FFI Forsvarets forskningsinstitutt

23/00600

FFI-RAPPORT

# Forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT

## – en innledende studie

Monica Endregard
Kjell Olav Nystuen
Bodil Hvesser Farsund
Ann-Kristin Elstad

# Forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT – en innledende studie

Monica Endregard
Kjell Olav Nystuen
Bodil Hvesser Farsund
Ann-Kristin Elstad

Forsvarets forskningsinstitutt (FFI) 27. juni 2023

**Emneord**
IKT
Forsvarlig sikkerhetsnivå
Risiko
Sikkerhetsloven
Risikovurdering
Sikkerhetsstyring

**FFI-rapport**
23/00600

**Prosjektnummer**
1643

**Elektronisk ISBN**
978-82-464-3482-7

**Engelsk tittel**
Appropriate level of security for the Armed Forces' use of ICT – an introductory study

**Godkjennere**
Raymond Haakseth, *forskningsleder*
Jan Erik Voldhaug, *forskningssjef*

*Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur*.

# Sammendrag

Forsvarets IKT-strategi presiserer at informasjons- og kommunikasjonsteknologi (IKT) er en kritisk faktor for at Forsvaret skal kunne løse sine oppgaver i krig, krise og fred, og uunnværlig for at Forsvaret skal kunne gjennomføre sine operasjoner på en effektiv og sikker måte. IKT-sikkerhet er derfor avgjørende for å sikre at Forsvarets IKT-systemer er tilgjengelige, til å stole på og at sensitiv informasjon beskyttes mot uautorisert tilgang eller tap. Formålet med denne rapporten er å støtte Forsvaret og Forsvarsstaben innenfor styring av risiko og sikkerhet på IKT-området.

Utgangspunktet for rapporten er at det ikke er etablert tilnærminger for hvordan Forsvaret kan utføre funksjons- og risikobaserte vurderinger for bruk av IKT som grunnlag for kontinuerlig å opprettholde et forsvarlig sikkerhetsnivå, slik sikkerhetsloven krever. Funksjonsbegrepet er sentralt. Vi velger å benytte begrepet IKT-baserte funksjoner som et samlebegrep for både IKT-tjenester, informasjonssystemer og IKT-infrastruktur. En IKT-basert funksjon inkluderer menneskelige, teknologiske og organisatoriske ressurser.

Rapporten presenterer et forslag til et rammeverk for forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT. Rammeverket søker å etablere sammenheng mellom overordnede nasjonale sikkerhets-interesser og gjennomføring av militære operasjoner, til risiko og sikkerhet på teknisk nivå. Det har en klar top-down tilnærming, der verdien av IKT-baserte funksjoner, sikkerhet og risiko er knyttet til hva funksjonene brukes til og hvordan de bidrar til nasjonale sikkerhetsinteresser, i tråd med sikkerhetslovens systematikk. Det legges også til grunn at detaljert kunnskap om militære operasjoner og innsikt i systemer og teknologier er nødvendig, det vil si en bottom-up tilnærming.

Rammeverket har tre deler. Den første delen er et verdihierarki for nasjonal sikkerhet for forsvarssektoren. Nasjonale sikkerhetsinteresser, og grunnleggende nasjonale funksjoner med underfunksjoner, skal ligge til grunn for å vurdere risiko og oppnå et forsvarlig sikkerhetsnivå.

Bruken av IKT i Forsvaret må vurderes i en operativ kontekst. Det viktige er funksjonaliteten som IKT utgjør for Forsvaret i ulike situasjoner. Det vil si hvilke operative evner IKT-baserte funksjoner bidrar til, både direkte og indirekte. Vi har brukt et forenklet eksempel for å utvikle og illustrere tilnærmingen. Å innhente og systematisere informasjon om operativ kontekst utgjør andre trinn, informasjonsfremkalling, i rammeverket.

Siste del av rammeverket ser på hvordan det kan etableres et forsvarlig sikkerhetsnivå basert på en funksjons- og risikobasert vurdering for operativ bruk av IKT-baserte funksjoner for å oppnå militær effekt. Vi anbefaler at slike vurderinger utføres ved å kombinere metoder og fremgangsmåter, og at risiko- og sikkerhetsstyring bør være en kontinuerlig prosess. En system-teoretisk tilnærming til risiko og sikkerhet kan være nyttig, og FFI anbefaler å utforske dette i videre arbeid.

Før rammeverket kan anbefales tatt i bruk, er det behov for å teste og foredle rammeverket gjennom praktiske, relevante anvendelser.

