige til «kontorbruk» tilsvarende en vanlig sivil bedrift eller offentlig foretak, samtidig som IKT inngår som en integrert og uunnværlig del av evnen til å gjennomføre militære operasjoner.

De teknologiske endringene som skjer former organisasjoner og arbeidsprosesser, og skaper nye utfordringer som må håndteres (Cortellazzo et al., 2019). Valg og strategi rundt IKT kan derfor potensielt påvirke hvordan Forsvaret løser oppgavene sine. Ofte kan det være vanskelig å skille ut IKT fra selve gjennomføringen av en aktivitet, slik at IKT blir en nødvendig betingelse for at Forsvaret kan være i stand til å utføre aktiviteter som en del av kjernevirksomheten.

Deler av den IKT-en som benyttes i militære operasjoner skiller seg fra IKT i andre virksomheter. Dette skyldes blant annet at noe IKT må spesialtilpasses til Forsvarets anvendelser for å oppnå tilstrekkelig robusthet og sikkerhet i hele krisespekteret. To eksempler på spesialtilpasset IKT som Forsvaret benytter er a) kommando- og kontrollsystemer og våpensystemer som kommuniserer via taktiske datalinker og b) radioer som er spesialutviklet for kommando og kontroll. Den store variasjonen innen IKT i Forsvaret har implikasjoner blant annet for kompetansebehov, noe vi kommer tilbake til i kapittel 2.7.

En del informasjon i Forsvaret er sikkerhetsgradert fordi det kan skade rikets sikkerhet dersom uvedkommende får tak i informasjonen. Slik informasjon må behandles på skjermingsverdige IKT-systemer, og dette medfører at det stilles spesielle krav til sikkerhetsgodkjenning av IKT-systemer jf. sikkerhetsloven. Dette kommer vi tilbake til i kapittel 3.

Et enkelt IKT-system er satt sammen av både maskinvare og programvare. Programvaren kan være satt sammen av drivere, operativsystem og applikasjoner. Når en bruker benytter seg av IKT er det ofte flere ulike systemer involvert som kan befinne seg på ulike geografiske lokasjoner koblet sammen gjennom et kommunikasjonsnettverk. For eksempel kan programvare på en PC benytte informasjon som er lagret på en server som nås via et internt kommunikasjonsnettverk eller via Internett. Ulike IKT-systemer er dermed koblet sammen og avhengige av hverandre og danner såkalte digitale verdikjeder og verdistrømmer. Dette diskuterer vi videre i kapittel 2.3.

2.2 Forsvarets IKT-virksomhet

IKT-virksomheten er ifølge Forsvarets IKT-strategi (Forsvarsstaben, 2021)

> […] de personer og organisasjoner som produserer varer, tjenester eller utfører aktivitet innen utvikling, drift, vedlikehold og forvaltning av Forsvarets IKT; være seg Forsvarets og forsvarssektorens egne eller andre offentlige og private aktører.

Når vi i denne rapporten skal skille mellom intern og ekstern utførelse av tjenester, definerer vi intern utførelse som at tjenesten leveres av personell ansatt i forsvarssektoren. Hoveddelen av Forsvarets IKT-virksomhet er i dag håndtert av Forsvarsmateriell (FMA) IKT-kapasiteter og Cyberforsvaret. FMA IKT-kapasiteter «har ansvaret for å planlegge, anskaffe og forvalte materiell som utruster Forsvaret med sikre kommunikasjonsløsninger» (Forsvarsmateriell, u.å.), mens Cyberforsvaret «etablerer, drifter og beskytter Forsvarets kommunikasjonssystemer og digitale infrastruktur» (Forsvaret, u.å.). I tillegg driftes noe IKT av avdelingene selv, slik som Hæren gjør med sitt eget sambandsmateriell. I tillegg til den IKT som Forsvarets IKT-virksomhet håndterer er også IKT integrert i mange av Forsvarets andre systemer som våpenplattformer. Disse systemene tas hånd om av de enkelte forsvarsgrenene (som Hæren, Sjøforsvaret og Luftforsvaret).

2.3 Digitale verdikjeder

I denne delen av rapporten starter vi med en forklaring av hva vi legger i verdi- og effektbegrepene før vi går nærmere inn på verdikjeder generelt og digitale verdikjeder.

2.3.1 Verdibegrepet

Grunnet den raske utviklingen blir det stadig vanskeligere å definere hva merverdien av IKT er og hva den bør være, siden IKT i dag er innebygget i produkter, tjenester, forholdet til ulike interessenter og i arbeidsprosessene (Paré et al., 2020). IKT-en i seg selv isolert sett skaper ikke

verdi, det er den bevisste målrettede anvendelsen som er med på skape en verdi for organisasjonen (se, f.eks. Elstad et al., 2022).

I en forsvarskontekst kan verdien av IKT ses gjennom et hierarki av evner eller verdier som knytter IKT til Forsvarets oppgaver og primære formål, som er ivaretakelse av nasjonal sikkerhet. Verdien vil i denne sammenhengen si noe om fordelen, viktigheten og kritikaliteten av IKT for å oppnå mål.[4] Videre er det slik at en organisasjon må ha ulike former for evner for å kunne være i stand til å ivareta de ulike verdiene.

> Eksempler på overordnede verdier er nasjonale sikkerhetsinteresser, liv og helse, omdømme, kompetanse og leveranser. Verdier knyttet til IKT i en organisasjon sier noe om viktigheten, kritikaliteten og fordelen IKT gir, både internt og eksternt, for at organisasjonen skal oppnå sine mål og opprettholde og beskytte overordnede verdier.

2.3.2 Effektbegrepet

Effekt er et annet begrep som det er nødvendig å tydeliggjøre. Effekt tilsier en eller annen form for endring i en tilstand. Denne forandringen i tilstand kan ha flere årsaker, for eksempel en handling eller et tiltak.

> Effekt vil si noe om en forandring i tilstand hos brukerne, organisasjonen eller samfunnet som har oppstått på bakgrunn av en handling, tiltak eller endring (se, f.eks. Direktoratet for økonomistyring, 2014; Senter for statlig økonomistyring, 2010).

Effekt er dermed noe annet enn en verdi. Verdi sier noe om fordelen, kritikaliteten og viktigheten av IKT for at organisasjonen kan nå sine mål, mens effekten er tilstandsendringen grunnet handlingsvalg. Operativ effekt vil derfor si tilstandsendringen som oppstår i Forsvarets virksomhet grunnet et handlingsvalg som gjennomføres.

2.3.3 Verdikjeder

Porter[5] beskriver en verdikjede som en organisasjons verdiskapningsprosesser, og foreslo i sin tid at en verdikjede består av to hovedkategorier, nemlig primær- og støtteaktiviteter (basert på Barney, 2002). Primæraktiviteter er de aktivitetene i en organisasjon som skaper verdi, og kan være knyttet til inngående logistikk, drift og produksjon, utgående logistikk, markedsføring og salg samt service. I Forsvaret kalles disse primæraktivitetene for Forsvarets kjernevirksomhet. Dette er strategisk viktige aktiviteter, eller aktiviteter nært tilknyttet til disse, som med mangelfull utføring vil få store konsekvenser. Støtteaktivitetene er de aktivitetene som er nødvendige forutsetninger for at primæraktivitetene skal skape verdi, eksempelvis knyttet til ulike former

[4] For flere detaljer om verdibegrepet, se Elstad et al., 2018; Endregard et al., under arbeid; Sagdahl, 2019).
[5] Michael Porter er professor ved Harvard, og er kjent for sine teorier innenfor bl.a. økonomi og forretningsstrategi.

for anskaffelser og infrastruktur (Barney, 2002). Støtteaktiviteter i Forsvaret omtales gjerne som tilretteleggende virksomhet (de øvrige aktivitetene).

2.3.4 Digitale verdikjeder

De digitale verdikjedene øker stadig i omfang og kompleksitet og kan gjerne strekke seg over flere sektorer og landegrenser. Vår forståelse av digitale verdikjeder baseres på en rapport fra en arbeidsgruppe ledet av professor Lysne «Risikostyring i digitale verdikjeder» (2020 s. 10).

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

Rapporten fra Lysne (2020 s. 13) benytter fremtidens Nødnett som et eksempel på en digital verdikjede. Eksempelet tar utgangspunkt i at realiseringen skjer ved hjelp av kommersielle tilbydere, som er avhengig av andre, eksempelvis regionale nettleverandører som 5G-basestasjoner er koblet til. De regionale tilbyderne er igjen avhengig av at det landsdekkende nettet de er tilkoblet fungerer, for å kunne levere de tjenestene de skal. Ulike former for systemer samvirker med basestasjonene, og disse systemene må fungere for at 5G-nettet kan fungere, eksempelvis kundedatabaser og styringssystemer. Som vi ser av eksempelet er det komplekse sammenhenger av ulike elementer innen IKT som er vanskelig å skille fra hverandre. Som Lysne (2020 s. 10) fremhever:

> Enkelte tjenester, som internettilgang og transmisjonsfunksjonaliteten i ekom-nettet, inngår i svært mange slike verdikjeder, uten at de ansvarlige for disse tjenestene selv nødvendigvis har oversikt over hvilke samfunnsfunksjoner de er bærere av.

2.4 Sourcing og samarbeidsformer

I denne delen av rapporten forklarer vi hva vi legger i ulike begreper knyttet til samarbeid. Vi starter først med *sourcing*, etterfulgt av *outsourcing* og avslutningsvis introduserer vi ulike former for *samarbeid*, herunder strategisk samarbeid.

2.4.1 Sourcing

Sourcing som begrep står sentralt i denne rapporten, og det er derfor av betydning at vi klargjør hva vi legger i dette begrepet og hva forskjellen er på sourcing og outsourcing (beskrives i kapittel 2.4.2).

Direktoratet for forvaltning og økonomistyring (DFØ) definerer sourcing som «Dei strategiske vala omkring kva tenester du skal sette ut til eksterne, og kva tenester verksemda di skal utføre sjølv» (www.anskaffelser.no). DFØ sier at organisasjonen kan ta utgangspunkt i to sentrale spørsmål ved utarbeidelse av en sourcingstrategi. Det første spørsmålet handler om hvor strategisk viktig tjenesten er for organisasjonen. Det andre spørsmålet handler om det finnes et velfungerende marked med leverandører som tilbyr den tjenesten til en konkurransedyktig pris.

> Sourcing er en strategisk beslutning om hvorvidt en tjeneste skal utføres med interne ressurser eller om hele eller deler av tjenesten skal leveres som et tjenestekjøp eller samarbeid med ekstern virksomhet.

Sourcing er altså den strategiske beslutningen som skjer i forkant av kjøp av tjenester. I forkant av den strategiske beslutningen utarbeides det ulike handlingsalternativer, med begrunnelse og redegjørelse, inkludert fordeler og ulemper ved valg av alternativet. Eksempelvis kan overordnede handlingsalternativer være (1) intern utførelse av tjenesten, (2) tjenesten leveres som et tjenestekjøp (transaksjonsbasert), (3) tjenesten leveres gjennom samarbeid med ekstern virksomhet og (4) selve tjenesten eller aktiviteten elimineres, det vil si utføres ikke lenger. Inkludert i disse fire ulike handlingsalternativene er det en rekke vurderinger som gjøres, som til sammen danner grunnlaget for hvert enkelt handlingsalternativ.

2.4.2 Outsourcing

Outsourcing handler om å betale andre organisasjoner til å gjennomføre én eller flere tjenester på vegne av organisasjonen. Sourcing er dermed den strategiske beslutningen om hele eller deler av aktiviteten skal leveres av eksterne leverandører, mens outsourcing er selve prosessen (etter at den strategiske beslutninger er tatt) hvor eksterne leverandører leverer én eller flere tjenester innenfor de gitte rammene.

> Outsourcing er en prosess der en organisasjon etablerer et leverandørforhold til en annen organisasjon som utfører en funksjon eller tjeneste som tidligere ble utført internt innenfor gitte rammer.

Det å sette ut tjenester eller aktiviteter til eksterne leverandører har vært en trend de siste tiårene (Lahiri et al., 2022). Mange bedrifter benytter seg av outsourcing innen IKT, men det har også vært rapportert om økende grad av *insourcing*, det vil si at bedrifter som tidligere har outsourcet IKT tar tilbake hele eller deler av IKT-porteføljen sin. En undersøkelse fra industrien i 2022 indikerer at litt flere bedrifter vurderer å benytte seg av outsourcing enn av insourcing (Lystad, 2022). En undersøkelse fra Ernst & Young indikerer at de fleste bedrifter ikke ønsker å outsource aktiviteter som krever unike eller spesialiserte ferdigheter, mens aktiviteter som gjelder mer standardiserte tjenester i større grad outsources (Ernst & Young, 2019).

2.4.3 Grad av samarbeid – ulike leverandørperspektiv

Leverandørforhold kan grovt deles inn i transaksjonsbaserte og samarbeidsbaserte leverandørforhold. I virkeligheten er dette et samarbeidsspekter hvor ulike grader av samarbeid kan benyttes, som illustrert i figur 2.1.

Figur 2.1 Samarbeidsspekter for leverandørforhold, basert på Pedersen (2022 figur 5.1).

Transaksjonsbaserte leverandørforhold handler gjerne om produkter og tjenester med lav kritikalitet for kjøperen og preges gjerne av standardiserte produkter og tjenester med lite kundetilpasning. Disse er gjerne kostnadsdrevet og av kortsiktig art. Samarbeidsbaserte leverandørforhold har kjennetegn som gjensidighet, deling av ressurser, risiko og gevinster som til sammen vil oppnå større nytte enn de ville gjort i isolasjon hver for seg. Det vil si at informasjonsdeling og koordinering er sentralt i et samarbeidsbasert leverandørforhold. En slik tilnærming benyttes gjerne ved kritiske eller strategisk viktige innkjøp.

Sourcing, det vil si den strategiske beslutningen, fører til en avgjørelse om hvorvidt en tjeneste skal utføres med interne ressurser eller om hele eller deler av tjenesten skal leveres som et tjenestekjøp eller gjennom et samarbeid med ekstern virksomhet. Den strategiske beslutningen kan være å outsource enkelte tjenester, som for eksempel brukerstøtte. Da har en leverandør ansvaret for å gjennomføre tjenesten, her brukerstøtte, innenfor gitte rammer fra kunden. Graden av samarbeid mellom kjøper og leverandør er i dette eksempelet tettere enn ved et transaksjonsbasert leverandørforhold, men lavere enn ved et fullstendig strategisk samarbeidsforhold. Ved inngåelse av strategisk partnerskap er det en gjensidig avhengighet mellom partene og det er en høy grad av informasjonsdeling. Strategisk partnerskap er en form for samarbeidsbasert leverandørforhold. Forsvarets IKT-strategi (Forsvarsstaben, 2021) skriver følgende om partnerskap:

> Partnerskap skal benyttes strategisk og langsiktig for å utnytte muligheter i den sivile industrien og akademia for rådgiving, innovasjon, utvikling, drift og vedlikehold av IKT, etter en modell som kan benyttes i hele krisespekteret.

Vi ser her at kjennetegnene *langsiktighet og strategisk* går igjen både i IKT-strategien og i samarbeidsspekteret.

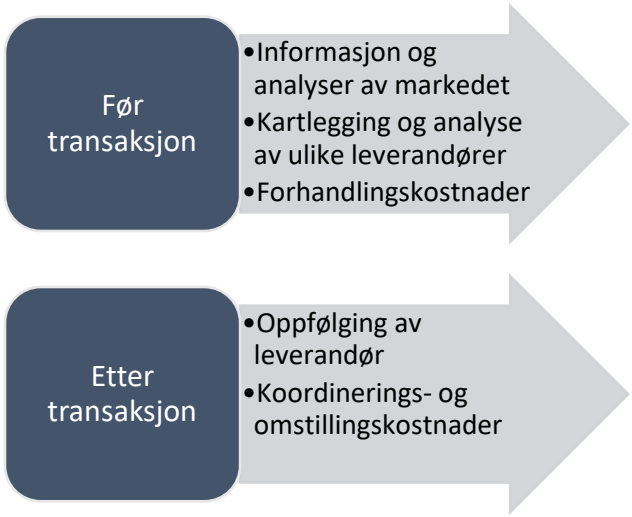
> Strategisk partnerskap eksisterer når to eller flere uavhengige organisasjoner samarbeider i utvikling, produksjon eller salg av produkter og tjenester (Barney, 2002).

2.5 Transaksjonskostnadsøkonomi

Transaksjonskostnadsøkonomi (TCE) er én av teoriene som har dominert innen forskning på outsourcing (Jansson et al., 2021). I dette kapittelet vil vi derfor gi en overordnet innføring i TCE og knytte teorien opp mot relevante problemstillinger en organisasjon må ta hensyn til sett fra et TCE-perspektiv ved vurdering av de ulike handlingsalternativene som ligger til grunn for valget av sourcingstrategi.

2.5.1 Transaksjonskostnader

Ved TCE står transaksjonskostnader sentralt, men hva er det egentlig? Transaksjonskostnader er de kostnadene en organisasjon har i forbindelse med å organisere, gjennomføre og følge opp en transaksjon eller handel. Det vil forekomme transaksjonskostnader før og etter at en transaksjon er gjennomført, som illustrert i figur 2.2.



Figur 2.2 Transaksjonskostnader før og etter en transaksjon.

Før en transaksjon vil det kunne forekomme en rekke ulike kostnader, for eksempel:

- kostnader til informasjon og analyse av markedet, inkludert hvilke potensielle leverandører som kan ivareta de behovene organisasjonen skal dekke ved gjennomføring av transaksjonen

- kostnader i forbindelse med kartlegging og analyse av ulike leverandører med tanke på omdømme, leveringskvalitet også videre

- forhandlingskostnader

Etter at selve transaksjonen er gjennomført vil det forekomme transaksjonskostnader knyttet til

- oppfølging av leverandør samt

- interne koordinerings- og omstillingskostnader.

Ved en intern produksjon eller prosess vil ikke transaksjonskostnader forekomme, siden kostnadene ved en intern produksjon er knyttet til produksjonskostnader.

I følge Williamson (1979) er de tre kritiske aspektene ved en transaksjon (1) usikkerhet, (2) frekvens og hyppighet samt (3) transaksjonsspesifikke investeringer.

Usikkerhet i denne sammenheng er knyttet til ulike elementer ved transaksjonen, hvor det er manglende eller ufullstendig informasjon. Et eksempel på usikkerhet i kontekst av denne rapporten er knyttet til tempoet i IKT-utvikling. Usikkerhet vil også være knyttet til fremtidige leveranser fra potensielle strategiske partnere, ved at organisasjonen ikke vet hva leverandører kan levere om noen år. I tillegg vil usikkerhet inngå i atferdsmessige mekanismer, som beskrives i kapittel 2.5.2. Det vil også være ulike former for usikkerhetsmomenter ved faktorer som nasjonal sikkerhet, forsvarlig sikkerhetsnivå og krigens folkerett (se kapittel 3). I tillegg er det en rekke andre ikke-kontrollerbare variabler som vil innvirke på usikkerhet, som den sikkerhetspolitiske situasjonen, klima og miljø samt andre uforutsette hendelser. Frekvens og hyppighet inngår også som et kritisk aspekt ved en transaksjon, og sier noe om hvor ofte en transaksjon gjennomføres.