# Summary

The Norwegian Armed Forces' ICT strategy specifies that Information and Communication Technology (ICT) is a critical factor for the Armed Forces to be able to solve their tasks in war, crisis and peace, and indispensable for the Armed Forces to be able to carry out their operations in an efficient and safe manner. ICT security is therefore crucial to ensure that the Norwegian Armed Forces' ICT-systems are available, can be trusted and that sensitive information is protected against unauthorized access or loss. The purpose of this report is to support the Norwegian Defence Staff and the Norwegian Armed Forces in general within the management of risk and security in the ICT area.

Our point of departure is that there are no established approaches for how the Norwegian Armed Forces can carry out functional and risk-based assessments for the use of ICT as a basis for continuously maintaining an appropriate level of security in accordance with the Security Act. We choose to use the term ICT-based functions as a collective term for both ICT services, information systems and ICT infrastructure. An ICT-based function includes human, technological and organizational resources.

We have developed a proposed framework to achive an appropriate level of security for the Armed Forces' use of ICT. The framework seeks to establish a connection between overall national security interests and the implementation of military operations, to risk and security at a technical level. It has a clear top-down approach, where the value of ICT-based functions, security and risk is linked to what these functions are used for, and how they contribute to national security interests, in line with the Security Act. Also, detailed knowledge of military operations and insight into systems and technologies is necessary, i.e. a bottom-up approach.

The framework has three parts. The first part is a national security value hierarchy for the defence sector. National security interests, and fundamental national functions with sub-functions, must form the basis for assessing risk and achieving an appropriate level of security.

The use of ICT in the Armed Forces must be assessed in an operational context. What is important is the functionality that ICT provides for the Armed Forces in various situations. That is, the direct and indirect contribution of ICT-based functions to operational capabilities. We have used a simplified example to develop and illustrate the approach. Obtaining and systematizing information about operational context constitutes the second step, information elicitation, in the framework.

The last part of the framework looks at how an appropriate security level can be established based on a functional and risk-based assessment for the operational use of ICT-based functions to achieve military effects. We recommend that such assessments are carried out by combining methods and approaches, as part of continuous risk and security management. A system-theoretic approach to risk and security can be useful, and we recommend exploring this in further work. Before the framework can be recommended for use, there is a need to test and refine the framework through practical, relevant applications.

# Innhold

# Forord

I 2021 etablerte Forsvarssjefen IKT-avdelingen i Forsvarsstaben (FST J6). FST J6 støtter Forsvarssjefen innen strategisk styring av Forsvarets informasjons- og kommunikasjonsteknologi (IKT)-virksomhet. Forsvarets forskningsinstitutt (FFI) støtter FST J6 med råd og kunnskaps-utvikling gjennom FFI-prosjekt 1643 «IKT for morgendagens forsvar – støtte til FST J6».

Rapportens problemstilling er meget omfattende og krevende og har krevd betydelig innsats. Problemstillingen er nær de utfordringer som adresseres i FFI-prosjekt 1613 «Risiko og sikkerhet for kritiske digitale systemer og infrastruktur». Rapporten har krevd innsats også fra FFI-prosjekt 1613, og er derfor en leveranse i både FFI-prosjekt 1643 og 1613.

Vi vil rette en stor takk til Wilhelm Damsleth (FST) og Åshild Grønstad Solheim (FFI) for innspill til og grundig gjennomlesing av rapporten.

Kjeller, 12. juni 2023
Monica Endregard
Kjell Olav Nystuen
Bodil Hvesser Farsund
Ann-Kristin Elstad

# 1 Innledning

> «Informasjons- og kommunikasjonsteknologi (IKT) er en kritisk faktor for at Forsvaret skal kunne løse sine oppgaver i krig, krise og fred. […] IKT er uunnværlig for at Forsvaret skal kunne gjennomføre sine operasjoner på en effektiv og sikker måte.»[1]

Forsvarets bruk av IKT kobler sammen hovedkvarterene og de ulike militære enhetene og gir mulighet for felles kommando og kontroll (K2) og synkroniserte militære operasjoner. Uten IKT-systemer og digitale tjenester som er tilgjengelige ved behov, er det utfordrende for Forsvaret å lede og gjennomføre militære operasjoner, utveksle informasjon, utvikle og dele situasjonsbilder basert på ulike sensordata, få til samhandling og ta koordinerte beslutninger. I tillegg er IKT en integrert del av våpenplattformer som fregatter, kampfly og sensorer, eksempelvis radarer. IKT er også helt nødvendig for en rekke støttefunksjoner for eksempelvis logistiske og administrative prosesser. IKT-systemene og -tjenestene må derfor både være sikre med hensyn til konfidensialitet og tilgjengelighet, og de må være til å stole på.