Ved transaksjonsspesifikke investeringer eksisterer det leverandør- og kundetilpassede ressurser, som kan miste hele eller deler av sin verdi dersom kundeforholdet opphører (Barney, 2002). Leverandør kan etablere et miljø for å drifte og utvikle et proprietært, gjerne gammelt, IKT-system som kun brukes av det norske Forsvaret. Hvis Forsvaret sier opp avtalen kan leverandøren i liten grad benytte kompetansen til å levere tjenester til andre organisasjoner. For IKT-virksomheten vil Forsvaret ha en del transaksjonsspesifikke investeringer for å oppnå tilstrekkelig robusthet og sikkerhet i hele krisespekteret.[6] Dersom sivile forutsettes å bidra til at slike funksjoner utføres i en væpnet konflikt, må det vurderes om de konkrete funksjonene innebærer direkte deltakelse i fiendtlighetene eller ikke, fordi det kan komme i konflikt med folkeretten. Dersom det handler om leveranser som militært personell i forsvarssektoren selv deretter utfører, uten direkte bidrag fra sivil part, stiller det seg nok annerledes. I tillegg kan dette også knyttes sammen med spesifikke behov for kompetanse, som vi kommer tilbake til i

[6] F.eks. ved spesialtilpassing av materiell, utstyr, programvare i kommando- og kontrollsystemer.

kapittel 2.7. Standardiserte produkter eller tjenester vil ikke på samme måte som transaksjonsspesifikke investeringer miste hele eller deler av sin verdi. Standardiserte produkter innen IKT, såkalt hyllevare, har altså lav spesifisitet.

2.5.2 Atferdsmessige mekanismer

To atferdsmessige mekanismer ligger til grunn for TCE, nemlig *begrenset rasjonalitet* og *opportunisme*. I dette kapittelet vil vi kort gå inn på disse begrepene og setter de inn i konteksten til denne rapporten.

Begrenset rasjonalitet

I litteraturen om rasjonelle beslutninger antas det, ifølge March (1994), at beslutningstakerne har perfekt kunnskap for beslutninger ved at (1) alle handlingsalternativer er kjent, (2) alle konsekvenser ved alternativene er kjent samt (3) alle preferanser til valg av handlingsalternativ er kjent, presist, konsistent og stabilt. Det vil si at en aktør tar fullstendig rasjonelle valg basert på alternativer, forventninger, preferanser og beslutningsregler.

Beslutningstakere kan ikke imøtekomme disse kravene til rasjonelle beslutninger, dette inkluderer også sourcing. Mennesker har kognitive begrensninger i håndtering av informasjonsmengden som en rasjonell tilnærming krever. Som vi var inne på under digitale verdikjeder har disse et omfang og en kompleksitet som kan strekke seg over flere sektorer og landegrenser. Beslutningstakere har begrensninger ved for eksempel oppmerksomhet, lagring av informasjon og sammenligning av informasjon. Vi har ofte relevant informasjon, men feiler å se at den er relevant.

Begrenset rasjonalitet vil være en faktor som påvirker valg av handlingsalternativer ved strategiske beslutninger. Valg som mennesker tar kan derfor være tilfredsstillende, men ikke ideelle. Sett i sammenheng med utarbeidelse av handlingsalternativer for komplekse avtaler, vil handlingsalternativene ta utgangspunkt i det beslutningstakerne vet, og innebefatter scenarioer beslutningstakerne kan se for seg. Forskjellige grupper av mennesker bruker forskjellig rammeverk for å forenkle verden. Vi har derfor begrenset kapasitet til å kommunisere og dele kompleks informasjon på tvers av kulturer og fagområder (March, 1994). Ved inngåelse av komplekse avtaler vil begrenset kognitiv kapasitet inngå som en faktor, ved at misforståelser og konflikter kan oppstå grunnet ulikt rammeverk for å forenkle verden.

Opportunisme

Den andre atferdsmessige mekanismen vi skal se på er opportunisme. Opportunisme eksisterer når en av partene i en transaksjon utnytter sårbarhetene til transaksjonspartneren (Barney, 2002). Opportunisme vil si at aktørene handler ut fra egen interesse fremfor å ta hensyn til transaksjonspartnerens interesser.

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

kompleksitet i en transaksjon er stor, er trusselen for opportunisme også stor (Barney, 2002). Trusselen for opportunistisk atferd vil på samme måte også kunne øke dersom det kun er én leverandør i markedet, ved at denne har enerett, og ingen reelle konkurrenter i markedet.

Det vil alltid være en viss risiko for opportunisme, men risikoen for opportunisme vil reduseres når partene vil oppfatte at en opportunistisk atferd er for kostbar (Barney, 2002). For å unngå opportunistisk atferd fra en av kontraktspartene, er det behov for en gjensidig avhengighet mellom dem for å unngå en skjev maktbalanse. Et tett samarbeid mellom partene kan være et initiativ for å få best mulig kontroll på transaksjonen, og gjennom dette håndtere potensielle muligheter for opportunisme.

2.6 Ressursbasert teori

Vi har til nå gått gjennom TCE, et perspektiv som tar utgangspunkt i kostnader knyttet til transaksjonen som skal gjennomføres. Ressursbasert teori (RBV) er en annen av teoriene som har dominert innen forskning på outsourcing (Lahiri et al., 2022). RBV tar utgangspunkt i organisasjonen og overordnet velges handlingsalternativer ut fra en vurdering av hvordan organisasjonens ressurser har innvirkning på konkurransefortrinn. Det vil si at de ressurser som er strategisk viktige for at organisasjonen kan oppnå konkurransefortrinn kan beholdes internt i organisasjonen, mens resterende ressurser kan være fra for eksempel en strategisk partner.

2.6.1 Hva er en ressurs?

Barney (1991) beskriver ressurser som:

> Firm resources include all assets, capabilities, organizational processes, firm attributes, information, knowledge, etc. controlled by a firm that enable the firm to conceive of and implement strategies that improve its efficiency and effectiveness (Daft, 1983). In the language of traditional strategic analysis, firm resources are strengths that firms can use to conceive of and implement their strategies (Learned, Christensen, Andrews, & Guth, 1969; Porter, 1981). (Barney, 1991 s. 101).

Vi kan se av definisjonen at Barney (1991) vektlegger ressurser som en styrke. Imidlertid kan det også hende at ressursene ikke er en styrke, men en svakhet, noe som ble påpekt tidlig av Wernerfelt (1984):

> By a resource is meant anything which could be thought of as a strength or weakness of a given firm. More formally, a firm's resources at a given time could be defined as those (tangible and intangible) assets which are tied semipermanently to the firm (see Caves, 1980).» (Wernerfelt, 1984 s. 172).

2.6.2 Fire forskjellige ressurskategorier

Overordnet kan ressurser deles inn i fire forskjellige kategorier (Barney, 2002):

1. *Finansielle* ressurser – som inkluderer all form for pengestrøm i organisasjonen.

2. *Fysiske* ressurser – som organisasjonens utstyr, råmateriale, inventar også videre. Eksempler her kan være både programvare og maskinvare som organisasjonen innehar, i tillegg til ulike bygningsmasser og kampplattformer.

3. *Menneskelige* ressurser sett fra et individnivå – disse ressursene inkluderer opplæring, kompetanse, erfaring, vurdering, relasjoner, innsikt, holdninger, osv.

4. *Organisatoriske* ressurser – som består av en samling av de individuelle ressursene. Eksempler på organisatoriske ressurser er formelle strukturer knyttet til rapportering og virksomhetsstyring, formell og uformell planlegging, kontroll, koordinering, kultur, omdømme og uformelle relasjoner mellom grupper.

2.6.3 Konkurransefortrinn for ulike ressurskategorier

IKT brukes som nevnt ofte om fysiske ressurser, fra den digitale grunnmuren, til IT-plattform, IT-infrastruktur og kommunikasjon til brukernært utstyr som PC-er og skjermer. Samtidig kan ikke IKT kun ses på som en type fysisk ressurs. IKT bør ses i sammenheng med de andre ressurskategoriene. Eksempelvis bør organisasjonen ha mulighet til å dele informasjon på tvers av organisatoriske grenser og menneskene som benytter IKT-løsningene vil være avgjørende for hvor vellykket anvendelsen av IKT-en blir. IKT er derfor koblet til alle de andre ressurskategoriene, og helheten på tvers av ressurskategoriene kan potensielt avgjøre om organisasjonen har et konkurransefortrinn eller ikke.

Det at en ressurs er *sjelden* og *verdifull* er nødvendige, men ikke tilstrekkelige betingelser for å oppnå konkurransefortrinn. Hvis ressursene samtidig *verken er imiterbare, substituerbare* og *overførbare*, kan de skape vedvarende konkurransefortrinn for organisasjoner (Priem & Butler, 2001).

Sett i en IKT-kontekst er ikke fysiske ressurser i form av sjeldent og verdifullt IKT-utstyr tilstrekkelige betingelser for at IKT skaper konkurransefortrinn. IKT som et rasjonaliseringsverktøy vil potensielt skape effekter som reduserte transaksjons- og investeringskostnader, for eksempel reduserte overføringskostnader eller redusert behov for arbeidskraft, bygninger eller lagerplass (Elstad et al., 2022), men vil altså i seg selv ikke skape konkurransefortrinn.

For å oppnå konkurransefortrinn[7], handler det om å se på IKT som mer enn et rasjonaliseringsverktøy og hjelpemiddel. Forsvaret må også være i stand til å gjøre de riktige tingene, gjennom bedre styring, mer effektiv kommunikasjon og informasjonsdeling samt bedre beslutningsstøtte (Elstad et al., 2022). Det å gjøre de riktige tingene inkluderer andre ressurskategorier i tillegg til den fysiske, som menneskelige og organisatoriske ressurser. Det er ikke alltid slik at IKT-en i seg selv er sjelden eller verdifull, men det er hvordan lederne utnytter systemet som avgjør om

[7] Vi vurderer at begrepet «konkurransefortrinn» ikke vil være gjenkjennelig for aktører i forsvarssektoren og foreslår i stedet å benytte begrepet «operativt fortrinn» i denne sammenheng. Se kapittel 4.2.1.

det blir et konkurransefortrinn eller ikke ved å sørge for at ressurser *verken er imiterbare, substituerbare* eller *overførbare* til andre organisasjoner.

2.6.4 Ressurser i verdikjeden

Som tidligere nevnt i kapittel 2.3.3 består en verdikjede av ulike aktører som er gjensidig avhengige av hverandre gjennom prosesser og aktiviteter som samlet kan bidra til at verdikjeden leverer mest mulig verdi og skaper en effekt hos aktøren lengst nedstrøms i kjeden. For hvert av stegene i verdikjeden er det typisk assosiert ressurser knyttet til alle de fire ressurskategoriene, finansielle, fysiske, menneskelige og organisatoriske ressurser.

Barney (2002) fremhever at den økte risikoen for opportunisme er en type kostnad organisasjonen må være villig til å ta for å skaffe tilgang til nødvendige ressurser eksternt, som er for kostbare å anskaffe internt. I denne konteksten vil det si at organisasjonen må vurdere om det er forsvarlig å sette ut aktiviteter til en ekstern leverandør, dersom man selv ikke er i stand til å utføre aktiviteten på en slik måte at den bidrar til konkurransefortrinn. Dette kan ses i sammenheng med prinsippet om så sivilt som mulig, så militært som nødvendig. Dersom organisasjonen har aktiviteter som den selv ikke kan gjennomføre på en slik måte at man oppnår konkurransefortrinn, bør aktiviteten settes ut til en organisasjon som har konkurransefortrinn innen dette området. Det vil si at dersom en organisasjon har områder eller aktiviteter med manglende kompetanse, kapasitet, teknologi også videre, kan en organisasjon ved hjelp av en ekstern aktør kombinere ressurser med denne og dermed oppnå større effektivitet og potensielt styrke konkurransefortrinnet (Barney, 2002). Alternativt kan organisasjonen utvikle evner internt for selv å utvikle konkurransefortrinn innen området. Samtidig kan det være andre ikke kontrollerbare variabler, som forsvarlig sikkerhetsnivå og krigens folkerett som kan hindre at en organisasjon som Forsvaret kan sette ut aktiviteter.

Forsvaret skal dekke et behov for sikkerhet og militær beskyttelse av landet (Forsvaret, 2013), og det skal gjøres innenfor visse økonomiske rammer. Legger vi RBV til grunn må de ressursene som direkte kan bidra til dette vurderes som verdifulle og viktige, uavhengig av om vi omtaler dette som kilder til konkurransefortrinn, kilder til et bærekraftig forsvar, eller noe annet. Ressurser som ikke er kilder til dette kan vurderes å settes ut til en tredjepart[8] dersom det eksempelvis frigjør midler som heller kan brukes på de verdifulle ressursene. Følgelig sier sjelden- og ikke-imiterbar-kriteriet også noe om hvilke ressurser som er viktige for at Forsvaret skal kunne nå sitt overordnede mål[9]. For å vurdere hvorvidt Forsvaret er i stand til å utnytte disse ressursene, vil det åpenbart være flere forhold som spiller inn, som kompetanse, kapasitet og tilgang på teknologi.

[8] F.eks. vedlikehold av administrative kjøretøy, innkjøp av lite kritiske varer, leasing av biler.
[9] Det overordnede formålet for Forsvaret og forsvarssektoren er å bidra til å ivareta statssikkerheten og nasjonale sikkerhetsinteresser, dvs. Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser. Se kapittel 3 for flere detaljer.

2.7 Digital kompetanse

En nødvendig faktor som bidrar både direkte og indirekte til å sikre IKT-virksomhetens leveranseevne i krisespekteret, og dermed Forsvarets operative evne, er tilgang på tilstrekkelig personell med relevant kompetanse (Birkemo et al., 2021; Svendsen-utvalget, 2020).

2.7.1 Hva er digital kompetanse

Kompetanse består av dimensjonene kunnskap, ferdigheter, evner og holdninger (Lai, 2011, 2013). Disse dimensjonene benyttes også til å beskrive digital kompetanse.

Digital kunnskap vil si at en person innehar teoretisk innsikt og forståelse som man har fått gjennom ulike former for opplæring og gjennom erfaring, mens de *digitale ferdighetene* handler om selve gjennomførelsen – altså det å sette de teoretiske kunnskapene ut i praksis. Eksempelvis vil en del av den digitale kompetansen til en sluttbruker være grunnleggende bruk av tekstbehandlingsverktøy, presentasjonsverktøy, e-post, osv. Andre elementære ferdigheter vil være lagring av dokumenter, grunnleggende kunnskap og ferdigheter om filbehandling og mappestruktur. En persons *digitale evner* handler om det å ha personlige egenskaper og talent til å benytte IKT, og noen mennesker kan ha bedre forutsetninger for dette enn andre. Dette er imidlertid en dimensjon ved digital kompetanse som vi ikke berører nærmere i denne rapporten.

Som definisjonen på kompetanse viser, velger vi å inkludere *digitale holdninger* som en del av digital kompetanse. Sentralt i holdningskomponentene er en persons tanker og følelser. I ulike atferdsteorier argumenteres det med at holdninger leder til atferdsvalg (se, f.eks. Davis et al., 1989; Fishbein & Ajzen, 1975; Ilie & Turel, 2020). Det vil si at hvilket atferdsvalg en sluttbruker velger, kan være ledet ut fra vedkommendes holdninger. Dette kan være alt fra et valg om å lagre et dokument i en filstruktur til vedkommendes holdninger til strategisk partner innen IKT. Personens ansvars- og lojalitetsfølelse er også en del av holdninger – og kan knyttes til de atferdsmessige mekanismene som nevnt tidligere i rapporten.

Hva slags type digital kompetanse en person bør inneha, vil være avhengig av hvilken rolle personen besitter i organisasjonen (Elstad et al., 2022). En toppleder vil for eksempel ha behov for én type digital kompetanse, mens en driftstekniker bør inneha en helt annen type kompetanse. Det er for eksempel ikke nødvendig at en toppleder har detaljkunnskap om ulike former for kommunikasjonsprotokoller, mens dette kan være en grunnleggende nødvendig kunnskap for en driftstekniker. *Sluttbrukerkompetanse* omhandler grunnleggende bruk av IKT, og er den digitale kompetansen brukeren må besitte for å kunne benytte IKT på en effektiv måte (Elstad et al., 2022). van Laar et al. (2017) inkluderer også kommunikasjon[10] som en del av den digitale kompetansen. *Driftskompetanse* «handler overordnet om utvikling, installasjon, drift og vedlikehold.» (Elstad et al., 2022). Det er ofte eksperter innenfor sitt felt, gjerne med IKT-utdannelse, som innehar denne rollen. Rollen er rådgiver for aktører som tar strategiske veivalg. «Det vil si

[10] Kommunikasjon i denne sammenheng vil si kompetanse til å bruke forskjellig IKT for å overføre informasjon til flere mottakere og sikre at meningen med informasjonen er effektivt uttrykt. Med andre ord, inkludert i den digitale kompetansen er at mottaker får informasjonen, på en slik form at mottaker forstår informasjonen (Elstad et al., 2022).

at en organisasjon vil være avhengig av å ha noe slik digital kompetanse for opprettholdelse av daglig drift, vedlikehold og utvikling, samtidig som denne kompetansen alene ikke er nok for en organisasjon til å oppnå organisatorisk effektivitet.» (Elstad et al., 2022).

Strategisk IKT-kompetanse vil si «hvordan organisasjonen, gjennom ledelsen, innretter seg for å oppnå økt organisatorisk effektivitet […]. En del av den strategiske IKT-kompetansen omhandler helhet og en overordnet forståelse for IKTs rolle i organisasjonen, inkludert hvordan og innenfor hvilke rammer en ønsker å utvikle organisasjonen.» (Elstad et al., 2022). Strategisk IKT-kompetanse vil derfor være en nødvendig kompetanse i utarbeidelsen av ulike handlings-alternativer i forbindelse med sourcing. Det vil med andre ord si at alt som drøftes i denne rapporten er ulike eksempler på strategisk IKT-kompetanse.

2.7.2 Digital kompetanse som må inngå i utarbeidelse av handlingsalternativ

Ved sourcing er digital kompetanse en sentral faktor som må inngå i de ulike handlings-alternativene som utarbeides, og vi vil derfor i dette kapittelet gå inn på ulike typer digital kompetanse som bør inngå, oppsummert i figur 2.3.

I utarbeidelsen av handlingsalternativene vil det typisk være involvert ulike grupperinger fra organisasjonen, fra sluttbrukere, via ansatte som utfører drift, vedlikehold og utvikling til ansatte med ansvar for strategisk IKT-styring. Ved utarbeidelse av ulike handlingsalternativer i forbindelse med sourcing kreves det flere ulike former for digital kompetanse.

> Forsvaret som kunde må ha tilstrekkelig kompetanse til å stille krav til den strategiske partneren og sentrale underleverandører som sikrer leveranseevne til en lavest mulig kostnad. IKT-virksomheten må samtidig kunne gjennomføre gode og helhetlige risikoanalyser av leveranseevnen i krisespekteret, noe som også forutsetter et bredt spekter av kompetanse. (Birkemo et al., 2021 s. 68).

Bestillerkompetanse er et begrep som ofte nevnes i forbindelse med sourcing. IKT-strategien for forsvarssektoren (Forsvarsdepartementet, 2019) knytter bestillerkompetanse til «hvordan behov skal beskrives for å gi leverandører handlingsrom og mulighet til å anbefale riktig løsning på behovet». Bestillerkompetanse er en sammensetning av flere av kompetanseområdene nevnt i figur 2.3.[11] Vi vil understreke at det ikke er slik at hver enkelt person kan inneha alle delene av denne kompetansen, men at det er et tverrfaglig team som til sammen innehar den nødvendige kompetansen beskrevet i figur 2.3. «God tverrfaglig kompetanse i IKT-virksomheten er den viktigste faktoren som vil kunne bidra til mer presise risikovurderinger og dermed mindre usikre og bedre beslutningsgrunnlag.» (Birkemo et al., 2021 s. 75).

[11] For flere detaljer, se Birkemo et al. (2021).

Figur 2.3 Ulike typer kompetanse det er behov for i forsvarssektoren for å utøve strategisk IKT-styring (de ulike delene er inspirert av Birkemo et al., 2021 s. 68–74; og Elstad et al., 2022).

2.7.3 Behov for digital kompetanse internt i forsvarssektoren

Overordnet, dersom en organisasjon velger å holde en IKT-funksjon/kapabilitet internt, vil ikke organisasjonen være avhengig av strategiske partnere eller andre leverandører. Ved at organisasjonen velger insourcing får organisasjonen mulighet til å utvikle mer intern kompetanse i organisasjonen og gjennom det mer kvalifisert personell (Jae-Nam et al., 2003). Digital kompetanse kan også dermed utvikle seg til et konkurransefortrinn.

Problemet oppstår når organisasjonen ikke har den ønskede kompetansen internt. I et slikt tilfelle må organisasjonen vurdere ulike perspektiver opp mot hverandre, for å se hvilket alternativ som er best. Det er denne problemstillingen forsvarssektoren nå står overfor innen IKT-området, spesielt siden utviklingen går raskt og de digitale verdikjedene blir mer og mer komplekse. Med dagens hurtige teknologiske utvikling kan det spørres om det er realistisk for forsvarssektoren å ha nok kompetanse internt til å ivareta alle kompetanseområder innen IKT. Forsvarssektoren er i dag avhengig av ekstern kompetanse, grunnet større grad av komplekse digitale verdikjeder, hvor det i fremtiden vil bli vanskeligere å skille de ulike bestanddelene i den digitale verdikjeden fra hverandre (se f.eks. Lysne, 2020).

En strategisk partner vil sannsynligvis ikke kjenne Forsvarets prosesser på samme måte som lederne internt i forsvarssektoren gjør. Dette kan også være knyttet til uskrevne regler og taus kunnskap, og usikkerhet knyttet til den strategiske partneren[12]. En strategisk partner har mindre virksomhetskompetanse enn forsvarssektorens egne ledere (Lacity et al., 1996). Samtidig kan forsvarssektoren ved bruk av strategisk partner få tilgang til flere teknologiske kapabiliteter, gjennom tilgang til ny teknologi og personell til å håndtere teknologien. Her er det et sentralt poeng at teknologien i seg selv ikke skaper noen verdi, det er den bevisste målrettede anvendelsen som er med på å skape verdi for Forsvaret (Elstad, 2014; Elstad & Hafnor, 2017; Elstad et al., 2022).

3 Nasjonal sikkerhet, forsvarlig sikkerhetsnivå og krigens folkerett

Innledningsvis i denne rapporten nevnte vi ikke-kontrollerbare variabler, det vil si ytre rammebetingelser som må ligge til grunn for sourcing. To slike variabler er *forsvarlig sikkerhetsnivå* for å ivareta nasjonal sikkerhet og *krigens folkerett*. Valgt løsning for hvordan Forsvarets behov for IKT-baserte funksjoner skal dekkes må ivareta nasjonale sikkerhetsinteresser og et forsvarlig sikkerhetsnivå for de aktiviteter og verdier som er avgjørende for nasjonal sikkerhet samt være i tråd med krigens folkerett. I dette kapittelet tar vi derfor for oss sikkerhetslovens krav om et forsvarlig sikkerhetsnivå for Forsvaret og IKT-virksomheten. Videre inkluderer vi forhold rundt

[12] Se kapittel 2.5, for mer om usikkerhet knyttet til transaksjonskostnader.

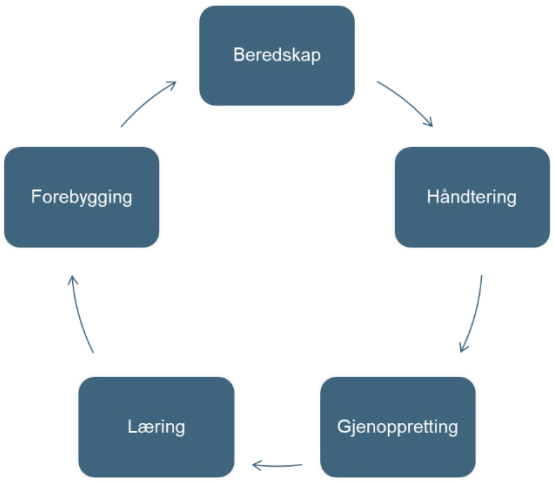
krigens folkerett og forholdet til bruk av sivile kontraktører gjennom kommersielle avtaler med vekt på leveranser av utstyr og tjenester innen IKT-området.

3.1 Forsvarlig sikkerhetsnivå

Sikkerhet er fravær av risiko, eller det motsatte av risiko (Aven, 2022). Formålet med risiko- og sikkerhetsstyring er å etablere og kontinuerlig opprettholde et akseptabelt sikkerhetsnivå for alle verdier i en virksomhet. Arbeidet for å få dette til består av flere deler som henger sammen og påvirker hverandre:

- *Forebygging* handler om å iverksette tiltak for å redusere muligheten for en uønsket hendelse, eller på forhånd redusere konsekvenser av en mulig hendelse.
- *Beredskap* handler om å planlegge og forberede tiltak som styrker evnen til å oppdage og håndtere uønskede hendelser slik at skadeomfanget blir minst mulig.
- *Håndtering* handler om å omsette beredskapen til innsats og samvirke for å håndtere uønskede hendelser best mulig slik at konsekvensene blir minst mulig.
- *Gjenoppretting* handler om evnen til å gjøre tapte funksjoner virksomme igjen etter en hendelse.
- *Læring* etter øvelser og hendelser er viktig for å identifisere tiltak for å hindre at tilsvarende hendelser skjer, forberede bedre beredskap og for bedre evnen til å håndtere fremtidige hendelser.

Figur 3.1 illustrerer risiko- og sikkerhetsstyring som en sirkel.



Figur 3.1 Kontinuerlig risiko- og sikkerhetsstyring.

Sikkerhet omfatter både tilsiktede og utilsiktede hendelser. Ved sourcing er det viktig at begge hensyn ivaretas, og at sikkerhetsarbeidet har et helhetlig perspektiv.

I vårt rammeverk for sourcing (se kapittel 4.2) har vi imidlertid valgt å avgrense oss til sikkerhetslovens innretning for å beskytte *nasjonale sikkerhetsinteresser*, og gjennom det etablere faktoren *forsvarlig sikkerhetsnivå*. Sikkerhetsloven med tilhørende regelverk utgjør et viktig verktøy for å beskytte nasjonale sikkerhetsinteresser, ikke primært andre verdier slik som skade på helse og miljø som dekkes av andre regelverk. Begrepet forsvarlig sikkerhetsnivå er en rettslig norm i henhold til sikkerhetsloven.

Beskyttelse og beredskap for utilsiktede uønskede hendelser er ikke regulert av sikkerhetsloven. Slike hendelser omfatter for eksempel

- skade på IKT-infrastruktur på grunn av bortfall av strømforsyning på grunn av naturhendelser slik som storm,
- utilgjengelige IKT-systemer på grunn av bortfall av elektronisk kommunikasjon som følge av ulykker og
- tap av sensitiv informasjon eller at sensitiv informasjon blir utilgjengelig på grunn av menneskelige feil eller programvarefeil som fører til utilsiktede hendelser i cyberdomenet.

Det kan være overlapp mellom tiltak for å beskytte mot henholdsvis tilsiktede og utilsiktede hendelser, men tiltakene kan også komme i konflikt.

3.2 Verdihierarki for nasjonal sikkerhet

Formålet med sikkerhetslovens bestemmelser er å beskytte og ivareta nasjonale sikkerhetsinteresser og sørge for at alle virksomheter har et forsvarlig sikkerhetsnivå slik at sikkerhetstruende virksomhet ikke får alvorlige skadefølger for nasjonal sikkerhet. Dette skjer gjennom å plassere ansvar samt sette krav og rammer for det forebyggende sikkerhetsarbeidet. Utgangspunktet for å kunne vurdere og sette krav til sikkerhetsnivået er å identifisere hvilke verdier og aktiviteter i virksomheten som har avgjørende betydning for nasjonal sikkerhet, det vil si å identifisere sammenhengen mellom virksomhetens verdier og aktiviteter og overordnede nasjonale sikkerhetsinteresser. Systematikken kan illustreres i form av et verdihierarki vist i figur 3.2.

Det overordnede formålet for Forsvaret og forsvarssektoren er å bidra til å ivareta statssikkerheten og nasjonale sikkerhetsinteresser, det vil si Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser. Å ivareta statens sikkerhet er den overordnede oppgaven for Forsvaret. Politiske myndigheters oppdrag til Forsvaret er spesifisert i ni oppgaver, hvorav de syv første er dimensjonerende (Forsvarsdepartementet, 2020). Forsvarsdepartementet (FD) har identifisert følgende fem grunnleggende nasjonale

funksjoner (GNF-er) for Forsvaret, det vil si tjenester, produksjon og andre former for virksomhet som er av en slik betydning at helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser (Forsvarsdepartementet, 2022a s. 122):

1. Situasjonsforståelse – Evnen til etterretning, situasjonsforståelse og rettidig varsling.

2. Innsats – Evnen til å håndtere episoder og sikkerhetspolitiske kriser og om nødvendig forsvare norsk eller alliertes territorium.

3. Kommando og kontroll – Evnen til kommando og kontroll over norske og allierte styrker.

4. Beskyttelse – Evnen til beskyttelse av norske og allierte styrker, kritiske samfunnsfunksjoner, samt kritiske funksjoner for Forsvaret.

5. Forsvarsdepartementets virksomhet, handlefrihet og beslutningsdyktighet. Dette omfatter departementets rolle som faglig sekretariat for politisk ledelse, utøvelse av myndighet, og styring og oppfølging av underliggende virksomheter, samt departementets beredskapsfunksjoner.

De andre departementene har spesifisert GNF-er innenfor sine ansvarsområder.

FD har operasjonalisert Forsvarets GNF-er i underfunksjoner, formulert som militære evner. Dette utgjør derfor et verdihierarki for Forsvarets kjernevirksomhet som kobler militære evner til GNF-er og de overordnede nasjonale sikkerhetsinteressene, i tråd med systematikken i sikkerhetsloven (se figur 3.2).

Som påpekt tidligere, IKT isolert sett skaper ikke verdi, det er den bevisste målrettede anvendelsen av IKT gjennom IKT-baserte funksjoner som er med på skape en verdi for organisasjonen. Det overordnede verdihierarkiet i figur 3.2 er et utgangspunkt for å identifisere hvordan ulike deler av IKT-virksomheten inngår i, og er nødvendig for, underfunksjonene (militære evner) til GNF-ene. Med dette som utgangspunkt kan kritikaliteten og fordelen som IKT-baserte funksjoner gir, vurderes for forsvarssektoren for å oppnå sektorens mål og opprettholde overordnede verdier og nasjonal sikkerhet.

Figur 3.2 Verdihierarki for forsvarssektorens virksomhet (evner/underfuksjoner) som understøtter grunnleggende nasjonale funksjoner (GNF), Forsvarets oppgaver og nasjonal sikkerhet (gjengitt fra Endregard et al., under arbeid).

3.3 Relevante krav i sikkerhetsloven

En rekke bestemmelser i sikkerhetsloven er relevante når det gjelder samarbeid med sivile aktører innen Forsvarets IKT-virksomhet. De viktigste bestemmelsene presenteres kort i de følgende deler. Dette gjelder forhold rundt ansvar og krav for forebyggende sikkerhetsarbeid og sikkerhetsstyring, beskyttelse av skjermingsverdige verdier, personellsikkerhet, eierskaps-kontroll samt sikkerhetsgraderte anskaffelser.

3.3.1 Ansvar for forebyggende sikkerhetsarbeid og risiko- og sikkerhetsstyring

Sikkerhetsloven plasserer ansvaret for forebyggende sikkerhetsarbeid og sikkerhetsstyring hos virksomhetens leder. Dette innebærer for Forsvarets del at dette ansvaret ligger hos forsvarssjefen (FSJ). For de øvrige etatene i forsvarssektoren er ansvaret plassert hos disse virksomhetenes respektive ledere. Når det gjelder strategisk styring av IKT, har FD gitt FSJ koordinerende ansvar for hele forsvarssektoren. Det lovpålagte ansvaret for et forsvarlig sikkerhetsnivå i forsvarssektorens etater, ligger, slik vi har forstått det, fortsatt hos den respektive etats leder.

Ansvaret for forebyggende sikkerhetsarbeid og sikkerhetsstyring innebærer blant annet at virksomheten skal:

- Sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig *risiko- og sikkerhetsforståelse* (sikkerhetsloven § 4-1).
- Regelmessig gjennomføre *vurdering av risiko* som grunnlag for forebyggende sikkerhetstiltak (sikkerhetsloven § 4-2).
- Gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et *forsvarlig sikkerhetsnivå* og redusere risikoen knyttet til sikkerhetstruende virksomhet samt regelmessig gjennomføre øvelser for å vurdere effekten av sikkerhetstiltak (sikkerhetsloven § 4-3).
- Dokumentere vurderingen av risiko og gjennomførte og planlagte sikkerhetstiltak (sikkerhetsloven § 4-4).
- Varsle sikkerhetsmyndigheten ved sikkerhetstruende hendelser eller brudd på krav (sikkerhetsloven § 4-5).

3.3.2 Skjermingsverdige verdier og personellsikkerhet

Skjermingsverdige verdier er de verdier som er av betydning for, og kan skade nasjonale sikkerhetsinteresser dersom de blir kjent for uvedkommende, endret, utilgjengelig, går tapt, mister funksjonalitet, skades eller blir overtatt av uvedkommende. Skjermingsverdige verdier omfatter følgende kategorier: informasjon (lagret både fysisk og digitalt), informasjonssystemer, objekter og infrastruktur (se sikkerhetslovens kapitler 5, 6 og 7).

Tilgang til skjermingsverdig informasjon skal kun gis ut fra et tjenstlig behov. Det krever autorisasjon, og for informasjon som er sikkerhetsgradert KONFIDENSIELT eller høyere kreves sikkerhetsklarering. Skjermingsverdig informasjon skal beskyttes i henhold til et forsvarlig sikkerhetsnivå. Kun kryptosystemer som sikkerhetsmyndigheten har godkjent, kan brukes for å beskytte skjermingsverdig informasjon. Skjermingsverdige informasjonssystemer skal godkjennes av sikkerhetsmyndigheten. Virksomheten skal overvåke sine skjermingsverdige informasjonssystemer. Virksomheten skal ivareta et forsvarlig sikkerhetsnivå for objekter og

infrastruktur ved sikkerhetstiltak som eksempelvis barrierer, adgangskontroll, overvåkning og varsling.

Det kreves sikkerhetsklarering, autorisasjon og adgangsklarering for personer som skal ha tilgang til sikkerhetsgradert informasjon, skjermingsverdige objekter og infrastruktur (se sikkerhetsloven kapittel 8).

3.3.3 Sikkerhetsgradert anskaffelse

En *sikkerhetsgradert anskaffelse* innebærer at leverandøren av en vare eller tjeneste får tilgang til eller tilvirker sikkerhetsgradert informasjon eller får tilgang til et skjermingsverdig objekt eller infrastruktur (sikkerhetsloven § 9-1). For en sikkerhetsgradert anskaffelse kreves:

- Sikkerhetsavtale med leverandør som tydeliggjør og konkretiserer plikter og ansvar, samt hvilken sikkerhetsgradering anskaffelsen skal ha (sikkerhetsloven § 9-2).
- Leverandørklarering dersom leverandøren får tilgang til informasjon gradert KONFIDENSIELT eller høyere (sikkerhetsloven § 9-3).
- Varsling til ansvarlig sektordepartement dersom anskaffelsen innebærer en ikke ubetydelig risiko. Virksomheter som ikke er underlagt et departement skal varsle NSM. (se sikkerhetsloven § 9-4).

Forskrift 20. desember 2018 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften) utdyper krav til sikkerhet i anskaffelser og varslingsplikt i § 18 og 19. Virksomhetens ansvar er å vurdere og håndtere risikoen, og dersom risikoen ikke er ubetydelig varsle departementet. Det presiseres at tilleggsanskaffelser og kontrakter som tildeles under en rammeavtale også er en anskaffelse, og dermed at de samme kravene gjelder.

3.3.4 Eierskapskontroll

Den som ønsker å kjøpe en kvalifisert eierandel i en virksomhet underlagt sikkerhetsloven, skal varsle ansvarlig sektordepartement. Sikkerhetslovens § 10-1 angir en *kvalifisert* eierandel å innebære at kjøper oppnår minst en tredjedel av aksjekapitalen, andelene eller stemmene i virksomheten, eller får rett til en tredjedel av aksjekapitalen eller andelene, eller oppnår en betydelig innflytelse over forvaltningen av selskapet. Departement eller sikkerhetsmyndigheten skal vurdere risikopotensialet ved et slikt erverv av virksomhet og oppkjøpers sikkerhetsmessige pålitelighet og om det godkjennes (sikkerhetsloven § 10-2). Dersom vurderingen er at ervervet «kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet, kan Kongen i statsråd fatte vedtak om at ervervet ikke kan gjennomføres, eller at det skal settes vilkår for gjennomføringen.» (sikkerhetsloven § 10-3). Kongen kan gi forskrift om stans av erverv av virksomhet.

Virksomhetsikkerhetsforskriftens § 93 gir en oversikt over hvilken informasjon en melding til departementet eller sikkerhetsmyndigheten skal inneholde. Dette inkluderer eierstruktur og

eventuelle utenlandske eierinteresser i erververs virksomhet og erververens eventuelle eier-interesser i utlandet samt nasjonaliteten.

Det pågår et arbeid for å stramme inn sikkerhetslovens bestemmelser for eierskapskontroll. Regjeringen sendte et forslag til høring i desember 2021 med høringsfrist 10. januar 2022 (Justis- og beredskapsdepartementet, 2021). Det forventes derfor innstramninger i loven på dette punktet som også kan påvirke sourcing på IKT-området.

3.4 Hva betyr bestemmelsene i sikkerhetsloven og virksomhet-sikkerhetsforskriften for sourcing?

I det følgende konsentrerer vi oss om Forsvarets IKT-virksomhet som FSJ har et ansvar for.

I henhold til sikkerhetsloven har Forsvaret et helhetlig ansvar for å sørge for et *forsvarlig sikkerhetsnivå* for Forsvarets IKT-virksomhet, uavhengig av sourcing.

Dette innebærer at Forsvaret som ledd i sourcingprosessen:

- Må kunne foreta *helhetlige risikovurderinger* som grunnlag for sikkerhetsmål for å oppnå et forsvarlig sikkerhetsnivå for verdiene og de IKT-baserte funksjonene og tjenestene som inngår i, eller understøtter verdiene og militære evner.
- Som et grunnlag for risikovurderinger, må Forsvaret kunne foreta *verdivurderinger* som følger systematikken i sikkerhetsloven (se kapittel 3.2).
    - Hvordan inngår den delen av IKT-virksomheten som vurderes tjenesteutsatt i Forsvarets militære evner (underfunksjoner til GNF), og hvilken kritikalitet er knyttet til disse IKT-baserte funksjonene?
- IKT-baserte funksjoner kjennetegnes som vi tidligere har vært inne på av økende kompleksitet på grunn av koblinger og avhengigheter, sammensatte verdikjeder, rask teknologiutvikling og endringshastighet som gir usikkerhet. *Usikkerheter* må identifiseres i risiko- og verdivurderingene og inngå i beslutningsunderlaget.

Analyser av risiko, verdier og tilhørende usikkerheter er nødvendig for å vurdere om det er mulig å oppnå forsvarlig sikkerhetsnivå for alternative sourcingkonstellasjoner for Forsvarets IKT-virksomhet samt identifisere nødvendige sikkerhetstiltak og tilhørende konsekvenser og kostnader.