Forsvarssektoren står overfor en omfattende modernisering og digitalisering, der strategisk samarbeid og partnerskap med næringslivet blir et viktig virkemiddel for å kunne oppnå gode resultater. Sivile og militære IKT-systemer veves stadig tettere sammen, og IKT-systemer og deres verdikjeder blir mer komplekse. Forsvaret tar i bruk kommersielle teknologier og deler av Forsvarets IKT-infrastruktur er basert på avtaler med sivile tilbydere av elektronisk kommunikasjon (ekom). Disse tilbyderne er nå i gang med å bygge ut femte generasjons mobilnett (5G). Forsvaret bruker i liten grad skyteknologi i dag, men det er nå planer for bruk av både privat og offentlig sky. Forsvarsmateriell (FMA) har søkt en strategisk partner som skal være en integrert del av IKT-virksomheten i forsvarssektoren, selv om denne prosessen nå er satt på vent.[2] Målet er å oppnå mer effektiv informasjonsdeling, samhandling og gjennomgående tjenester for nasjonale styrker i operasjoner, samt med øvrige aktører i totalforsvaret og allierte nasjoner.

Sikkerhet blir stadig viktigere i lys av denne utviklingen. Anvendelsen av nye løsninger både for nettverk, applikasjoner og datalagring, og ikke minst innføring av kunstig intelligens og teknikker basert på dyp læring, gir utfordringer knyttet til sporbarhet og gjennomsiktighet.[3] Som nevnt ovenfor, blir IKT-systemene og deres tilhørende verdikjeder mer komplekse og med sterke avhengigheter.[4] Samtidig krever stadig mer sofistikerte cybertrusler nye, avanserte evner innen cybersikkerhet og cyberforsvar for å sikre IKT-ressurser som Forsvaret er avhengig av, oppdage

[1] Forsvaret (2021). *Forsvarets IKT-strategi.* Desember 2021, s. 4.
[2] Forsvarsmateriell (januar 2021). *Strategisk samarbeidspartner innen IKT-leveranser* (fma.no); Forsvarsmateriell (20. februar 2023). *MAST*. https://www.fma.no/anskaffelser/virksomhetsprogrammet-mast
[3] For flere detaljer knyttet til sporbarhet og gjennomsiktighet i Forsvarets beslutningsprosesser, se Elstad, A.-K., Lund, K., Kristiansen, S. & Bloebaum, T. H. (2022). *Informasjonsdeling i Forsvarets beslutningsprosesser – kritiske suksessfaktorer.* FFI-rapport 22/00146. Kjeller: Forsvarets forskningsinstitutt.
[4] Nasjonal sikkerhetsmyndighet (2023). *Sikkerhetsfaglig råd. Et motstandsdyktig Norge*, s. 8. Sikkerhetsfaglig råd - Et motstandsdyktig Norge - Nasjonal sikkerhetsmyndighet (nsm.no).

trusler og dempe uønskede konsekvenser av cyberangrep.[5] Samlet sett fører utviklingen til store utfordringer for hvordan Forsvaret skal kunne styre risiko og sikkerhet.

I 2018 etablerte Forsvaret en digitaliseringsstrategi med et overordnet mål om å sikre økt operativ evne.[6] Ett av prinsippene er at digitaliseringen skal være *sikkerhetsorientert* ved at krav til informasjonssikkerhet er retningsgivende i prioritering, utvikling og implementering av tiltak. Forsvarsdepartementet (FD) besluttet en IKT-strategi for forsvarssektoren 27. mars 2019.[7] To av de strategiske tiltaksområdene er å «forbedre styring av sikkerhet og risiko» og «etablere en styringsmodell for IKT» i forsvarssektoren.

Den 1. januar 2021 fikk Forsvarssjefen (FSJ) ansvar for strategisk styring av IKT i forsvarssektoren.[8] I 2021 opprettet han en egen IKT-avdeling (J6) i Forsvarsstaben (FST) med ansvar for å støtte ham i dette arbeidet. I henhold til IKT-styringsmodell for forsvarsektoren er *sikkerhet* et eget styringsområde.[9] Styringsområdet sikkerhet skal «sørge for at Forsvaret og forsvarssektoren opprettholder et forsvarlig IKT-sikkerhetsnivå for å ivareta Forsvarets oppgaver, samfunnsoppdrag og lovpålegg. Styringsmodellen for IKT-sikkerhet bygges opp som en tredelt risikostyringsmodell, med avgrensninger i oppgaver, ansvar og leveranser».[10]