De ovenstående vurderingene krever kunnskap i hele spennet fra Forsvarets operative evner i militære operasjoner, via andre deler av Forsvarets virksomhet til teknologi. Vurdering av risiko må knyttes til Forsvarets behov for og bruk av IKT-baserte funksjoner i sin virksomhet, både i væpnet konflikt, krise og fred. Behovet for IKT-baserte funksjoner, og hvor kritisk dette behovet er, bestemmes av hva disse funksjonene brukes til i en militær operasjon eller i administrative eller andre systemer som understøtter en militær virksomhet. Det er den funksjonaliteten IKT-systemene utgjør for Forsvaret i ulike situasjoner som er viktig, det vil si hvilke operative evner som disse bidrar til, både direkte og indirekte. Det er viktig å presisere at sikkerhet innebærer både å ivareta konfidensialitet, integritet og tilgjengelighet for skjermingsverdig informasjon, informasjonssystemer, objekter og infrastruktur. Risikobildet må kontinuerlig oppdateres i lys av endringer innen verdier, sårbarheter og trusler.

I en sourcingprosess er det derfor nødvendig å gjøre risikovurderinger for de ulike aktuelle handlingsalternativene. Dette gjøres best i samarbeid med aktuelle partnere og leverandører fordi handlingsalternativene må detaljeres i tilstrekkelig grad. Deretter må risiko og usikkerhet for de ulike alternativene vurderes ut fra et verdisentrisk utgangspunkt, det vil si ut fra viktighet, kritikalitet og fortrinn for Forsvaret, og i hvilken grad, og hvordan, et forsvarlig sikkerhetsnivå kan oppnås. Her må brukerne i forsvarssektoren involveres da det er disse som kan vurdere skadefølger dersom verdier blir kjent eller tilgjengelig for uvedkommende, går tapt eller blir endret eller ikke er tilgjengelig eller fungerer som de skal.

Av hensyn til nasjonal sikkerhet må Forsvaret til enhver tid ivareta et forsvarlig sikkerhetsnivå for IKT-virksomheten. Det betyr blant annet at Forsvaret må gjøre følgende:

- I sourcingprosessen:
    - Gjennomføre helhetlige verdi- og risikovurderinger i henhold til systematikken i sikkerhetsloven, med utgangspunkt i hvordan IKT inngår i Forsvarets militære evner (underfunksjoner) og understøtter skjermingsverdige verdier.
    - Vurdere forsvarlig sikkerhetsnivå for alternative løsninger opp mot dagens løsning, basert blant annet på tilstrekkelig innsikt i IKT-verdikjeder og eierskapsforhold.
    - Inngå sikkerhets- og leverandøravtaler og autorisasjon og sikkerhetsklareringer for det personellet som trenger det.
- Ved kontraktsinngåelse:
    - Sørge for å inkludere system og egnede krav til risiko- og sikkerhetsstyring slik at Forsvaret kontinuerlig har tilstrekkelig innsikt og kontroll med risiko og forsvarlig sikkerhetsnivå for IKT-virksomheten.
- I hele IKT-systemenes levetid:

- Sikre seg, og aktivt benytte styringsrett, innsikt og kontroll med IKT-virksomheten, inkludert den som leveres av partner og/eller andre leverandører, for å sørge for et forsvarlig sikkerhetsnivå for skjermingsverdige verdier.

- Sørge for at ansatte hos strategisk partner og leverandører har tilstrekkelig risiko- og sikkerhetsforståelse og nødvendige sikkerhetsklareringer og autorisasjoner der det vurderes påkrevd.

- Kontinuerlig ha tilstrekkelig oversikt over og kontroll med eierskaps- og leverandørforhold for IKT-virksomheten, vurdere risikoforhold knyttet til nasjonale sikkerhetsinteresser ved eventuelle endringer og eventuelle tiltak som følge av dette for å opprettholde et forsvarlig sikkerhetsnivå for Forsvarets verdier.

Vi tar forbehold om at ovenstående momenter ikke er en komplett liste. De er å anse som et utgangspunkt for vurderinger av sourcing som skal sikre et forsvarlig sikkerhetsnivå for IKT-virksomheten i tråd med sikkerhetslovens bestemmelser og dens forskrifter.

3.5 Krigens folkerett og kontraktører

Formålet med dette kapitlet er å løfte problemstillinger innenfor temaet krigens folkerett og sourcing innen IKT-virksomheten med henvisning til krav i styrende dokumenter. FFIs hensikt med å inkludere dette er at krigens folkerett skal vurderes i konkrete tilfeller knyttet til sourcing.

Forsvarets IKT-strategi forutsetter at Forsvarets IKT-virksomhet skal virke i hele krisespekteret, det vil si «Informasjons- og kommunikasjonsteknologi (IKT) er en kritisk faktor for at Forsvaret skal kunne løse sine oppgaver i krig, krise og fred.» (hentet fra Forsvarsstaben, 2021 kapittel 1). En forutsetning for innrettingen av IKT-virksomheten og valg av sourcingstrategi er at den må være i henhold til gjeldende lov og rett i hele krisespekteret.

I væpnet konflikt kommer krigens folkerett til anvendelse. Folkeretten er den rett som gjelder mellom stater, og den delen av folkeretten som kalles «krigens folkerett» eller «internasjonal humanitærrett» regulerer væpnet konflikt (Johansen, 2019 s. 125). I henhold til LTP skal planlegging for sivil støtte i væpnet konflikt være i henhold til krigens folkerett (Forsvarsdepartementet, 2020 s. 80). Sivil støtte omfatter både støtte fra offentlige myndigheter og støtte fra kommersielle sivile aktører gjennom leveranser av varer, tjenester og infrastruktur for å dekke Forsvarets behov.

3.5.1 Distinksjonsprinsippet og proporsjonalitetsprinsippet

Nasjonal krisehåndtering og beredskap, inkludert forsvaret av Norge i væpnet konflikt, er tuftet på omfattende gjensidig sivil-militær støtte og samarbeid i tråd med totalforsvarskonseptet. Konseptet er etablert fordi samfunnets ressurser er begrensede, og det ikke er hensiktsmessig, eller på mange områder mulig, å etablere parallelle militære og sivile kapasiteter. De senere

årene har forsvarssektoren i økende grad inngått frivillige avtaler med private aktører for å sikre Forsvaret varer og tjenester i hele krisespekteret. Det har altså vært en økende kommersialisering i Forsvaret knyttet til varer og tjenester. Imidlertid forutsetter distinksjonsprinsippet et skille mellom sivile og militære personer og objekter. Det norske totalforsvarskonseptet og den utstrakte sivile støtten til Forsvaret i væpnet konflikt som det legger opp til, utfordrer krigens folkerett. Planlegging og innretting av Forsvarets virksomhet skjer innenfor rammen av totalforsvarskonseptet, men må skje på en slik måte at Norges forpliktelser i henhold til folkeretten ivaretas. Dette gjelder også for samarbeidskonstellasjoner og avtaler med sivile aktører innen IKT-virksomheten.

Vi konsentrerer oss om det Johansen skriver om bruk av kontraktører og folkerett (Johansen, 2019 s. 130–131). Hun slår fast at «[…] sivil, kommersiell støtte er tillatt etter folkeretten, men at det går en grense for hvor omfattende den sivile støtten kan være uten at den kommer i konflikt med forutsetningen om demokratisk kontroll med militærmakten.». IKT-støtte er et område hvor tjenester kan utføres av sivile uten å utfordre prinsippet om demokratisk kontroll, ifølge Johansen (2019), men som presisert i LTP skal slik sivil kommersiell støtte være i henhold til krigens folkerett.

«Krigens folkerett bygger på prinsippene om distinksjon mellom sivile og stridende, militær nødvendighet, humanitet og proporsjonalitet.» (Forsvarsdepartementet, 2020 s. 80). *Distinksjonsprinsippet* forplikter krigførende parter til kun å angripe lovlige mål, det vil si stridende personer og militære objekter. Alle sivile personer som ikke er stridende samt sivile objekter skal beskyttes mot angrep. Det synes i utgangspunktet å være en enkel regel, men Johansen (2019 s. 125) sier «djevelen ligger i detaljene».

Distinksjonsprinsippet forutsetter et skille mellom stridende som er lovlige angrepsmål, og sivile personer som har beskyttelse mot angrep. De stridende deles i to kategorier (Forsvarssjefen, 2013 kapittel 3): 1) De lovlige stridende som har rett til å ta del i fiendtligheter på vegne av en stat, nyter strafferettslig immunitet for lovlige krigshandlinger, og gis krigsfangestatus ved tilfangetakelse. 2) Sivile personer som deltar direkte i fiendtlighetene og som er en av flere personkategorier man finner under de «andre stridende». Personer i den siste kategorien har ikke rett til å ta del i fiendtlighetene på vegne av staten, og har ikke krigsfangestatus. Sivile som deltar direkte i fiendtligheter kan derfor straffeforfølges for dette. Dersom sivile personer deltar direkte i fiendtligheter mister de sin beskyttelse mot angrep. «Nasjonalt regelverk forbyr Forsvaret å benytte sivile i funksjoner som utgjør direkte deltakelse.» (Forsvarsdepartementet, 2020 s. 81). Stridsdeltakelse og funksjoner som kan føre til deltakelse i strid, forutsettes utført av lovlig stridende militært personell fordi det ellers ville være i strid med plikten til å beskytte sivile mot farene ved militære operasjoner. I tillegg er det uheldig fordi det undergraver etterlevelse av distinksjonsprinsippet. FD har derfor i tildelingsbrevet i 2022 gitt Forsvaret følgende oppdrag (Forsvarsdepartementet, 2021d):

> Forsvaret skal identifisere funksjoner som skal bekles av lovlig stridende i væpnet konflikt. Dersom sivile bekler slike funksjoner, skal de erstattes av lovlige stridende. Alternativt må det iverksettes tiltak slik at de aktuelle personene er å anse som lovlige stridende med de rettigheter og plikter som følger av krigens folkerett.

Hva som innebærer direkte deltakelse i fiendtlighetene på IKT-området og dermed skal utføres av militært personell i væpnet konflikt, må derfor identifiseres av Forsvaret. «Manual i krigens folkerett» representerer Norges posisjon for vilkårene for direkte deltakelse, og disse gjelder derfor for Forsvaret (Forsvarssjefen, 2013 s. 52–58). Direkte deltakelse i fiendtligheter omfatter rene stridshandlinger, uavhengig av stridssone. Videre omfatter det blant annet planlegging, ildledelse, formidling av taktisk etterretningsinformasjon og frakt av militært materiell frem til en stridssone.

Aktiviteter som innebærer indirekte støtte til fiendtlighetene, anses ikke å være en del av stridighetene. «Felles for alle sivile kontraktører er at deres oppgaver må innebære sivile, ikke stridende funksjoner.» (Johansen, 2019 s. 130). Sivile, herunder kontraktører, som utfører *sivile* oppgaver til støtte for Forsvaret har en særstilling i folkeretten som «sivile som følger de væpnede styrker». Etter tredje Genèvekonvensjon av 1949 art. 4 A nr. 4 skal sivile som følger de væpnede styrker ha et identitetskort som samsvarer med vedlegg til tredje Genèvekonvensjon, for å vise at de har fått denne statusen av staten. Dette er derfor noe man må ha, dersom staten skal gi denne statusen. De gis krigsfangestatus dersom de blir tatt til fange. De har status som sivile, og er derfor beskyttet på lik linje med andre sivile, men løper en risiko dersom de oppholder seg i et lovlig militært mål.

> Proporsjonalitetsprinsippet medfører at stridende skal unngå å angripe lovlige mål dersom det er antatt at dette vil medføre tilfeldig tap av sivile liv eller ødeleggelse av sivile gjenstander som vil overstige den konkrete, militære nytten som er forventet av angrepet. (Cooper, 2022).

Proporsjonalitetsprinsippet innebærer at sivile kan bli utsatt for lovlig følgeskade dersom de oppholder seg i eller nær lovlige militære mål. Dette er en fare som sivile kontraktører kan utsettes for. I henhold til folkeretten plikter norske myndigheter å holde risikoen for følgeskade for sivile lav. Derfor sier FD at «Det skal etableres mekanismer for risikovurdering av sivil følgeskade, […].» (Forsvarsdepartementet, 2020 s. 80). Slike risikovurderinger forutsettes å inngå ved sourcing, og at sourcing innrettes slik at denne risikoen holdes så lav som mulig.

Det er kun tillatt å angripe militære objekter. Hvilke objekter som er lovlige mål, bestemmes av objektets funksjon, det vil si om objektet «[…] ut fra sin art, plassering, formål eller bruk gir et effektivt bidrag til militære aksjoner, og som det etter de rådende omstendigheter vil by på en avgjort militær fordel å gjennomføre en total eller delvis ødeleggelse, erobring eller nøytralisering av» (Forsvarssjefen, 2013 s. 139). En slik funksjonsbasert definisjon betyr at en del forsyninger, transportinfrastruktur, kraftforsyning og annen kritisk infrastruktur som både Forsvaret og sivile er avhengig av kan bli lovlige mål. Når Forsvarets IKT-virksomhet og sourcingstrategi planlegges videre, er dette et viktig hensyn som må tas slik at de løsninger Forsvaret velger innen sourcing ikke fører til fare for uforholdsmessig stor følgeskade for sivile samfunnsfunksjoner som befolkningen er avhengig av. Politiske myndigheter sier eksplisitt at «Ved utvikling av konsepter for sivil støtte skal det foretas en folkerettslig vurdering for å identifisere begrensninger i krigens folkerett og ta hensyn til disse begrensningene i innretningen av konseptene.» (Forsvarsdepartementet, 2020 s. 81).

3.5.2 Tjenesteplikt

En potensiell risiko for Forsvaret er hvordan sikre at sivile som bekler stillinger i fred som innebærer direkte deltakelse i fiendtligheter jf. krigens folkerett, kan gjøres til lovlig stridende militært personell og forpliktes til tjeneste i sikkerhetspolitisk krise og væpnet konflikt. Norge benytter reglene om tjenesteplikt i forsvarsloven for å knytte til seg lovlig stridende militært personell. Slikt personell må oppfylle krav om uniformering (Forsvarssjefen, 2013 pkt. 3.13).

Forutsetningen for at Forsvaret kan disponere en person inn i styrkestrukturen, er at personen har en tjenesteplikt etter Lov om verneplikt og tjeneste i Forsvaret, m.m. (forsvarsloven). Tjenesteplikten er plikten til i fred og krig å utføre de oppgavene som Forsvaret tildeler den enkelte, i den stillingen den enkelte blir disponert i, og på det stedet Forsvaret bestemmer, jf. forsvarsloven § 2 tredje ledd. En person kan pålegges en tjenesteplikt i Forsvaret enten fordi vedkommende har verneplikt, er militært tilsatt eller har inngått annen kontrakt om tjenesteplikt i Forsvaret, jf. forsvarsloven § 2, første ledd.

Hjemmel til å inngå kontrakt om tjenesteplikt i Forsvaret fremgår av forsvarsloven § 2 første ledd. Forsvaret har i dag en særskilt lovregulert adgang til å inngå kontrakter om frivillig tjeneste i Heimevernet (forsvarsloven § 24) og om frivillig tjeneste for kvinner født før 1. januar 1997 (forsvarsloven § 25). Disse kontraktsforholdene reguleres nærmere av Forskrift om verneplikt og heimevernstjeneste (Vernepliktsforskriften). Forsvaret har også en lovfestet adgang til å inngå kontrakt om tjenesteplikt i internasjonale operasjoner (forsvarsloven § 50).

«Forsvarets adgang til å inngå kontrakter om tjenesteplikt er lovfestet fordi tjenesteplikten i Forsvaret kan være inngripende utover det som er vanlig i et ansettelsesforhold.» (Forsvarsdepartementet, 2021a s. 7). Det er dermed ikke egen lovhjemmel for inngåelse av kontrakt om tjenesteplikt etter forsvarsloven med ansatte i sivile selskaper med leveranseavtaler til Forsvaret.

Regjeringen har foreslått å utvide Forsvarets adgang til å inngå kontrakt om tjenesteplikt ved endring av forsvarsloven, dette også for å sikre forutsigbar tilførsel av kompetanse til styrkestrukturen (Forsvarsdepartementet, 2022b). Det er viktig å merke seg at det er Forsvarsdepartementets syn at en endring av forsvarsloven ikke vil gi hjemmel for å inngå kontrakt om tjenesteplikt med innleide konsulenter eller ansatte hos en sivil strategisk partner (Forsvarsdepartementet, 2022b s. 26).

> I den grad Forsvaret i en krigssituasjon har behov for personell ansatt hos strategiske samarbeidspartnere eller andre steder som ikke er tjenestepliktig, vil dette måtte løses med hjemmel i beredskapslovgivningen og de muligheter militære myndigheter har til å rekvirere ressurser (Forsvarsdepartementet, 2022b s. 26).

Regjeringen kan for eksempel utskrive arbeidsplikt med hjemmel i Lov av 15. desember 1950 nr. 7 om særlige rådgjerder under krig, krigsfare og liknende forhold (Beredskapsloven) §3. Dette er imidlertid noe annet enn tjenesteplikt etter forsvarslovens regler, som er den måte Norge som utgangspunkt knytter til seg lovlig stridende militært personell.

I henhold til forsvarsloven kan sivilt ansatte dermed bare styrkedisponeres i henhold til reglene om verneplikt, eller ved tilsetting som militært personell i henhold til forsvarsloven § 44. Verneplikten gjelder i utgangspunktet ikke kvinner født før 1997 og menige over 44 år jf. forsvarsloven § 6. Ansatte hos en leverandør kan være utenlandske statsborgere, noe som kompliserer bildet ytterligere. Utenlandske statsborgere som oppholder seg i og har en fast tilknytning til Norge, kan bli pålagt verneplikt hvis ikke avtale med landet de er statsborgere av, er til hinder for det jf. forsvarsloven § 6 tredje avsnitt.

Forsvarets muligheter for å gjøre avtaler om tjenesteplikt med norske kontraktører er altså begrenset. Dermed er også mulighetene til å gjøre om sivilt personell til lovlig stridende militært personell begrenset til de øvrige reglene i forsvarsloven om tjenesteplikt for vernepliktige, eller militært tilsatte. Beredskap og leveransesikkerhet må derfor også vurderes som ledd i sourcing.

3.5.3 Krigens folkerett i cyberdomenet

Cyberdomenet er «rommet» som skapes av IKT.[13] Internett er den største og mest kjente delen av cyberdomenet. Cyberdomenet rommer mer og mer, alt fra nettbutikker, sosiale og tradisjonelle medier til ventilasjonsanlegg og kjøleskap. I forsvarssammenheng kan det handle om viktige deler av stridsvogner eller kommando- og kontrollsystemer. Cyberdomenet er følgelig også et krigføringsdomene. Militære styrker er i dag avhengig av det for å gjennomføre militære operasjoner. De øvrige fire domenene for krigføring er landdomenet, luftdomenet, sjødomenet og romdomenet. Forsvarets fellesoperative doktrine definerer cyberoperasjoner som «militære eller strategiske handlinger som foregår i eller gjennom cyberdomenet for å sikre egen handlefrihet, og ramme fienden for å oppnå militære og strategiske målsetninger. Alt som kan nås via cyberdomenet, er mulige mål og mulige trusler.» (Forsvarsstaben, 2019, s. 125).

I cyberdomenet er forholdet til krigens folkerett kjennetegnet av uklarheter. I følge Cooper (2021 s. 1) utløser krigføring i cyberdomenet særlige spørsmål:

> Krigens folkerett skiller mellom militære og sivile, og mellom personer og gjenstander. Sivile personer og gjenstander skal ikke være mål for angrep. Men hva er en gjenstand i cyberdomenet? Og hvordan skiller man mellom sivile og militære når mye av infrastrukturen er delt? Både det å gjennomføre militære operasjoner på en god måte også i cyberdomenet og samtidig jobbe for å unngå at militære operasjoner forårsaker skade og lidelse for sivile og sivilbefolkningen, byr på både praktiske og rettslige problemstillinger. Dette er et område hvor det fremdeles er noe uklart hvordan folkeretten skal komme til anvendelse. Samtidig tilsier moderne samfunn med stor og økende avhengighet av digital infrastruktur at vi trenger tydelig regulering av krigføring også i cyberdomenet.

I den kommende versjonen av den norske «Manual i krigens folkerett» er cyberoperasjoner viet et eget kapittel. Denne manualen ligger per november 2022 til godkjenning i FD. Cooper fremhever at direkte deltakelse i fiendtligheter er et av de vanskeligste konseptene i krigens folkerett (Cooper, 2021 s. 25). Den kommende manualen har flere eksempler for cyberdomenet. Når det

[13] Se https://www.ffi.no/forskning/tema/ikt-og-cyberdomenet.

gjelder ansvaret for cyberoperasjoner har Etterretningstjenesten ansvar for offensive cyber-operasjoner, mens Cyberforsvaret er Forsvarets avdeling for etablering, drift og beskyttelse av Forsvarets egen IKT (Forsvarsdepartementet, 2020 s. 75).

3.5.4 Andre forhold

Utviklingen går i retning av at Forsvarets IKT-virksomhet og sivil IKT-virksomhet blir stadig mer gjensidig avhengig og integrert. Videre er det politisk besluttet at Forsvaret bør tjeneste-utsette den delen av virksomheten som kan utføres av sivile aktører, jamfør prinsippet om så sivilt som mulig, så militært som nødvendig. På IKT-området er det ikke enkelt å skille militær og sivil virksomhet, og dermed er det heller ikke enkelt å avgrense hvilke deler av IKT-virksomheten som kan egne seg for outsourcing. I det fysiske domenet kan slike vurderinger være enklere. Sivile transportører kan fremføre ammunisjon til lagre som geografisk ikke ligger nært stridsområdet. Men den siste transportstrekningen fra et lager og til de militære styrkene bør Forsvaret utføre selv. Slike skiller er vanskeligere på IKT-området.

Et annet aspekt ved sourcing på IKT-området er at det kan føre til at store selskaper leverer IKT-tjenester og -infrastruktur både til sivile kritiske samfunnsfunksjoner og Forsvaret. Hvordan Forsvaret innretter seg, kan derfor få konsekvenser for andre kritiske samfunns-funksjoner som da kan bli mer utsatt for angrep. Eksempelvis kan det føre til at sivile personer og objekter som er kritiske for det sivile samfunnets funksjonalitet, samtidig blir lovlige militære mål fordi de også står for kritiske leveranser til Forsvaret. Det kan for eksempel gjelde samlokaliserte datasentre, eller en sivil leverandørs personell eller infrastruktur. I en slik ut-vikling er det derfor viktig at folkerettslige forhold knyttet til valg av sourcingstrategi blir vurdert i en helhetlig samfunnsmessig kontekst.

3.5.5 Oppsummering

Når forsvarssektoren planlegger og gjennomfører sourcing innen IKT-virksomheten må det gjøres konkrete folkerettslige vurderinger fra sak til sak. Det er i liten grad mulig å trekke generelle konklusjoner. Hva en eventuell leverandør konkret skal levere til Forsvaret av IKT-systemer og -tjenester, utvikles ofte i en dialog og gjennom forhandlinger mellom partene. Derfor må de folkerettslige vurderingene inngå i hele sourcingprosessen og oppdateres etter hvert som mer detaljer om sivile leveranser og partnerskap kommer på plass. Oppsummert gjelder følgende forutsetninger:

1. Forsvaret må konkretisere hvilke funksjoner innen IKT-virksomheten som utgjør direkte deltakelse i fiendtlighetene. Dette gjelder både funksjoner i cyberdomenet som krigføringsdomene og de funksjonene som innebærer annen direkte støtte til militære operasjoner som for eksempel kommunikasjonsmidler for å understøtte kommando og kontroll i et stridsområde eller prosessering og overføring av sensordata som direkte bidrar til kommando- og kontrollfunksjoner ved Forsvarets hovedkvarter.

2. Forsvaret må identifisere hvilke funksjoner innen IKT-virksomheten som sivile kontraktører kan utføre uten å utfordre krigens folkerett og nasjonale bestemmelser.

Dette kan eksempelvis være generell understøttelse ved leveranser og vedlikehold knyttet til rent administrative IKT-systemer.

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

4. Forsvaret må vurdere samfunnsmessige konsekvenser for både kritiske samfunnsfunksjoner og sivilbefolkningen ved sourcing for å sørge for at måten Forsvaret innretter seg på ikke motvirker en motparts evne, eller vilje, til å beskytte disse.

4 Sourcing for Forsvarets IKT-virksomhet

Dette kapittelet starter med en overordnet gjennomgang av et forskningsarbeid ved FFI som omhandler porteføljemodell for valg av sourcingstrategi i forsvarssektoren, heretter forkortet «modell for valg av sourcingstrategi» (kapittel 4.1). Modellen for valg av sourcingstrategi danner grunnlaget for videre studier av sourcingstrategi i Forsvaret og forsvarssektoren. I kapittel 4.2 tar vi derfor utgangspunkt i modell for valg av sourcingstrategi (presentert i kapittel 4.1) og utvider denne med momenter som etter vårt syn er viktige for sourcing for Forsvarets IKT-virksomhet. Utvidelsene av modellen baseres på det teoretiske rammeverket presentert i kapittel 2 og 3.

4.1 Modell for valg av sourcingstrategi i forsvarssektoren

I det følgende presenteres et forskningsarbeid ved FFI knyttet til modell for valg av sourcingstrategi for forsvarssektoren, og teksten er i all hovedsak hentet fra dette arbeidet, dersom annet ikke er nevnt.[14]

Modell for valg av sourcingstrategi tar utgangspunkt i ulike aktiviteter som inngår i Forsvarets virksomhet og forskningsarbeidet adresserer tre grunnleggende spørsmål: (1) Hva er Forsvarets kjernevirksomhet? (2) Hvilke aktiviteter bør beholdes internt i forsvarssektoren? og (3) Hvilke leverandørforhold bør forsvarssektoren velge for de aktivitetene som kan eller bør utføres av en tredjepart? Disse spørsmålene diskuteres ut fra to dimensjoner, nemlig *strategisk viktighet* av aktiviteten og *relativ evne* til å gjennomføre aktiviteten.

[14] For mer utdypende litteraturgjennomgang og flere detaljer se Pedersen (2022).

4.1.1 Strategisk viktighet

Overordnet handler strategisk viktighet om hvor nært aktiviteten er knyttet til organisasjonens primæraktiviteter, altså de aktivitetene som er direkte knyttet til organisasjonens eksistens. For Forsvaret vil det inkludere alle aktiviteter som bidrar til gjennomføring av styrkeoppbygging og militære operasjoner. Forsvaret skiller som nevnt mellom kjernevirksomhet (primæraktiviteter) og tilretteleggende virksomhet (støtteaktiviteter) som inkluderer de øvrige aktivitetene. Strategisk viktige aktiviteter vil da være aktiviteter som er en del av Forsvarets kjernevirksomhet eller nært tilknyttet til denne, siden det vil få store konsekvenser ved mangelfull utføring av disse aktivitetene. Vi understreker at aktiviteter med lav strategisk betydning ikke er ensbetydende med at aktiviteten er uviktig eller unødvendig.

Modell for valg av sourcingstrategi foreslår at aktiviteter deles inn etter høy og lav strategisk viktighet. Høy strategisk viktighet krever større grad av intern kontroll på aktiviteten enn lav strategisk viktighet. Ved lav strategisk viktighet anbefales en rent transaksjonsbasert tilnærming, mens med høyere viktighet anbefales større grad av samarbeid med leverandøren. For høy strategisk viktighet kan man alternativt velge intern leveranse. Oppsummert kan vi si:

- Aktiviteter som er strategisk viktige bør kontrolleres i større grad internt enn aktiviteter med lavere grad av viktighet.

- Ved lav strategisk viktighet for aktiviteten er strategisk samarbeid mindre aktuelt, siden aktivitetene kan ivaretas gjennom transaksjonsbaserte leverandørforhold. Det foreslås tre måter det transaksjonsbaserte leverandørforholdet kan ivaretas enten internt i forsvarssektoren eller at strategisk partner kan ivareta dette på vegne av sektoren. Forsvaret kan også velge å avslutte aktiviteten dersom det er et alternativ.

- Ved høy strategisk viktighet er tilnærminger som samarbeidsbaserte leverandørforhold eller å investere for å kunne utføre aktiviteten internt i forsvarssektoren, aktuelle.

- Ved valg av samarbeidsbaserte leverandørforhold for strategisk viktige aktiviteter (aktuelt dersom det ikke er et alternativ å gjennomføre aktiviteten selv) er prinsippet at jo mer strategisk viktig aktiviteten er for Forsvaret, jo tettere samarbeid bør det være med leverandøren.

4.1.2 Relativ evne

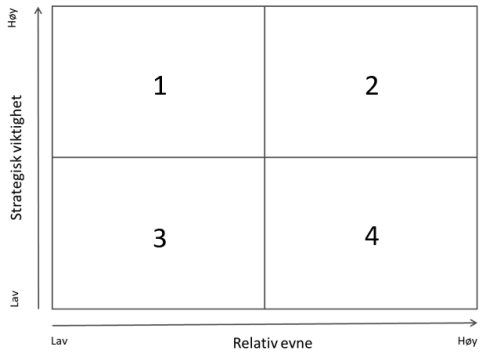
Den andre dimensjonen som vurderes i modell for valg av sourcingstrategi er relativ evne. Relativ evne sier noe om egen organisasjons evne til å utføre aktiviteter sammenlignet med andre eksterne aktører, slik som leverandører og konkurrenter. Evne i denne sammenheng favner bredt og kan inkludere kvalitet på utførelse, kapasitet, fleksibilitet, skalerbarhet og kostnadseffektivitet.

For å være i stand til å ta en vurdering av ulike handlingsalternativer knyttet til sourcing, må en vurdering av organisasjonens relative evne inngå, for å kunne avklare hvilke aktører som er i

best stand til å gjennomføre aktiviteten. En vurdering av relativ evne for forsvarssektorens del vil si å vurdere egen evne sammenlignet med potensielle leverandørers evne.

Modell for valg av sourcingstrategi foreslår en todeling av relativ evne, hvor de ulike aktivitetene deles inn etter hvorvidt forsvarssektoren har høy eller lav relativ evne til å gjennomføre aktiviteten. Oppsummert betyr dette at ved lav relativ evne har potensielle leverandører på markedet en bedre evne enn det forsvarssektoren selv har til å utføre aktiviteten, og aktiviteten er en kandidat til å bli overtatt av en leverandør som har denne aktiviteten som en del av sin kjernevirksomhet. Ved høy strategisk viktighet og lav evne vil løsningen bli enten et samarbeidsbasert leverandørforhold eller at forsvarssektoren investerer for å kunne utføre aktiviteten internt. Ved høy relativ evne har forsvarssektoren like god eller bedre evne til å utføre aktiviteten selv enn potensielle leverandører i markedet, og da bør aktiviteten beholdes internt.

Modell for valg av sourcingstrategi presenterer fire generiske kvadranter for overordnede handlingsalternativer, som vist i figur 4.1: Vi vil i det videre kort presentere hver av disse kvadrantene.



Figur 4.1 Fire generiske kvadranter basert på dimensjonene strategisk viktighet og relativ evne (Pedersen, 2022 s. 61).

4.1.3 Aktiviteter med høy strategisk viktighet hvor leverandører på markedet har bedre evne enn forsvarssektoren til å utføre dem

Den første kvadranten i figur 4.1 inneholder strategisk viktige aktiviteter hvor leverandøren(e) i markedet har bedre evne enn forsvarssektoren til å utføre aktivitetene. Dette er aktiviteter som omfatter deler av Forsvarets kjernevirksomhet og aktiviteter tett knyttet til denne. Aktiviteter i denne kvadranten er strategisk viktige og avgjørende for Forsvarets eksistens, slik at det er av avgjørende betydning at disse aktivitetene blir gjennomført med en viss kvalitet.

På en generell basis er det å ha kontroll over egne ressurser verdifullt i seg selv, og basert på RBV bør strategisk viktige ressurser beholdes og utvikles internt (Barney, 2002). Sett i et TCE-perspektiv kan det også argumenteres med å holde aktiviteten internt, dersom det krever betydelige transaksjonskostnader ved ekstern utførelse. For å beholde kontrollen over egne ressurser kan da forsvarssektoren velge å beholde aktiviteten internt og investere i nødvendige

ressurser for å dekke gapet mellom egen evne og den evnen leverandøren har. Kostnadene ved å investere i egne ressurser kan være høye, men samtidig nødvendige for å motvirke negative konsekvenser ved å sette ut aktiviteter til en ekstern leverandør.

Den eksterne leverandøren vil i kvadrant 1 være en naturlig kandidat for et samarbeidsbasert leverandørforhold – og leverandøren bør fortrinnsvis ha den aktuelle aktiviteten som en del av sin kjernevirksomhet. Ved en slik tilnærming bør leverandøren ses på som en utvidelse av egen organisasjon. Imidlertid er det slik at graden av samarbeid vil være avhengig av en rekke ulike faktorer som må vurderes i hvert tilfelle knyttet til å ha kontroll på transaksjonen og håndtere ulike former for risiko, inkludert risiko for opportunisme.

4.1.4 Aktiviteter med høy strategisk viktighet hvor forsvarssektoren har bedre evne til å utføre aktiviteten enn de alternative leverandørene på markedet

Aktiviteter i kvadrant 2 er strategisk viktige aktiviteter hvor forsvarssektoren selv har bedre evne til å utføre aktiviteten enn de andre alternative leverandørene på markedet. Disse aktivitetene vil være nært knyttet til Forsvarets kjernevirksomhet, og Forsvarets eksistens er avhengig av at disse aktivitetene gjennomføres med tilstrekkelig kvalitet.

Aktiviteter i denne kvadranten bør utføres internt, og det kan antas at det ikke finnes andre reelle alternativer enn en ren intern utførelse. Ved denne kvadranten kan det også vurderes om det er behov for å styrke den interne evnen ytterligere. Eksempelvis er dette tilfeller hvor oppgaver må utføres av militært personell med militære ressurser, som for eksempel ledelse av militære operasjoner. I denne kvadranten vil det også være ikke-kontrollerbare variabler som setter rammer for at aktiviteten må utføres internt, for eksempel krigens folkerett og forsvarlig sikkerhetsnivå.

4.1.5 Aktiviteter med lav strategisk viktighet der forsvarssektorens evne til å utføre aktiviteten er lavere enn de potensielle leverandørenes evne

Aktiviteter i kvadrant 3 er aktiviteter hvor den strategiske viktigheten er lav – og forsvarssektorens evne til å utføre aktiviteten er lavere enn potensielle leverandører. Dette er deler av Forsvarets tilretteleggende virksomhet, og inkluderer ulike administrative oppgaver og deler av Forsvarets støttevirksomhet. Eksempler på aktiviteter i denne kvadranten kan være vedlikehold av administrative kjøretøy, innkjøp av lite kritiske varer, leasing av biler, m.m.

Modell for valg av sourcingstrategi foreslår to handlingsalternativ for aktiviteter i denne kvadranten: Forsvarssektoren kan enten etablere et transaksjonsbasert leverandørforhold eller eliminere aktiviteten. Et transaksjonsbasert leverandørforhold behøver ikke være kortsiktig dersom det er behov for leveranser over en lengre tidsperiode eller det er behov for store volum av leveransene.

4.1.6 Aktiviteter med lav strategisk viktighet der forsvarssektoren har bedre evne til å utføre aktiviteten enn de alternative leverandørene på markedet

Aktiviteter i kvadrant 4 er av lav strategisk viktighet hvor forsvarssektoren selv er bedre i stand til å utføre aktiviteten enn andre alternative leverandører på markedet. I modell for valg av sourcingstrategi nevnes musikk og drill i Forsvaret eller museumstjenester som eksempler på aktiviteter innenfor denne kvadranten. Aktiviteter i denne kvadranten påvirker ikke direkte evnen til å oppfylle Forsvarets formål med blant annet å sikre norsk suverenitet og territoriell integritet.

Siden forsvarssektoren selv er i bedre stand til å utføre aktiviteten, kan det argumenteres for å beholde aktiviteten internt. Samtidig er ikke aktiviteten strategisk viktig, og kan derfor være en kandidat til aktivitet som utføres av eksterne leverandører eller besluttes ikke utført. Dersom forsvarssektoren velger å sette ut aktiviteter i denne kvadranten kan sektoren potensielt spare ressurser.

4.1.7 Svakheter og begrensninger

Modell for valg av sourcingstrategi har noen svakheter og begrensninger. Modellen er kun todimensjonal, og ved komplekse problemstillinger kan dette være noe mangelfullt ved at den blir sensitiv for hvilke kriterier som benyttes. Samtidig kan enkelheten til modellen ses på som en styrke, fordi modellen kan bli mindre anvendbar dersom den blir for kompleks. Videre tar ikke modellen hensyn til avhengigheter. Det foreslås også at modellen bør utvides til et rammeverk med flere steg.

4.2 Skisse til rammeverk for sourcing av Forsvarets IKT-virksomhet

Dette kapittelet tar utgangspunkt i modellen som ble beskrevet i det kapittel 4.1 og knytter inn spesielle forhold rundt IKT generelt, og Forsvarets IKT spesielt. Kapittelet går nærmere inn på hva som kan inngå som en del av handlingsalternativene for strategiske beslutninger om hvorvidt en tjeneste kan utføres med interne ressurser eller om hele eller deler av tjenesten kan leveres som et tjenestekjøp eller samarbeid med én eller flere eksterne virksomheter.

Spørsmålet er hvilke momenter som kan inngå i en slik vurdering for å utvikle handlingsalternativer for aktiviteter og evner innen IKT og plassere alternativene i de ulike kvadrantene. Hvilke vurderinger er det som må gjøres, og hvilke analyser eller verktøy kan organisasjonen benytte som et grunnlag for å utvikle de ulike handlingsalternativene? Det er disse spørsmålene vi søker å svare på i dette kapittelet.

Vurderingene som gjøres tar utgangspunkt i de to teoretiske perspektivene vi har presentert tidligere, nemlig transaksjonskostnadsøkonomi (TCE) og ressursbasert teori (RBV). Dette er to ulike perspektiver, som vi mener kan være relevante å ta med i en vurdering av sourcingstrategi. TCE tar utgangspunkt i kostnader knyttet til transaksjonen som skal gjennomføres, mens RBV

velger handlingsalternativer ut fra en vurdering av hvordan organisasjonens ressurser har innvirkning på konkurransefortrinn. Ved RBV vil det si at de ressurser som er strategisk viktige for at organisasjonen kan oppnå konkurransefortrinn kan beholdes internt i organisasjonen, mens resterende ressurser kan være fra for eksempel en strategisk partner. I tillegg inkluderer vurderingene ikke-kontrollerbare variabler som må hensyntas knyttet til forsvarlig sikkerhet og folkerettslige bestemmelser.

Før det er mulig å utføre vurderinger knyttet til sourcing, må det tas en strategisk beslutning om hvilken del eller hvilke deler av IKT-virksomheten som skal vurderes. Videre må de ulike handlingsalternativer beskrives. Handlingsalternativene innebærer ulike sourcingstrategier, fra å gjøre alt i egen organisasjon til ulike grader av samarbeid med leverandører inkludert langsiktig strategisk partnerskap. Ett av handlingsalternativene kan være basert på dagens situasjon. Disse handlingsalternativene må beskrives i form av hvilke IKT-tjenester, IKT-systemer og/eller IKT-infrastrukturer som kan vurderes og ulike konsepter og samarbeidsformer for dette. Denne beskrivelsen av de ulike handlingsalternativene vil være et utgangspunkt som det jobbes videre med og som justeres, tilpasses og detaljeres ytterligere gjennom sourcingprosessen.