I tillegg til styringsområdet sikkerhet skal styringsområdet *risiko* «sørge for at sektoren og etatene har en systematisk tilnærming til vurdering og håndtering av risiko på IKT-området. Etatene skal ha et dokumentert forhold til risikovillighet og akseptabel risiko, og løpende identifisere, analysere og evaluere risiko på IKT-området og iverksette nødvendige tiltak for å redusere risiko til et akseptabelt nivå.»[11]

Begrepet *forsvarlig sikkerhetsnivå* ble introdusert i sikkerhetsloven som trådte i kraft 1. januar 2019, og er et ansvar som påligger alle virksomheter som er underlagt sikkerhetsloven.[12] Som presisert i Forsvarets IKT-strategi, skal forsvarlig sikkerhetsnivå baseres på vurdering av risiko for Forsvarets operative evne og verdier.[13] Videre skal sikkerhetstiltak balansere risiko, effekt og kostnad.[14]

[5] Nasjonal sikkerhetsmyndighet (2023), s. 54–57.
[6] Forsvarsstaben (2018). *Digitaliseringsstrategi for Forsvaret*.
[7] Forsvarsdepartementet (2019). *IKT-strategi for forsvarssektoren*. Datert 27. mars 2019.
[8] FD har fra 1. januar 2021 gitt FSJ «Ansvar, myndighet og funksjon for å utøve og videreutvikle den strategiske IKT-styringen i sektoren […]» (jf. FDs tildelingsbrev for Forsvaret 2021, ref. 2020/50888-1/FD III 3/TOHAB, s. 21).
[9] Forsvarsstaben (2022). *IKT-styringsmodell for forsvarssektoren*. September 2022. Ugradert – kan deles eksternt med godkjenning fra informasjonseier. Skal ikke publiseres åpent.
[10] Forsvarsstaben (2022), s. 8.
[11] Ibid.
[12] Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven).
[13] Forsvaret (2021), s. 7.
[14] Ibid., s. 8.

## 1.1 Problemstilling, formål og FFIs bidrag

Formålet med denne rapporten er å støtte FST J6 innen styringsområdene sikkerhet og risiko samt støtte øvrige aktører i forsvarssektoren for eksempel Forsvarets sikkerhetsavdeling, Cyberforsvaret og FMA. Etter vår oppfatning er FST J6 i gang med å etablere et styringssystem for IKT-sikkerhet i forsvarssektoren på militær-strategisk nivå. Et avgjørende spørsmål er hvilke faktorer som er kritiske i et slikt styringssystem. Styringssystemet skal bidra til å utvikle et egnet beslutningsgrunnlag for FSJ innen IKT-sikkerhet for å sørge for at Forsvaret har et forsvarlig sikkerhetsnivå.

Sikkerhetsloven med forskrifter setter klare krav til virksomhetenes evne til sikkerhetsstyring.[15] Annet regelverk legger også føringer for strategisk sikkerhetsarbeid. Sikkerhetsloven med forskrifter legger til grunn at forsvarlig sikkerhetsnivå i en virksomhet skal fremkomme som følge av verdibaserte risikovurderinger, og at det er virksomheten selv som har ansvaret for å oppnå et forsvarlig sikkerhetsnivå, og for å kunne dokumentere dette. Dette er prinsipielt ulikt det tidligere sikkerhetsregimet som i stor grad bygget på en regelbasert tilnærming. Sikkerhetsregimet som ble innført i 2019, krever en omstilling innen både kunnskap og forvaltning. Forsvarssektoren må derfor utvikle en tilnærming til sikkerhet som oppfyller moderne sikkerhetsprinsipper.

I denne innledende studien presenterer FFI sentrale problemstillinger for styring av risiko og sikkerhet, og foreslår et rammeverk for verdi- og risikobaserte vurderinger for Forsvarets bruk av IKT som et nødvendig beslutningsgrunnlag for å etablere et forsvarlig sikkerhetsnivå. Rapporten vektlegger verdivurderinger. Dette er det flere grunner til. For det første er sikkerhetsloven tydelig på at det er verdibaserte risikovurderinger som skal legges til grunn for et forsvarlig sikkerhetsnivå. Verdivurdering er helt avgjørende for å kunne utføre en helhetlig risikovurdering. For det andre er dette en utfordrende del av en risikovurdering. En tredje grunn er at innholdet i en trussel- eller sårbarhetsvurdering ofte kan bli sensitivt om det skal gi mening. Vurdering av disse faktorene er på grunn av sensitivitet ikke like utførlig behandlet i denne rapporten. Dette fokuset gjenspeiles også i eksempelet som benyttes for å illustrere rammeverket.