For å strukturere sourcingprosessen slik at viktige momenter belyses, og for å bidra til etterprøvbare, gjennomsiktige og sporbare vurderinger, foreslår vi å utdype modell for valg av sourcingstrategi med syv faktorer. Noen av disse faktorene har direkte innvirkning på handlingsalternativer, eksempelvis at enkelte handlingsalternativ ikke er mulige eller må endres. Andre faktorer kan føre til tiltak som må iverksettes underveis i prosessen eller som må reflekteres som krav til leverandører i eventuelle kontrakter. I det følgende gis en gjennomgang av de syv faktorene.

4.2.1 Operativt fortrinn

I kapittel 2.6.3 introduserte vi begrepet konkurransefortrinn. Litteraturen om konkurransefortrinn tar utgangspunkt i en bedrift som konkurrerer mot andre bedrifter. Konteksten i forsvarssammenheng virker å være noe annerledes. Gjeldende LTP slår fast at det «er behov for å opprettholde Forsvarets operative evne og relative effekt målt opp mot en potensiell motstander» (Forsvarsdepartementet, 2020). Konkurransefortrinn vil derfor i konteksten av Forsvaret, innebære å oppnå en fordel sammenlignet med en potensiell motstander. Et eksempel på en konkurransefortrinn oppnådd gjennom IKT er at bedre tilgang til informasjon kan bidra til at Forsvaret klarer å gjennomføre beslutningsprosesser raskere enn en motstander.

Vi vurderer at begrepet «konkurransefortrinn» ikke vil være gjenkjennelig for aktører i forsvarssektoren og foreslår i stedet å benytte begrepet «operativt fortrinn» i denne sammenheng. Dette begrepet er valgt ut i fra at Forsvaret ønsker å få en økt operativ effekt gjennom å utnytte IKT (Forsvarsstaben, 2021), og at man dermed kan oppnå et fortrinn sammenlignet med en eventuell motstander grunnet tilstandsendringen. Hovedspørsmålet denne faktoren belyser er om Forsvaret kan få et operativt fortrinn sammenlignet med en eventuell motpart ved å utføre en aktivitet internt. Dette spørsmålet kan være vanskelig å svare på. Vi foreslår å bryte problemstillingen ned med en serie spørsmål og analyser for å svare på disse spørsmålene og med forslag til vurderinger av resultater, se tabell 4.1:

Operativt fortrinn	
Spørsmål	1. Er det lettere å reagere på muligheter og trusler fra omgivelsene dersom en aktivitet utføres med interne ressurser fremfor eksterne ressurser?
	2. Blir IKT-en mer robust, og får den bedre sikkerhet og ytelse ved at aktiviteten utføres internt sammenlignet med bruk av eksterne ressurser?
	3. Er det slik at ressursen(e) som er nødvendige for å gjennomføre aktiviteten er kontrollert av et lavt antall konkurrerende organisasjoner?
	4. Er Forsvaret, gjennom strategier og prosedyrer, i stand til å utnytte den verdifulle, sjeldne, ikke-imiterbare kapabiliteten eller ressursen – ved at aktiviteten utføres internt?
Analyser	Analysen kan ta utgangspunkt i VRIO[15]-rammeverket (vedlegg A), som er en analyse av ressurskategorier, med et hensiktsmessig detaljnivå, for å avdekke om de ulike ressursene er verdifulle, sjeldne, ikke imiterbare og om de er utnyttet av organisasjonen.
Resultat og ev. konsekvens for handlings-alternativene	• Dersom svaret på spørsmål 1 er ja, er intern utførelse antakeligvis å foretrekke. Det kan være vanskelig å svare på spørsmål 1, derfor inkluderes spørsmål 2-4. • Er ressursen verken verdifull eller sjelden, dvs. at svarene på ett av spørsmålene 2–4 er «nei», er et transaksjonsbasert leverandørforhold antakeligvis å foretrekke. Ved slike ressurser/kapabiliteter er det gjerne snakk om ulike former for produkter og tjenester med lav kritikalitet, f.eks. standardiserte produkter og tjenester med lite kundetilpasning. • Dersom svaret på spørsmålene 2–4 ovenfor er «ja», tyder det på at ressursen er verdifull eller sjelden og kan gi et operativt fortrinn. I dette tilfellet vil det beste overordnede handlingsalternativet være intern utførelse og ev. hvis behov styrke og utvikle evnen ytterligere gjennom investeringer i materiell og kompetanse.

Tabell 4.1 Forslag til spørsmål som kan stilles knyttet til faktoren operativt fortrinn, analyser som kan gjøres samt resultater og eventuelle konsekvenser for ulike handlings-alternativer.

4.2.2 Forsvarlig sikkerhetsnivå

Forsvarlig sikkerhetsnivå er en faktor vi anbefaler bør inngå i rammeverket. Årsaken til utvidelsen er at forsvarlig sikkerhetsnivå for Forsvarets IKT-virksomhet er avgjørende for å ivareta Forsvarets operative evne og nasjonale sikkerhetsinteresser – og det er et lovpålagt krav i henhold til sikkerhetsloven (se kapittel 3).

Forsvaret kan overlate oppgaver til sivile aktører, men kan ikke overlate det overordnede ansvaret for forebyggende sikkerhet og sikkerhetsstyring som skal sørge for at IKT-virksomheten har et forsvarlig sikkerhetsnivå for skjermingsverdige verdier, herunder skjermingsverdig informasjon, informasjonssystem, objekter og infrastruktur. Forsvaret har ansvar for at sivile

[15] *Valuable, Rare, Imitable, Organized*.

leverandører har tilstrekkelig risiko- og sikkerhetsforståelse og gjennomfører oppgavene slik at et forsvarlig sikkerhetsnivå ivaretas.

Forsvarlig sikkerhetsnivå er dermed en kritisk faktor som må vurderes og sikres ivaretatt ved sourcing, se tabell 4.2 for spørsmål, analyser og resultat og konsekvens av handlingsalternativene. Sikkerhet må inkluderes helt fra starten av prosessen slik at en vurdering av risiko og eventuelle sikkerhetstiltak tas inn i handlingsalternativene, og at «røde flagg» ikke dukker opp sent i partnerdialogen.

Forsvarlig sikkerhetsnivå	
Spørsmål	1. Hva er risiko og status for forsvarlig sikkerhetsnivå for dagens situasjon? 2. Hva er risiko for de andre handlingsalternativene? 3. Hvordan kan et forsvarlig sikkerhetsnivå oppnås for handlingsalternativene (krav og tiltak)? Dersom det ikke er mulig å oppnå et forsvarlig sikkerhetsnivå, må dette begrunnes.
Analyser	• For å besvare spørsmålene må det utføres helhetlige verdi- og risikovurderinger basert på en god systemforståelse. Forsvaret må ha evne til å vurdere sine verdier, dvs. definere behov og hvilken betydning og kritikalitet som er knyttet til handlingsalternativene for Forsvarets operative evner. Dermed må Forsvaret forstå og synliggjøre hvordan IKT griper inn i og er integrert i militære evner. Dette er nødvendig for å vurdere operative konsekvenser og de skadefølger det kan få dersom skjermingsverdige verdier blir utsatt for ulike former for sikkerhetstruende virksomhet. Dette er igjen grunnlag for å definere sikkerhetskrav for IKT-virksomheten. • I en utviklings- og anskaffelsesfase er dette grunnlag for å vurdere alternative løsninger for å oppnå et forsvarlig sikkerhetsnivå, og sammen med andre vurderinger (kost, nytte, m.m.) velge beste løsning. Forsvaret må ha teknologiforståelse, dog ikke om alle detaljer, men nok til en kunnskapsbasert dialog og vekselvirkning med partneren (bestillerkompetanse).
Resultat og ev. konsekvens for handlings-alternativene	Ved å besvare spørsmål 1–3 og gjennomføre analysene beskrevet, vil Forsvaret ha et grunnlag for å vurdere forsvarlig sikkerhetsnivå for hvert handlingsalternativ. Valg av handlingsalternativ må baseres på vurdering av risiko og forsvarlig sikkerhetsnivå for dagens situasjon opp mot de ulike handlingsalternativene forsvarssektoren vurderer i forbindelse med sourcing. Det er FSJ som leder av Forsvaret som er ansvarlig for eventuell restrisiko. For de andre etatene i forsvarssektoren er det etatenes leder som har dette ansvaret.

Tabell 4.2 Forslag til spørsmål som kan stilles knyttet til forsvarlig sikkerhetsnivå, analyser som kan gjøres samt resultater og eventuelle konsekvenser for ulike handlingsalternativer.

4.2.3 Krigens folkerett

Planlegging og innretting av Forsvarets virksomhet i væpnet konflikt må skje i henhold til krigens folkerett. Folkerettslige vurderinger er særlig viktig når militær og sivil virksomhet knyttes sammen, og der Forsvaret blir avhengig av sivile aktørers bidrag. Selv om en del oppgaver innen IKT-virksomheten er ett område hvor tjenester i prinsippet kan utføres av sivile uten å bryte folkeretten og nasjonale bestemmelser, må implikasjonene vurderes i hvert konkrete tilfelle. I henhold til nasjonale bestemmelser forutsettes funksjoner som innebærer direkte deltakelse i fiendtlighetene i en væpnet konflikt at disse utføres av lovlig stridende militært personell, ikke sivile personer, verken sivilt ansatte i Forsvaret, i forsvarssektoren for øvrig, eller sivile kontraktører. Hensynet til krigens folkerett kan medføre at et handlingsalternativ for sourcing innen IKT-virksomheten vurderes å være i strid med krigens folkerett, og dermed ikke gjennomførbart. Alternativt, kan folkerettslige hensyn medføre justeringer og endringer av handlingsalternativenes innretning og ulike typer tiltak etter hvert som sourcingprosessen skrider frem. Det er flere hensyn å ta.

Se kapittel 3.5 for en kort introduksjon til noen av de problemstillinger innen krigens folkerett det vil være viktig å vurdere som ledd i en sourcingprosess innen IKT-virksomheten. Det må gjøres konkrete folkerettslige vurderinger fra sak til sak, og de folkerettslige vurderingene må inngå i hele sourcingprosessen og oppdateres etter hvert som mer detaljer om sivile leveranser og partnerskap kommer på plass. Forsvaret må følgelig sørge for å:

- Konkretisere hvilke funksjoner innen IKT-virksomheten som utgjør direkte deltakelse i fiendtlighetene og unngå at disse planlegges utført av sivile. Slike oppgaver skal utføres av lovlig stridende personell i væpnet konflikt.

- Identifisere hvilke funksjoner innen IKT-virksomheten som sivile kontraktører kan utføre uten å utfordre krigens folkerett og nasjonale bestemmelser.

- Utføre risikovurderinger for sivil følgeskade som ledd i sourcing for å holde denne risikoen så lav som mulig.

- Vurdere samfunnsmessige konsekvenser for kritiske samfunnsfunksjoner samt sivilbefolkningen ved sourcing for å sørge for at måten Forsvaret innretter seg på ikke motvirker en motparts evne, eller vilje, til å beskytte disse.

I tabell 4.3 listes noen spørsmål Forsvaret bør stille for å sikre at bestemmelser innen krigens folkerett ivaretas. Det presiseres at spørsmålene i tabellen ikke må anses å være uttømmende.

Krigens folkerett	
Spørsmål	1. Hvilke funksjoner og oppgaver i væpnet konflikt innebærer de ulike handlingsalternativene for sivil partner/leverandør? Utgjør disse oppgavene direkte deltakelse i fiendtlighetene etter krigens folkerett og må utføres av militært personell, eller er oppgavene av en art sivilt personell kan utføre? 2. Hvilken status i henhold til folkeretten vil sivile kontraktørers personell få ved tilfangetakelse av motparten? Er funksjonene av en slik art at Forsvaret bør gi personellet status som «sivile som følger de væpnede styrker» jf. tredje Genèvekonvensjon av 1949 art. 4 A nr. 4, og dermed ha rett til krigsfangestatus selv om de ikke er stridende personell? 3. Hvilke farer ved militære operasjoner kan handlingsalternativene innebære for sivile? Hvilken risiko innebærer handlingsalternativene for følgeskade på sivile personer og objekter dersom motparten angriper militære objekter eller stridende personer (både cyberangrep og konvensjonelle kinetiske angrep)? Er det andre virkninger av fiendtlighetene enn følgeskade ved angrep sivile kan bli utsatt for? Hvilke eventuelle tiltak, eller justeringer i handlingsalternativer, må til for å sørge for at risikoen for sivile er tilstrekkelig lav? 4. Innebærer handlingsalternativene at sivil virksomhet, objekter eller infrastruktur som det sivile samfunnet er avhengig av, også får en militær funksjon, og dermed kan bli vurdert av en motstander som et lovlig militært mål i henhold til reglene om når objekter blir lovlige mål i krigens folkerett? Hvilke skadefølger kan dette få for kritiske samfunnsfunksjoner og sivilbefolkningen? Er dette et akseptabelt risikonivå, eller må handlingsalternativer enten utelates eller endres?
Analyser	• Det må gjøres konkrete folkerettslige vurderinger etter krigens folkerett fra sak til sak. Hva en ev. leverandør konkret skal levere til Forsvaret av IKT-systemer og -tjenester, utvikles ofte i en dialog og gjennom forhandlinger mellom partene. Derfor må de folkerettslige vurderingene inngå i hele sourcingprosessen og oppdateres etter hvert som mer detaljer om sivile leveranser og partnerskap kommer på plass. Vurderingene må baseres på tilstrekkelig innsikt i hva de ulike handlingsalternativene innebærer i væpnet konflikt, og hvilke forutsetninger for IKT-virksomheten som ligger i Forsvarets planverk. • For å kunne vurdere folkerettslige forhold, konsekvenser og mulige tiltak må kompetanse innen krigens folkerett involveres. Slik kompetanse finnes bl.a. i FD og ved Forsvarets høgskole. • For å besvare spørsmål 4, er det nødvendig både med innsikt om sivil partner/ leverandør og dennes leveranser til samfunnskritisk virksomhet, og hvilken annen aktivitet som eventuelt er samlokalisert med viktige IKT-funksjoner for Forsvaret i de ulike handlingsalternativene.

Krigens folkerett	
Resultat og ev. konsekvens for handlings-alternativene	Valg knyttet til sourcing må baseres på vurdering av folkerettslige konsekvenser for dagens situasjon opp mot de ulike alternativene man vurderer å innføre. Ved faktoren krigens folkerett vil det derfor ikke være klare anbefalinger av handlings-alternativer, siden disse vurderingene er sammensatte. Hvert av de konkrete tilfellene må vurderes av en sammensatt gruppe med ekspertise innen krigens folkerett, IKT og militære operasjoner.

Tabell 4.3 Forslag til spørsmål som kan stilles knyttet krigens folkerett, analyser som kan gjøres samt resultater og eventuelle konsekvenser for ulike handlingsalternativer.

4.2.4 Transaksjonskostnader

Vi har valgt å ta med transaksjonskostnader som en faktor som kan vurderes spesifikt i en IKT-kontekst. I forbindelse med den strategiske beslutningen som tas knyttet til hvorvidt en tjeneste kan utføres med interne ressurser eller om hele eller deler av tjenesten kan leveres som et tjenestekjøp eller samarbeid med ekstern virksomhet, vil det være nødvendig med en vurdering av transaksjonskostnader. Transaksjonskostnader vil, som tidligere nevnt, omhandle alle kostnader organisasjonen har i forbindelse med å gjennomføre en bestemt handel, både i forkant underveis og i etterkant av selve handelen.

Vi ønsker å synliggjøre faktoren transaksjonskostnader, for å bevisstgjøre og synliggjøre kostnader knyttet til ressurser, oppfølging og vedlikehold av tjenesten, dersom tjenesten kan leveres som et tjenestekjøp eller strategisk samarbeid. Vi har valgt å behandle de tre kritiske aspektene ved en transaksjon (1) usikkerhet[16], (2) frekvens og hyppighet[17] og (3) transaksjonsspesifikke investeringer[18] jamfør Williamson (1979) samlet under denne faktoren. Digitale verdikjeder øker i omfang og kompleksitet, hvor momenter som hvem som eier, vedlikeholder og opererer de forskjellige delene inngår. Ved etablering av en overordnet oversikt over hvilke digitale tjenester som utveksles mellom de forskjellige delene i verdikjeden, vil transaksjonskostnader avdekkes, både med tanke på usikkerhet, frekvens og graden av spesifisitet i aktiviteten.

Overordnet vil spørsmål om transaksjonskostnader være knyttet til forholdet mellom interne produksjonskostnader og transaksjonskostnader – og hva som er billigst for organisasjonen, se tabell 4.4.

[16] Usikkerhet er som nevnt knyttet til flere andre problemstillinger, og inngår i begrenset rasjonalitet og opportunistisk atferd, som vi presenterer som egne faktorer. De atferdsmessige mekanismene er egne faktorer for å synliggjøre kritikaliteten og viktigheten av at disse faktorene inngår i vurdering av handlingsalternativer. Samtidig inngår momenter knyttet til atferdsmekanismer også i transaksjonskostnader, grunnet den gjensidige avhengigheten. Se kapittel 5.6 for begrenset rasjonalitet og kapittel 5.7 for opportunistisk atferd. Usikkerhet er også en del av operativt fortrinn, forsvarlig sikkerhetsnivå og krigens folkerett. Det vil si at usikkerhet behandles under hver av faktorene, og ikke bare under faktoren transaksjonskostnader (i spørsmål 1–2 i tabell 5.4).

[17] Behandles for faktoren transaksjonskostnader i spørsmål 3 i tabell 5.4.

[18] Behandles for faktoren transaksjonskostnader i spørsmål 4–6 i tabell 5.4.

Transaksjonskostnader	
Spørsmål	1. Hvor raskt går den teknologiske utviklingen innenfor den aktuelle tjenesten og tilhørende digitale verdikjeder?
	2. Er det potensiale for at det er store endringer som vil skje grunnet denne teknologiske utviklingen? Hva med økning i kompleksitet ved digitale verdikjeder mtp. eierskap, vedlikehold m.m.? Er det mulig å si noe om ev. konsekvenser av disse endringene, f.eks. ifm. digitale verdikjeder?
	3. Hvor hyppig skal transaksjonen gjennomføres?
	4. Forutsetter handlingsalternativet investering i en ressurs med høy spesialisering? Eller er den generell?
	5. Innebærer handlingsalternativet leverandør- eller kundetilpassede ressurser?
	6. Innebærer handlingsalternativet personell med spesifikk kompetanse?
	7. Hvordan er det tenkt at forsvarssektoren i det daglige skal ha oppfølging av ev. strategisk partner? Hvilke kontrollmekanismer kan inkluderes i en ev. kontrakt? Hvordan kan ev. endringer i en kontrakt håndteres dersom det oppstår uforutsette behov for dette?
	8. Er det behov for strukturelle endringer i organisasjonen dersom forsvarssektoren går for strategisk partnerskap? Hvilke koordinerings- og omstillingskostnader vil påtreffe ved endring av organisasjon?
Analyser	• I forkant av en kontraktsinngåelse er det nødvendig å kartlegge informasjonsbehovet ifm. inngåelsen av strategisk partnerskap og gjennomføre analyser av markedet. Videre er det nødvendig å gjennomføre en kartlegging og en analyse av ulike leverandører i forkant av utarbeidelse av konkurransegrunnlag og ulike former for utlysninger. Dette innebærer å: • Kartlegge forhandlingskostnader, inkl. ressursbruk for sporbarhet og gjennomsiktighet i de vurderinger som ligger til grunn for hvert av handlingsalternativene. • Utarbeide en kostnadsoversikt ifm. selve kontraktinngåelsen og hva som kan inngå i denne. • Kartlegge hvordan forsvarssektoren kan følge opp strategisk partner i det daglige, og basert på kartleggingen(e) etablere rutiner for oppfølging. • Gjennomføre en systematisk kompetanseanalyse, for å avdekke kompetansebehov (se kompetansebehov i kapittel 4.2.5). Hvilke transaksjonskostnader vil påtreffe ved ev. kompetanseoverføring fra forsvarssektoren til strategisk partner? • Gjøre en vurdering basert på usikkerhet, frekvens og hyppighet og graden av transaksjonsspesifikke investeringer, for å kartlegge hvor høye transaksjonskostnadene vil bli (se også faktor om forsvarlig sikkerhetsnivå kapittel 4.2.2 og faktor om risiko for opportunisme kapittel 4.2.7). Ved et punkt vil transaksjonskostnadene bli så høye at det lønner seg å gjennomføre aktiviteten internt ved å investere i egne ressurser.

Transaksjonskostnader	
Resultat og ev. konsekvens for handlings-alternativene	• Høy usikkerhet om transaksjonskostnader peker i retning av intern utførelse i stedet for ekstern utførelse. • Dersom svaret på spørsmål 3 er lav frekvens, indikerer dette transaksjons-basert leverandørforhold og ikke strategisk partnerskap. • Dersom transaksjonene har høy frekvens vil et mer langsiktig alternativ (intern utførelse eller langsiktig kontrakt med ekstern leverandør) bidra til redusere kostnader til å lete etter leverandør, innhente informasjon, forhandling osv. • Det er mer utfordrende å identifisere egnede leverandører og forhandle med disse dersom ressursene må være spesialtilpassede. Spesialtilpassede ressurser vil kunne kreve mer oppfølging, og kostnaden ved feil vil trolig øke. • Høy transaksjonsspesifisitet kombinert med faktorer som opportunisme og usikkerhet kan gi ulike uheldige effekter, som leverandør- eller kunde-avhengighet med tilhørende innlåsingseffekter og forhøyede byttekostnader. • Et stort omfang av spesifikke investeringer taler generelt for at relasjonen til leverandøren kan opprettholdes over tid, gitt at intern utførelse ikke er et alternativ. Et bytte av leverandør vil medføre at verdien av investeringene reduseres og kan også føre til høye byttekostnader.

Tabell 4.4 Forslag til spørsmål som kan stilles knyttet transaksjonskostnader, analyser som kan gjøres samt resultater og eventuelle konsekvenser for ulike handlings-alternativer.

4.2.5 Kompetansebehov

I kapittel 4.2.3 og 4.2.4 var vi inne på kompetanse. Vi ser kompetanse som en avgjørende faktor, og har derfor valgt å legge til kompetanse som en egen faktor, for å synliggjøre kritikaliteten av kompetansedimensjonen i valg av handlingsalternativer for sourcing. Både RBV og TCE vektlegger kompetanse som en faktor av betydning i utarbeidelser av alternativer for sourcing.

I utarbeidelse av ulike handlingsalternativer vil det derfor være behov for å avdekke hvilken kompetanse organisasjonen har behov for internt, og hvilken kompetanse strategisk partner kan inneha.

> IKT-virksomheten må derfor forstå hvilken type kompetanse som må utvikles og/eller styrkes internt, og hvilke typer kompetanse som kan fases ut. En stadig økende mangel på personell med teknologikompetanse, gjør at IKT-virksomheten også må forstå hvilke sårbarheter som kan oppstå ved manglende kompetanse, og hvilke konsekvenser dette kan få. (Birkemo et al., 2021 s. 11).

Som nevnt tidligere er denne faktoren tett knyttet til de andre faktorene i vår utvidelse av modell for valg av sourcingstrategi, slik at momenter under denne faktoren vil sammenfalle med andre vurderinger vi har foreslått tidligere.

Kompetansebehov	
Spørsmål	1. Hvilken kompetanse kreves, dvs. er nødvendig/kritisk, for gjennomføring av kjernevirksomheten? • Hvilken type kompetanse er forsvarssektoren avhengig av internt for å gjennomføre daglig drift av kjernevirksomheten? Hvilken evne har forsvarssektoren til å ivareta driftsoppgavene internt? Hvilken evne har ev. strategiske partnere til å ivareta disse oppgavene? • Er det ikke-kontrollerbare variabler, som lover og regler, som setter føringer for hva slags kompetanse som må beholdes internt? Basert på dette, hvilken type kompetanse må videreutvikles internt?
	2. Hvilken type kompetanse kan settes ut til en ev. strategisk partner eller håndteres som et tjenestekjøp? • Hvilke sårbarheter vil ev. mangelen på en intern kompetanse medføre? Og hvilke konsekvenser kan det få? • Er det slik at risikoen ved å sette kompetanse ut til partner veier opp for muligheten for å ikke ha denne kompetansen i det hele tatt? • Er det en risiko for at kompetansen/personellet forsvarssektoren ønsker å beholde forsvinner ved ev. avgjørelse om tjenesteutsetting?
Analyser	Følgende analyser kan gjøres: • Gjennomføre en systematisk kompetanseanalyse som avdekker hvilken form for kompetanse som kreves for å kunne understøtterkjernevirksomheten med IKT. Analysen kan ta utgangspunkt i det generiske rammeverkets dimensjoner strategisk viktighet og relativ evne.[19] • Gjennomføre en overordnet, tilpasset SWOT[20]-analyse, som kan være et rammeverk for å avdekke styrker og svakheter internt mtp. digital kompetanse for kjernevirksomheten. Styrker vil være kompetanse som forsvarssektoren innehar og som muliggjør gjennomføring av kjernevirksomheten til Forsvaret. Svakheter vil være områder hvor forsvarssektoren mangler kompetanse internt, slik at det går utover kvaliteten til kjernevirksomheten. I tillegg kan rammeverket avdekke muligheter og farer dersom hele eller deler av tjenesten kan leveres som et tjenestekjøp eller samarbeid med ekstern virksomhet. • Gjennomføre en gapanalyse, som avdekker om det eksisterer et gap mellom kompetansen forsvarssektoren har og kompetansen man trenger.
Resultat og ev. konsekvens for handlingsalternativene	Ved aktivitet i kvadrant 1 med høy strategisk viktighet og lav relativ evne for forsvarssektoren er samarbeidsbasert leverandørforhold å foretrekke, under forutsetning av at leverandøren har den aktuelle kompetansen som en del av sin kjernevirksomhet. Alternativt kan forsvarssektoren bygge opp egen kompetanse innenfor området. Aktiviteter som plasseres i kvadrant 2 innebærer kompetanse som inngår som en del av kjernevirksomheten, og forsvarssektoren selv er best til å gjennomføre denne aktiviteten. I disse tilfellene må kompetansen beholdes

[19] Dersom organisasjonens kjernevirksomhet ikke er definert må dette gjøres på forhånd.
[20] *Strengths*, *weaknesses*, *opportunities*, *threats*.

Kompetansebehov	
	internt. Ved aktivitet i kvadrant 3 med lav strategisk viktighet – og forsvarssektoren har selv lavere evne enn potensielle leverandører – kan kompetansen på disse feltene overlates til en tredjepart. Aktiviteter i kvadrant 4 er aktiviteter med lav strategisk viktighet og hvor forsvarssektoren selv er i bedre i stand til å utføre aktiviteten enn andre alternative leverandører. Siden forsvarssektoren selv har bedre kompetanse kan det argumenteres med å beholde aktiviteten internt, samtidig som den lave strategiske viktigheten kan gjøre at kompetansen kan være hos eksterne leverandører. Vurderinger knyttet til folkerettslige prinsipper og forsvarlig sikkerhetsnivå vil være avgjørende for om kompetansen kan ivaretas eksternt eller må beholdes internt. Dersom et handlingsalternativ blir en eller annen form for samarbeid, anbefales det å lage kompetanse- og vedlikeholdsplaner sammen med strategisk partner, slik at samarbeidspartnere har god virksomhetsforståelse for forsvarssektoren. «En anbefalt måte å oppnå dette på er tett integrasjon mellom IKT-virksomheten og strategiske partnere. Dette vil bidra til gjensidig kompetanseutveksling og tillit, og vil også være avgjørende for å oppnå felles forståelse av hva som er de beste løsningene basert på forsvarssektorens behov.» (Birkemo et al., 2021 s. 75).[21] Forsvarssektoren må ha god strategisk IKT-styringskompetanse internt: • Angående transaksjonskostnader må forsvarssektoren følge opp kontrakt(er), leverandør(er), ivareta forsvarlig sikkerhetsnivå osv. • Ved strategisk partnerskap må forsvarssektoren vedlikeholde en viss grad av den kompetansen som settes ut internt – slik at forsvarssektoren får fulgt opp strategisk partner på en tilfredsstillende måte. • Forsvarssektoren må være klar over manglende innovasjonskapasitet siden mye som overlates til strategisk partner. • Ved høy strategisk viktighet og høy relativ evne kan kompetansen beholdes internt med ambisjon om å forsterke evnen ytterligere. Basert på gapanalysen bør forsvarssektoren etablere planer for motivering, kompetanseutvikling og rekruttering av den kompetansen forsvarssektoren må beholde internt.

Tabell 4.5 Forslag til spørsmål som kan stilles knyttet kompetansebehov, analyser som kan gjøres samt resultater og eventuelle konsekvenser for ulike handlingsalternativer.

[21] Kan også ses i sammenheng med opportunisme, se kapittel 4.2.7

4.2.6 Begrenset rasjonalitet

Som vi har skrevet tidligere i rapporten (kapittel 2.5.2) er det en utopi at beslutningstakere kan imøtekomme kravet til rasjonelle beslutninger ved valg av sourcingstrategi siden mennesker ikke klarer å overskue alle konsekvenser av de ulike handlingsalternativene som vurderes.

Begrenset rasjonalitet vil inngå også i de andre faktorene i vår skisse til rammeverk, for eksempel kan begrenset rasjonalitet inngå i faktoren transaksjonskostnader der hvor transaksjonen krever spesifikke investeringer og når teknologiutviklingen er rask. Komplekse avtaler, slik som en avtale om strategisk partnerskap innen IKT, vil kun ta høyde for hva de deltakende aktører er i stand til å tenke på som kan skje – og ikke dekke alt som faktisk kan skje. Dette kan føre til at avtalene ikke dekker oppdukkende situasjoner noe som igjen kan medføre risiko for konflikter og potensielle reforhandlinger. Vi har derfor valgt å inkludere begrenset rasjonalitet som en egen faktor i modellen for å sikre at disse problemstillingene eksplisitt blir vurdert.

Begrenset rasjonalitet	
Spørsmål	1. Hvordan kan forsvarssektoren best kravstille, slik at organisasjonen har mulighet til å følge med i IKT-utviklingen basert på endrede behov? Kan det være vanskelig å vurdere hva man har opp mot hva man vil få? Er det risiko for å bli påvirket av «oversalg» fra potensielle partnere?[22]
	2. Forsvarssektoren bruker dialogfase. Hva kan være fallgruver i dialogprosessen? Kan forsvarssektoren ha for høy tillit til hva tilbyderne sier? Er tilbydere gode selgere? Hvordan mottar forsvarssektoren informasjonen?[23]
	3. Hvordan sikrer forsvarssektoren sporbarhet og gjennomsiktighet i prosessen, for å sikre at begrunnelsene for de ulike handlingsalternativene er kjent og pålitelige i etterkant?
	4. Hvordan sikrer forsvarssektoren og en ev. strategisk partner en felles forståelse av forsvarlig sikkerhetsnivå? Hvordan sikres virksomhetskompetanse som den strategiske partneren må inneha for å ivareta et forsvarlig sikkerhetsnivå?[24]
	5. Hvilke punkter i kontrakten kan konkretiseres, for å redusere muligheter for konflikt og reforhandling?
Analyser	Det går ikke an å analysere seg bort fra begrenset rasjonalitet, siden vi ikke vet hva vi ikke vet. Pilotering og andre risikoreduserende tiltak bør vurderes for å motvirke omfanget og konsekvenser av begrenset rasjonalitet. Det bør etableres et rammeverk for helhetlig dokumentasjon og sporing i prosessen, som er omforent mellom partene.

[22] Dette spørsmålet kan ses i sammenheng med risiko for opportunisme i kapittel 4.2.7.
[23] Ibid.
[24] Dette spørsmålet kan ses i sammenheng med kompetansebehov i kapittel 4.2.5.

Begrenset rasjonalitet	
Resultat og ev. konsekvens for handlings-alternativene	Dersom man gjennom arbeidet med disse spørsmålene avdekker områder der det er divergens, er det av betydning at partene setter seg ned og kommer til en omforent forståelse av innholdet. Det må etableres rutiner eller mekanismer med forventningsavklaringer for de ulike partene.

Tabell 4.6 Forslag til spørsmål som kan stilles knyttet begrenset rasjonalitet, analyser som kan gjøres samt resultater og eventuelle konsekvenser for ulike handlings-alternativer.

4.2.7 Risiko for opportunisme

Risiko for opportunisme er hentet fra TCE og henger tett sammen med analyser av transaksjons-kostnader. Samtidig er risiko for opportunisme potensielt høy ved inngåelse av strategiske part-nerskap. Vi har derfor valgt å ha risiko for opportunisme som en egen faktor, for å synliggjøre problemstillinger forsvarssektoren må være klar over innenfor denne tematikken. Eksempelvis kan det være slik at leverandører eller strategiske partnere velger å prioritere andre markeder enn forsvarssektoren. En slik omprioritering fra strategiske partnere kan for eksempel medføre at de bruker mer tid og ressurser på andre kunder, og det kan også være at de utnytter de transaksjonsspesifikke investeringene – som forsvarssektoren har investert i – i andre markeder.

Risiko for opportunisme	
Spørsmål	1. Ved en ev. overføring av aktiviteten til strategisk partner – kreves det spesifikke investeringer hos partneren? Er det slik at den strategiske partneren senere kan utnytte disse ev. investeringene i andre markeder[25], for deretter å nedprioritere den strategiske avtalen som er inngått?
	2. Vil det være en balanse eller likevekt mellom ansvar fordelt mellom partene i det strategiske samarbeidet?
	3. Hvordan kan risikoen og kostnadene deles mellom partene som inngår strategisk partnerskap?
	4. Hvilke styringsmekanismer kan etableres for å kontrollere at partene i det strategiske samarbeidet er likeverdige?
	5. Kan en ev. innlåsingseffekt utgjøre en risiko, og hvor stor grad av innlåsing er i så fall akseptabelt for forsvarssektoren?[26]

[25] Dersom dette er tilfellet bør det fremheves som en viktig tilretteleggende effekt for samarbeid.
[26] Transaksjonsspesifikke investeringer vil være sentrale her. En høy spesifisitet kan gi innlåsingseffekter/høye bytte-kostnader – noe som igjen kan gjøre det vanskelig for nye leverandører å konkurrere når tjenesten skal reanskaffes eller kontrakten reforhandles. Dette fordi forsvarssektoren ikke vil få byttekostnadene dersom de beholder den eksis-terende leverandøren. Den eksisterende leverandøren har dermed et fortrinn sammenlignet med øvrige leverandører. Dette vil kunne påvirke prisutviklingen for tjenesten negativt (gitt at leverandøren er opportunistisk og utnytter fordelen).

Risiko for opportunisme	
Analyser	Analyse av risiko for opportunisme må ses i sammenheng med de faktorene som foreslås under forsvarlig sikkerhetsnivå. Dvs. at det må utføres helhetlige verdi- og risikovurderinger basert på en god systemforståelse. Inkl. i dette er en vurdering av de ulike punktenes strategiske betydning, hvilke verdier som inngår og definere behov og hvilken betydning og kritikalitet som er knyttet til handlingsalternativene for Forsvarets operative evner.
Resultat og ev. konsekvens for handlings-alternativene	Dersom det vurderes at risiko for opportunisme er høy, kan det vurderes å holde aktiviteten internt, spesielt dersom det er høy strategisk viktighet for aktiviteten som gjennomføres. Ved inngåelse av strategisk partnerskap må det være en bevissthet knyttet til fordeling av risiko og kostnader, slik at det blir redusert risiko for opportunisme.

Tabell 4.7 Forslag til spørsmål som kan stilles risiko for opportunisme, analyser som kan gjøres samt resultater og eventuelle konsekvenser for ulike handlingsalternativer.

5 Konklusjon

Samarbeid mellom forsvarsektoren og næringslivet har fått økt oppmerksomhet i de siste tre langtidsperiodene. Forsvarsdepartementet har etablert prinsippet *så sivilt som mulig og så militært som nødvendig* for å nyttiggjøre seg av både ressurser og kompetanse som allerede finnes i næringslivet (Forsvarsdepartementet, 2021c).

Formålet med denne rapporten er å identifisere faktorer det bør tas hensyn til ved vurdering av sourcing for Forsvarets IKT-virksomhet. Sourcing er en strategisk beslutning om hvorvidt en tjeneste skal utføres med interne ressurser eller om hele eller deler av tjenesten skal leveres som et tjenestekjøp eller samarbeid med ekstern virksomhet. De identifiserte faktorene danner grunnlaget for vår skisse til rammeverk for en strukturert sourcingprosess for IKT-området.

Ved utarbeidelsen av vårt anbefalte rammeverk har vi tatt utgangspunkt i en modell for valg av sourcingstrategi for Forsvaret og utvidet denne modellen ved å knytte inn spesielle forhold rundt IKT generelt, og IKT i Forsvaret spesielt. Rapporten går nærmere inn på hvilke spørsmål som bør stilles i utarbeidelsen av ulike handlingsalternativer for sourcing på IKT-området, hvilke analyser som kan gjøres for å få svar på spørsmålene samt hvilke vurderinger som kan gjøres på bakgrunn av disse analysene. Rapporten peker dermed på hvilke vurderinger og analyser som kan inngå for å utvikle og sammenligne handlingsalternativer. Dette kan utgjøre et metodisk underlag for strategiske beslutninger om hvorvidt en tjeneste kan utføres med interne ressurser

eller om hele eller deler av tjenesten kan leveres som et tjenestekjøp eller samarbeid med ekstern virksomhet.

Vårt anbefalte rammeverk består av syv faktorer det er viktig å belyse og dokumentere i et slikt beslutningsgrunnlag: operativt fortrinn, forsvarlig sikkerhetsnivå, krigens folkerett, transaksjonskostnader, kompetansebehov, begrenset rasjonalitet og risiko for opportunisme. Faktorene er utarbeidet på grunnlag av ressursbasert teori og transaksjonskostnadsøkonomi.

For å velge mellom handlingsalternativer for en gitt aktivitet eller aktiviteter relatert til IKT, anbefaler vi at de ulike må vurderes helhetlig. Helhetlig vil her si at faktorene ikke kan ses i isolasjon fra hverandre, men at de bør ses i sammenheng når de ulike handlingsalternativene vurderes opp mot hverandre.

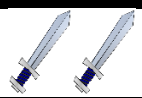
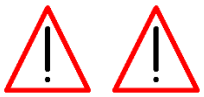
Det anbefales at forsvarssektoren foretar helhetlige risikovurderinger inkludert vurderinger av usikkerhet som grunnlag for sikkerhetsmål for å oppnå et forsvarlig sikkerhetsnivå for verdiene i sektoren. Inkludert i dette ligger det en vurdering av alternative sourcingløsninger og konsekvenser innen sikkerhet. For å kunne være i stand til å gjennomføre en slik vurdering kreves det kunnskap i hele spennet fra operativ kontekst og helt ned til teknologi. Risikobildet må kontinuerlig oppdateres i lys av endringer innen verdier, sårbarheter og trusler.