## 1.2 Avgrensninger

I utviklingen av et rammeverk for verdi- og risikovurderinger er det hensiktsmessig med et eksempel på en militær operativ kontekst. Et forsvarlig sikkerhetsnivå skal sørge for at Forsvaret kan utføre sine operasjoner og beskytter sine verdier. Derfor har vi tatt utgangspunkt i den operative militære evnen *hurtig reaksjonsvarsel*.[16] Basert på denne evnen har vi laget et forenklet eksempel som brukes som et hjelpemiddel og verktøy i utviklingen av rammeverket og for å kommunisere hvordan rammeverket kan anvendes.

Eksempelet er valgt fordi det er inspirert av åpen informasjon publisert av Forsvaret om den militære evnen og oppgaver som inngår i hurtig reaksjonsvarsel. Videre illustrerer eksempelet en

[15] Sikkerhetsloven; Forskrift 20. desember 2018 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften).
[16] Forsvaret (2023a). *Dette er QRA – Quick Reaction Alert*. Dette er QRA – Quick Reaction Alert - Forsvaret.

viktig militær evne for ivaretakelse av nasjonal sikkerhet. Evnen forutsetter bruk av IKT, og er derfor relevant for problemstillingen. Eksempelet er kun ment å illustrere metodikk og type vurderinger som kan gjøres. Det presiseres at alle vurderinger knyttet til risiko, sårbarheter og sikkerhet for dette eksempelet er fiktive. Vi har ikke involvert noen fagmiljøer i Forsvaret, da formålet med denne rapporten ikke er å utføre vurderingene, men kun å skissere hvordan vurderingene kan gjøres og foreslå momenter som bør inngå.

Når reelle vurderinger av risiko og forsvarlig sikkerhetsnivå skal foretas for bruken av IKT innen ulike militære evner, kreves kunnskap etablert gjennom et flerfaglig samspill der mange fagmiljøer i Forsvaret må bidra. Behovet for, og bruken av, IKT i militære operasjoner må defineres av de operative miljøene. Forståelse for hvordan Forsvarets IKT er bygget opp og henger sammen, og sårbarhetsvurderinger for komplekse IKT-systemer, krever bidrag fra fagmiljøene som er ansvarlige for IKT-virksomheten. Trusselvurderinger må bygge på etterretning og innspill fra ansvarlige fagmiljøer.

Det presiseres at dette er en innledende studie. Metodikk, tilnærming og forslag til rammeverk må også utforskes på andre typer eksempler, og ikke minst testes i praksis på konkrete problemstillinger. Det tas derfor forbehold om at FFIs forslag til rammeverk vil kreve videreutvikling for å sikre at det er hensiktsmessig for Forsvaret.

## 1.3 Rapportens oppbygning

Kapittel 2 tar for seg sentrale begreper og definisjoner innen risiko, sikkerhet og IKT. Kapittel 3 beskriver sikkerhetsloven og de relevante kravene som skal overholdes, knyttet til vurdering og styring av risiko, for å oppnå et forsvarlig sikkerhetsnivå. Kapittel 4 presenterer kort relevante standarder og veiledninger for risikostyring og -vurdering. Kapittel 5 diskuterer kilder til usikkerhet og kompleksitet, to meget viktige faktorer for vurderinger av risiko knyttet til Forsvarets IKT-virksomhet. Rammeverket som foreslås er blant annet inspirert av systemteoretiske tilnærminger til risiko og sikkerhet presentert i kapittel 6. Kapittel 7 går gjennom forslaget til rammeverk steg for steg. Kapittel 8 gir en kort oppsummering av rapporten, mens kapittel 9 skisserer behov for videre arbeid.

# 2 Begreper og definisjoner

Dette kapittelet presenterer et utvalg av sentrale begreper og definisjoner som vi benytter i denne rapporten. Det er ikke nødvendigvis enighet om disse begrepene og definisjonene, men dette er slik vi velger å benytte begrepene for vårt formål.

## 2.1 Sikkerhet, risiko og relaterte begreper

*Sikkerhet* er et sentralt begrep i denne rapporten, og det er derfor et behov for å avklare hva det er vi legger i begrepet. Store norske leksikon har følgende definisjon:

> «Sikkerhet kan defineres som en tilstand; fravær av uønskede hendelser eller frihet fra fare og frykt. Denne tilstanden er imidlertid ikke statisk, men påvirkes av endringer i faktorer som trussel og farer, sårbarhet og verdi.»[17]

Engelsk språk og risikofaglig terminologi skiller mellom *safety* og *security* der skillet ligger i hvilke type hendelser man søker sikkerhet mot. Safety kan defineres som fravær av uakseptabel risiko knyttet til utilsiktede hendelser, mens security kan defineres som fravær av uakseptabel risiko knyttet til tilsiktede handlinger utført av intelligente aktører.[18] Det har vært foreslått norske oversettelser, men her hersker det uenighet[19], og vi velger derfor å benytte de engelske ordene.

Sikkerhet og risiko er antonymer, det vil si ord som har motsatt betydning:

> «Begrepet «sikker» defineres som det å være uten uakseptabel risiko. […] Sikkerhet brukes på samme måte, i betydningen uten uakseptabel risiko. […] god sikkerhet svarer til lav risiko, og motsatt.»[20]

Sikkerhetsloven har etablert begrepet *forsvarlig sikkerhetsnivå* om det nivået som er akseptabelt med hensyn til beskyttelse av skjermingsverdige verdier (se kapittel 3.3).

*Risiko* handler om hva som kan skje i fremtiden. I dagligtale brukes begrepet ofte om noe negativt som kan skje, noe uheldig som kan ramme oss dersom vi ikke gjør noe med det. Det finnes en rekke ulike definisjoner av risiko. Blant annet i finanssektoren brukes risiko både om noe positivt og negativt. Å ta risiko gir muligheter for å tjene penger, men også for å tape penger. Den Internasjonale standardiseringsorganisasjonen (International Organization for Standardization, ISO) sin definisjon av risiko tar høyde for dette:

[17] Store norske leksikon. *Sikkerhet*. sikkerhet – Store norske leksikon (snl.no) [sist besøkt 07.07.22].
[18] Disse definisjonen er i tråd med definisjonene i: Society for Risk Analysis (2018). *Society for Risk Analysis Glossary*. The Risk Analysis Glossary from the Society for Risk Analysis - Society for Risk Analysis (sra.org) [sist besøkt 07.07.22].
[19] Se for eksempel: Språkrådet. *Samfunnskritisk sikkerhet*. Samfunnskritisk sikkerhet (sprakradet.no) [sist besøkt 07.07.22].
[20] Store norske leksikon, *Sikkerhet – risikostyring*. sikkerhet – risikostyring – Store norske leksikon (snl.no) [sist besøkt 07.07.22].

«[Risiko er] virkningen av usikkerhet knyttet til mål.»[21]

En ekspertgruppe i Society for Risk Analysis har etablert et utvalg av definisjoner av risiko, inkludert følgende definisjon:

«Risiko er usikkerhet om, og alvor av følgen av en aktivitet, på noe som mennesker verdsetter.»[22] (egen oversettelse)

Vi kan se av definisjonen at den vektlegger usikkerhet som en dimensjon av risiko, på samme måte som definisjonen fra ISO. Ekspertgruppen presiserer i tillegg to andre dimensjoner i definisjonen, nemlig alvoret av følgen av en aktivitet og det at det omhandler noe mennesker verdsetter, altså noe av verdi for oss.

En tredje definisjon er fra en norsk standardserie utviklet for risiko og sikkerhet mot tilsiktede uønskede handlinger, det vil si for security-feltet. Standardiseringskomitéen utviklet den såkalte tre-faktormodellen eller risikotrekanten basert på følgende definisjon av risiko:

«[Risiko er] forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifikke trusselen.»[23]

En ny norsk standard for krav til risikovurderinger gir et felles rammeverk for risiko knyttet til både safety og security, inkludert for risikovurdering i henhold til sikkerhetslovens krav. Den gir følgende definisjon:

«Risiko [er] usikkerhet knyttet til om en uønsket hendelse vil inntreffe og hvilke konsekvenser den kan få.»[24]

De mange definisjonene av risiko tilsier at det neppe kan oppnås enighet om en felles universell definisjon. Imidlertid er det mulig å bli enig om viktige elementer som inngår i risiko og som vi søker mer kunnskap om i risikovurderinger. Elementer som inngår i risiko er verdier med tilknyttede sårbarheter som vi ønsker å beskytte mot farer og trusler. Videre er usikkerhet en sentral dimensjon. Vi ønsker å identifisere risikoreduserende tiltak for å oppnå et forsvarlig sikkerhetsnivå for verdiene, det vil si et akseptabelt nivå av risiko.