For å velge mellom ulike handlingsalternativer for sourcingløsninger for IKT-virksomheten må de ulike faktorene fra kapittel 4.2 presenteres og vurderes samlet. Beslutningstakere må presenteres for et beslutningsunderlag som setter dem i stand til å veie ulike hensyn mot hverandre og ta informerte valg. Et sentralt moment i så måte er at faktorene ikke er direkte sammenlignbare. De har verken samme dimensjon eller samme relative vekt og kritikalitet i en samlet vurdering. Det vil si at det ikke er mulig å benytte en kvantitativ sammenligning av de ulike handlingsalternativene der resultatet fra de ulike faktorenes vurdering gis en score, og at disse deretter legges sammen til en samlet score for hver alternative sourcingløsning. Vi fraråder sterkt en slik fremgangsmåte. Formålet med tabell 5.1 er å tydeliggjøre nettopp dette.

Tabell 5.1 viser en fiktiv enkel fremstilling av resultatene av en vurdering der tre tenkte handlingsalternativer for sourcing skal sammenlignes. Vi anbefaler at alle syv faktorer inngår i vurdering av ulike handlingsalternativer. Vi gir et uformelt og enkelt forslag til hvordan resultatet av vurderinger av ulike faktorer for de ulike handlingsalternativene visuelt kan fremstilles. Vi foreslår å bruke grafiske symboler som tydelig viser at faktorene ikke er sammenlignbare slik at man ikke blir fristet til å kvantifisere resultatene og legge sammen til en samlet score. I et beslutningsunderlag er det viktig at resultatet av vurderinger forklares godt og presist, og at usikkerheter knyttet til vurderingene også forklares.

Hvilket handlingsalternativ en til slutt velger, vil være avhengig av hvordan de ulike faktorene kvalitativt blir vektlagt opp mot hverandre. Eksempelvis inngår ikke-kontrollerbare faktorer som må vurderes, forsvarlig sikkerhetsnivå og ivaretakelse av krigens folkerett. For et tenkt alternativ 3 kan resultatet for faktoren krigens folkerett være at dette alternativets innretning av IKT-baserte funksjoner strider mot folkerettslige prinsipper. Dette illustreres derfor med et stoppskilt. Alternativ 3 slik det er innrettet er derfor ikke gjennomførbart, og en må derfor enten

forkaste eller endre alternativet. Å justere alternativet kan være hensiktsmessig i og med at alternativet relativt sett vil gi det høyeste operative fortrinnet og også de laveste transaksjonskostnadene. Ved at organisasjonen vektlegger noen faktorer høyere enn andre, kan de handlingsalternativene som tilfredsstiller disse faktorene være å foretrekke, i motsetning til handlingsalternativer hvor disse faktorene ikke har et tilfredsstillende nivå.

Handlings-alternativ / Faktor	1	2	3
Operativt fortrinn			
Forsvarlig sikkerhetsnivå			
Krigens folkerett			
Transaksjonskostnader			
Kompetansebehov			
Begrenset rasjonalitet			
Risiko for opportunisme			

Tabell 5.1 Forslag til fremstilling av resultater for vurderinger av de sju faktorene for tre fiktive handlingsalternativer knyttet til sourcing for Forsvarets IKT-virksomhet.

Tabell 5.1 er ment som en forenklet illustrasjon som kan benyttes i dialog med beslutningstakere. Den samlede vurderingen, begrunnelser, avveininger og anbefalinger knyttet til handlingsalternativene kan ikke forenkles, men må inkluderes i det helhetlige beslutningsunderlaget slik at beslutningstakere kan ta stilling til ulike dilemmaer og viktige strategiske veivalg. Beslutningsunderlaget må også i tilstrekkelig grad belyse usikkerhetsdimensjonen.

Forkortelser

DFØ	Direktoratet for forvaltning og økonomistyring
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
FSJ	Forsvarssjefen
FST	Forsvarsstaben
GNF	Grunnleggende nasjonale funksjoner
IKT	Informasjons- og kommunikasjonsteknologi
LTP	Langtidsplanen for forsvarssektoren
RBV	Ressursbasert teori
SWOT	Strengths, weaknesses, opportunities, threats
TCE	Transaksjonskostnadsøkonomi
VRIO	Valuable, rare, imitable og organized

Referanser

Litteraturliste, inkludert lovforarbeider

Aven, T. (2022). *Sikkerhet – risikostyring i Store norske leksikon på snl.no.* Hentet 5.november 2022 fra .

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*(1), 99–120.

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

Barney, J., Wright, M. & Ketchen, D. J. (2001). The resource-based view of the firm: Ten years after 1991. *Journal of Management*, *27*(6), 625–641.

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

Cooper, C. G. (2021). Hybride trusler og cyberoperasjoner. I C. G. Cooper & E. Aasheim (Red.), Folkerettskonferansen 2021.

Cooper, C. G. (2022). Lovlige mål - personer - internasjonal humanitærrett i Store norske leksikon på snl.no. Hentet 8. november 2022 fra https://snl.no/lovlige_m%C3%A5l_-_personer_-_internasjonal_humanit%C3%A6rrett.

Cortellazzo, L., Bruni, E. & Zampieri, R. (2019). The Role of Leadership in a Digitalized World: A Review. *Frontiers in Psychology*, 10(1938).

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

Direktoratet for økonomistyring. (2014). *Veileder for gevinstrealisering – planlegging for å hente ut gevinster av offentlige prosjekter*. Direktoratet for forvaltning og økonomistyring. https://dfo.no/fagomrader/gevinstrealisering

Elstad, A. K. (2014). *Critical Success Factors When Implementing an Enterprise System – An Employee Perspective* (Publikasjonsnr. NO 2014/05 ISBN /978-82-405-0301-7) [Doctoral thesis, NO 2014/05 ISBN /978-82-405-03017. Norges Handelshøyskole (NHH)]. Bergen.

Elstad, A. K., Brattekås, K., Bruvoll, J. & Nystuen, K. O. (2018). *Hva er egentlig verdi-vurdering?* (FFI-rapport 18/01391). Forsvarets forskningsinstitutt.

Elstad, A. K. & Hafnor, H. (2017). *"Nytt vindu for læring" Fra ildsjeler til strategisk satsing i Forsvaret* (FFI-rapport 17/01537). Forsvarets forskningsinstitutt.

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

Endregard, M., Nystuen, K. O., Farsund, B. H. & Elstad, A. K. (under arbeid). *Forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT – en innledende studie*. Forsvarets forskningsinstitutt.

Ernst & Young. (2019). *EY Norwegian IT Outsourcing Survey 2019. Status and trends in the Norwegian IT outsourcing market*. https://www.cw.no/insourcing-outsourcing-undersokelser/bedrifter-vil-flytte-it-tjenester-hjem/2077777

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

Forsvaret. (u.å.). *Cyberforsvaret*. Hentet 25. oktober 2022 fra https://www.forsvaret.no/om-forsvaret/organisasjon/cyberforsvaret.

Forsvarets forskningsinstitutt. (u.å.). *IKT og cyberdomenet – IKT og cyberdomenet blir stadig viktigere*. Hentet 12. oktober 2022 fra https://www.ffi.no/forskning/tema/ikt-og-cyberdomenet.
Forsvarsdepartementet. (2019). *IKT-strategi for forsvarssektoren – Hoveddokument* (Godkjent av Forsvarsministeren 27. mars 2019.). www.regjeringen.no/
Forsvarsdepartementet. (2020). *Evne til forsvar – vilje til beredskap. Langtidsplan for forsvarssektoren* (Prop. 14 S (2020–2021)). www.regjeringen.no
Forsvarsdepartementet. (2021a). *Høringsnotat: Forslag til endringer i lov om verneplikt og tjeneste i Forsvaret m.m. (forsvarsloven)*. www.regjeringen.no
Forsvarsdepartementet. (2021b). *IKT-styringsmodell for forsvarssektoren. Versjon 0.85. Unntatt offentlighet*.
Forsvarsdepartementet. (2021c). *Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar* (Meld. St. 17 (2020–2021)). Forsvars-departementet.
Forsvarsdepartementet. (2021d). *Tildelingsbrev for Forsvaret 2022* (22.12.2021). https://www.regjeringen.no/contentassets/d88b9ee605634445a3165501cc0f8d12/tildelingsbrev-for-forsvaret-2022.pdf
Forsvarsdepartementet. (2022a). *Prop. 1 S (2022 –2023). Proposisjon til Stortinget (forslag til stortingsvedtak). Utgiftskapitler: 1700–1791. Inntektskapitler: 4700–4799. For budsjettåret 2023.*
Forsvarsdepartementet. (2022b). *Prop. 134 L (2021–2022). Endringer i forsvarsloven (utvidet adgang til å inngå kontrakt om tjenesteplikt mv.)*. www.regjeringen.no
Forsvarsmateriell. (2022). https://www.fma.no/anskaffelser/virksomhetsprogrammet-mast
Forsvarsmateriell. (u.å.). *Om oss – IKT-kapasiteter*. Hentet 25. oktober 2022 fra https://www.fma.no/om-oss/organisasjon-og-ledelse/ikt-kapasiteter
Forsvarssjefen. (2013). *Manual i krigens folkerett*. Forsvaret. https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/194213/manual_krigens_folkerett.pdf?sequence=1&isAllowed=y
Forsvarsstaben. (2019). Forsvarets fellesoperative doktrine (FFOD) 2019 (Ikrafttredelse 1.12.2019).
Forsvarsstaben. (2021). *Forsvarets IKT-strategi. Økt operativ effekt gjennom robust IKT i kontinuerlig utvikling – IKT for morgendagens forsvar*.
Ilie, V. & Turel, O. (2020). Manipulating user resistance to large-scale information systems through influence tactics. *Information & Management*, 57(3), 103178.
Jae-Nam, L., Huynh, M. Q., Ron Chi-Wai, K. & Shih-Ming, P. (2003). IT Outsourcing Evolution – Past, Present, and Future. *Communications of the ACM*, *46*(5), 84–89.
Jansson, M., Carlström, E., Karlsson, D. & Berlin, J. (2021). Drivers of outsourcing and backsourcing in the public sector—From idealism to pragmatism. *Financial Accountability & Management*, *37*(3), 262–278. https://doi.org/https://doi.org/10.1111/faam.12273
Johansen, S. R. (2019). «Nød kjenner ingen rett»? Totalforsvar, beredskapsrett og folkerett. I P. M. Norheim-Martinsen (Red.), *Det nye totalforsvaret* (s. 117–133). Gyldendal.
Justis- og beredskapsdepartementet. (2021). *Høring om endringer i sikkerhetsloven (eierskap mv.)*. https://www.regjeringen.no/no/dokumenter/horing-om-endringer-i-sikkerhetsloven-eierskap-mv/id2876352/
Lacity, M. C., Willcocks, L. P. & Feeny, D. F. (1996). The Value of Selective IT Sourcing. *Sloan Management Review*, *37*(3), 13–25.

Lahiri, S., Karna, A., Chittaranjan Kalubandi, S. & Edacherian, S. (2022). Performance implications of outsourcing: A meta-analysis. *Journal of Business Research*, *139*, 1303–1316. https://doi.org/https://doi.org/10.1016/j.jbusres.2021.10.061
Lai, L. (2011). Kompetansemobilisering og egenmotivasjon. *Magma*, *3*, 50–55.
Lai, L. (2013). *Strategisk kompetanseledelse* (3. utgave. utg.). Fagbokforlaget.
Lysne, O. (2020). *Risikostyring i digitale verdikjeder. Rapport fra en arbeidsgruppe ledet av professor Olav Lysne*. Direktoratet for samfunnssikkerhet og beredskap. https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf
Lystad, E. (2022, 4. april). Bedrifter vil flytte IT-tjenester hjem. *Computerworld*. https://www.cw.no/insourcing-outsourcing-undersokelser/bedrifter-vil-flytte-it-tjenester-hjem/2077777
March, J. (1994). *Primer on Decision Making: How Decisions Happen*. Simon and Schuster.
Paré, G., Guillemette, M. G. & Raymond, L. (2020). IT centrality, IT management model, and contribution of the IT function to organizational performance: A study in Canadian hospitals. *Information & Management*, *57*(3).
Pedersen, O. B. (2022). *Bør vi samarbeide? – en litteraturstudie om valg av sourcingstrategi* (FFI-rapport 22/01384, under arbeid). Forsvarets forskningsinstitutt.
Priem, R. L. & Butler, J. E. (2001). Is the resource-based 'view' a useful perspective for strategic management research? *Academy of Management Review*, *26*(1), 22–40.
Riksrevisjonen. (2022). *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner* (Ugradert versjon av Dokument 3:3 (2022−2023)). https://www.riksrevisjonen.no/globalassets/rapporter/NO-2022–2023/forsvarets-informasjonssystemer-ugradert-versjon.pdf
Sagdahl, M. S. (2019). *Verdi i Store norske leksikon*. Hentet 19.2.2022 fra https://snl.no/verdi
Senter for statlig økonomistyring. (2010). *Veileder for resultatmåling – mål– og resultatstyring i staten*. Direktoratet for forvaltning og økonomistyring https://dfo.no/publikasjoner/veileder-resultatmaling-mal-og-resultatstyring-i-staten
Store norske leksikon. (2019). *Informasjons- og kommunikasjonsteknologi i Store norske leksikon på snl.no.* https://snl.no/informasjons-_og_kommunikasjonsteknologi
Svendsen-utvalget. (2020). *Økt evne til å kombinere menneske og teknologi – Veier mot et høyteknologisk forsvar* (Svendsen-utvalget, 24. juni 2020). www.regjeringen.no
van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M. & de Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in Human Behavior*, *72*, 577–588.
Wernerfelt, B. (1984). A Resource-based View of the Firm. *Strategic Management Journal*, *5*(2), 171–180.
Whittle, R. (u.å.). *The Business Architecture, Value Streams and Value Chains*. BAInstitute.org. Hentet 29.3.2022 fra https://www.bainstitute.org/resources/articles/business-architecture-value-streams-and-value-chains.
Williamson, O. E. (1979). Transaction-cost economics: the governance of contractual relations. *The journal of Law and Economics*, *22*(2), 233–261.

Liste over lover, forskrifter og konvensjoner

Beredskapsloven. *Lov av 15. desember 1950 nr. 7 om særlige rådgjerder under krig, krigsfare og liknende forhold (beredskapsloven)*.
Forsvarsloven. *Lov av 12. august 2016 nr. 77 Lov om verneplikt og tjeneste i Forsvaret m.m. (forsvarsloven).*

Genève-konvensjonene. *Genève-konvensjonen om behandling av krigsfanger, med vedlegg (Konvensjon III) av 12. august 1949. Ratifisert 3. august 1951. Ikrafttredelsesdato: 3. februar 1952.*

Vernepliktsforskriften. *Forskrift av 16. juni 2017 nr. 779 om verneplikt og heimevernstjeneste (vernepliktsforskriften).*

Virksomhetsikkerhetsforskriften. *Forskrift 20. desember 2018 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften).*

Vedlegg

A VRIO-rammeverk

VRIO står for *Valuable*, *Rare*, *Imitable* og *Organized*, og er et rammeverk som kan benyttes for å analysere om en organisasjons ressurser kan være en kilde til konkurransefortrinn eller ikke. Rammeverket er basert på arbeidet til Barney (1991, 2002) og Barney et al. (2001). VRIO-rammeverket, gjennom en analyse av ressurskategorier, har som mål å avdekke om de ulike ressursene er verdifulle, sjeldne, ikke-imiterbare og om de er utnyttet av organisasjonen. For å avdekke om en ressurs kan skape et vedvarende konkurransefortrinn, eller i denne konteksten et operativt fortrinn er det ulike spørsmål en kan stille seg:

1. Er det lettere for organisasjonen å reagere på muligheter og trusler fra omgivelsene dersom en aktivitet utføres med interne ressurser enn dersom aktiviteten utføres med eksterne ressurser?

2. Blir IKT-en mer robust, og får den bedre sikkerhet og ytelse ved at aktiviteten utføres internt?

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

4. Er det slik at organisasjoner som ikke utfører aktiviteten internt i dag vanskelig vil kunne skaffe de nødvendige ressursene for å utføre den?

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

Spørsmål 1 og 2 forsøker å avdekke om en aktivitet er verdifull. Spørsmål 3 forsøker å avdekke om aktiviteten er sjelden. Spørsmål 4 forsøker å avdekke om aktiviteten er ikke-imiterbar og spørsmål 5 forsøker å avdekke om aktiviteten er utnyttet av organisasjonen.

Dersom ressursen eller kapabiliteten verken er verdifull eller sjelden (svarene på ett av spørsmålene (2-4 er nei) er et transaksjonsbasert leverandørforhold antakeligvis å foretrekke. Grunnen til dette er at ved slike ressurser eller kapabiliteter er det gjerne snakk om ulike former

for produkter og tjenester med lav kritikalitet, eksempelvis standardiserte produkter og tjenester med lite kundetilpasning (Pedersen, 2022).

Dersom svaret på spørsmålene 2–4 ovenfor er «ja», tyder det på at ressursen er verdifull eller sjelden og dermed kan gi et operativt fortrinn. I de tilfellene hvor det operative fortrinnet er midlertidig eller vedvarende vil det beste overordnede handlingsalternativet være intern utførelse og eventuelt styrke og utvikle evnen ytterligere gjennom investeringer.

Rammeverket er presentert i tabell A.1:

Er en ressurs eller kapabilitet …							
Verdifull	Sjelden	Ikke imiterbar	Utnyttet av organisasjonen	Konkurranse implikasjoner	Økonomisk ytelse		Fortrinn/ svakhet
Nei	-	-	Nei	Konkurranse ulempe	Under normal		Svakhet
Ja	Nei	-		Konkurranse ulikhet	Normal		Styrke
Ja	Ja	Nei		Midlertidig konkurransefortrinn	Over normal		Styrke og distinkt kompetanse
Ja	Ja	Ja	Ja	Vedvarende konkurransefortrinn	Over normal		Styrke og vedvarende distinkt kompetanse

Tabell A.1 VRIO-rammeverk.

Om FFI

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

FFIs formål

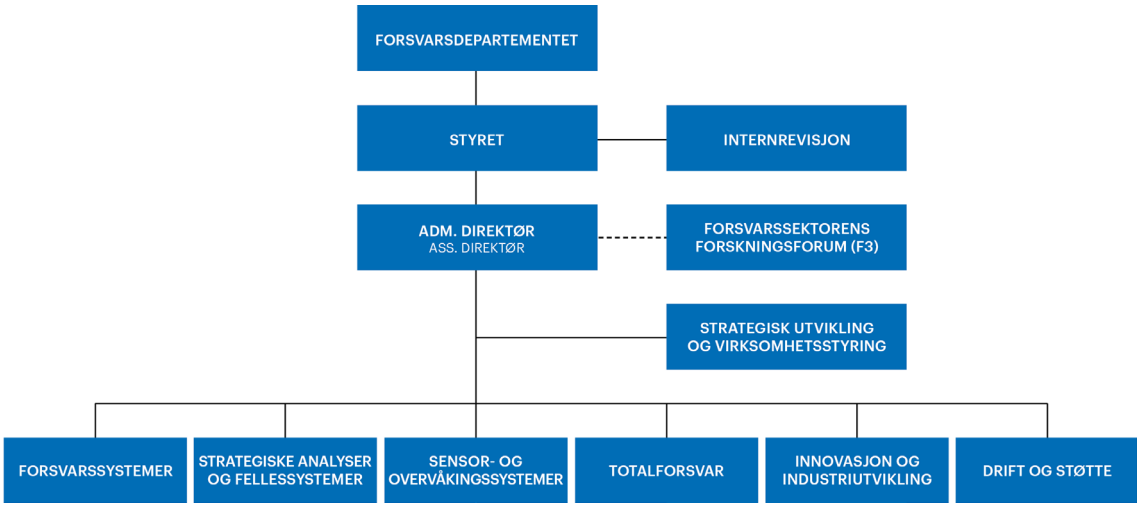
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som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