*Verdi* defineres som en «ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen».[25] Verdien kan være materiell eller immateriell. Eksempler er liv, helse, penger, infrastruktur, informasjon eller omdømme.

[21] Standard Norge (2009). *Risikostyring Terminologi.* SN-ISO Guide 73:2009.
[22] Society for Risk Analysis (2018). *Society for Risk Analysis Glossary*.
[23] Standard Norge (2012). *Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Terminologi*. NS 5830:2012.
[24] Standard Norge (2021). *Krav til risikovurderinger*. NS 5814:2021.
[25] Standard Norge (2012).

I følge Porter[26] er en verdikjede en organisasjons verdiskapningsprosesser, som består av primær- og støtteaktiviteter.[27] Aktivitetene som skaper verdi i en organisasjon kalles primæraktiviteter. For Forsvaret vil primæraktivitetene være knyttet til Forsvarets kjernevirksomhet, det vil si strategisk viktige aktiviteter, eller aktiviteter nært knyttet til disse, som vil få store konsekvenser ved mangelfull utføring. Støtteaktivitetene er nødvendige for at primæraktivitetene skal skape verdi. Støtteaktiviteter i Forsvaret omtales gjerne som tilretteleggende virksomhet (de øvrige aktivitetene).[28]

I kontekst av denne rapporten vil de digitale verdikjedene stå sentralt. 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 rapporten «Risikostyring i digitale verdikjeder»[29] fra en arbeidsgruppe nedsatt av Direktoratet for samfunnssikkerhet og beredskap, ledet av professor Olav Lysne:

> «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.»

Et illustrerende eksempel på en digital verdikjede er fremtidens Nødnett, hvor realiseringen skjer ved hjelp av kommersielle tilbydere. Disse tilbyderne er avhengig av andre, eksempelvis regionale nettleverandører, som tilbydernes 5G-basestasjoner kobles 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.[30]

NS 5814:2021 gir følgende definisjoner på andre begreper vi benytter i rapporten: [31]

- *Trussel* defineres som en «tilsiktet handling som kan føre til en uønsket hendelse».
- *Fare* defineres som «forhold som kan føre til en uønsket hendelse».
- *Konsekvens* er «tap av verdier som følge av en uønsket hendelse».

[26] Michael Porter er professor ved Harvard, og er kjent for sine teorier innenfor bl.a. økonomi og forretningsstrategi.
[27] Barney, J. (2002). *Gaining and sustaining competitive advantage*. Prentice Hall.
[28] Tekst hentet fra Elstad, A.-K., Endregard, M. & Mykkeltveit, A. (2022). *Sourcing for Forsvarets IKT-virksomhet – skisse til rammeverk*. FFI-rapport 22/02237. Kjeller: Forsvarets forskningsinstitutt.
[29] 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.
[30] Ibid.
[31] Standard Norge (2021).

- *Sårbarhet* defineres som «analyseobjektets manglende evne til å motstå uønskede hendelser eller varige påkjenninger, samt å opprettholde eller gjenoppta sin funksjon etterpå».

*Usikkerhet* er et viktig element i en risikobeskrivelse og inngår i flere av definisjonene av risiko. Det er flere kilder til usikkerhet i risikovurderinger. NS 5814:2021[32] og Njå et al. (2020) deler usikkerhetsaspekter i tre tidskategorier: fortid, nåtid og fremtid.[33] Usikkerhet i historisk informasjon (fortid) gjelder datamaterialet en analyse bygger på, inkludert ekspertvurderinger. Usikkerhet i analysetidspunktet (nåtiden) handler blant annet om hvorvidt relevant og nødvendig informasjon er tilgjengelig og i hvilken grad et analyseobjekt lar seg modellere. Usikkerhet om fremtiden er iboende og handler om at det alltid vil være usikkert hva som vil skje og hvilke konsekvenser som vil følge. Vi kommer tilbake til dette i kapittel 5.

*Sannsynlighet* er et sentralt begrep i analyser og vurderinger av risiko og kan defineres som «hvor trolig det er at en hendelse vil inntreffe»[34]. Sannsynlighet kan forstås på to måter: [35]

a) som den relative hyppigheten en hendelse opptrer med i en hypotetisk situasjon som gjentas et uendelig antall ganger (matematisk sannsynlighet eller frekvensbasert sannsynlighet).

b) som et mål for usikkerheten om fremtidige begivenheter og deres konsekvenser, sett gjennom øynene til den som vurderer, og basert på bakgrunnsinformasjon og kunnskap (subjektivt mål for usikkerhet basert på bakgrunnskunnskap, kunnskapsbasert sannsynlighet).

## 2.2 IKT og cyberdomenet

Informasjons- og kommunikasjonsteknologi (IKT) er en samlebetegnelse for teknologi for innhenting, overføring, bearbeiding, lagring og presentasjon av informasjon.[36]

I Forsvarets IKT-strategi defineres IKT-virksomheten som de personer og organisasjoner som produserer varer, tjenester eller utfører aktivitet innen utvikling, drift, vedlikehold og forvaltning av Forsvarets IKT: det være seg Forsvarets og forsvarssektorens egne aktører eller andre offentlige og private aktører. [37]

[32] Standard Norge (2021), s. 14–17.
[33] Njå, O., Sommer, M., Rake, E. L. & Braut, G. S. (2020). *Samfunnssikkerhet. Analyse, styring og evaluering*. Oslo: Universitetsforlaget, s. 228–230.
[34] Standard Norge (2021).
[35] Busmundrud, O., Maal, M., Kiran, J. H. & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. FFI-rapport 2015/00923. Kjeller: Forsvarets forskningsinstitutt, s. 17. Basert på en oversettelse av: Aven, T. (2010). On how to define, understand and describe risk. *Reliability Engineering and System Safety* 95, s. 623–631.
[36] Store norske leksikon. *Informasjons- og kommunikasjonsteknologi*. https://snl.no/informasjons-_og_kommunikasjonsteknologi#:~:text=Informasjons%2D%20og%20kommunikasjonsteknologi%2C%20samlebetegnelse%20for,lagring%20og%20presentasjon%20av%20informasjon. [sist besøkt 11.03.22]
[37] Forsvaret (2021). *Forsvarets IKT-strategi. Økt operativ effekt gjennom robust IKT i kontinuerlig utvikling – IKT for morgendagens forsvar*. Desember 2021.

Nasjonal sikkerhetsmyndighet (NSM) definerer et IKT-system som maskinvare, programvare og tilknyttet infrastruktur.[38]

NSM definerer et informasjonssystem som et «IKT-system, data og tjenestene det tilbyr, bruken av dette, samt menneskers interaksjon med IKT-systemet for å støtte opp under virksomhetsprosesser»[39]. NSMs definisjon av informasjonssystem er i overensstemmelse med følgende definisjon fra Forsvarsdepartementet (FD). I forarbeidene til sikkerhetsloven[40] stiller FD seg bak definisjonen av informasjonssystem som sikkerhetslovutvalget foreslo:

> «Med begrepet informasjonssystem menes systemer som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker. Informasjonssystem skal i sikkerhetslovens forstand forstås vidt. Begrepet omfatter både manuelle og digitale informasjonssystemer, og favner alt fra saksbehandlingssystemer, kontorstøttesystemer og rene kommunikasjonssystemer til kontroll- og styringssystemer.»[41]

*Infrastruktur* er et sentralt begrep i sikkerhetsloven, men uten at loven definerer hva som ligger i dette begrepet. Store norske leksikon har følgende definisjon som kan være nyttig for vårt formål:

> «Infrastruktur er en fellesbetegnelse på faste anlegg og systemer som er nødvendige for at en virksomhet eller et samfunn skal fungere.»[42]

Noen eksempler på infrastrukturer i samfunnet er kraftforsyning, elektroniske kommunikasjonsnett, jernbanenettet og vannforsyning. En egenskap som gjerne kjennetegner en infrastruktur er at den kan brukes av flere aktører for ulike formål, uten at den som leverer infrastrukturtjenesten nødvendigvis kjenner til hvilken verdi denne har for brukeren av tjenesten. Det er ikke et klart skille mellom hva som betegnes som henholdsvis informasjonssystem og infrastruktur.

Videre defineres gjerne begrepet IKT-tjeneste som en funksjon som leveres av programvare.[43] For vårt formål er dette det samme som en IKT-funksjon.

Funksjonsbegrepet er sentralt i sikkerhetsloven. Vi velger å benytte begrepet **IKT-baserte funksjoner** som et samlebegrep for både IKT-tjenester, informasjonssystemer og IKT-infrastruktur. En IKT-basert funksjon inkluderer menneskelige, teknologiske og organisatoriske ressurser.

[38] Nasjonal sikkerhetsmyndighet (2020). *NSMs Grunnprinsipper for IKT-sikkerhet.* Versjon 2.0. nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf [sist besøkt 05.12.22].
[39] Nasjonal sikkerhetsmyndighet (2020).
[40] Prop. 153 L (2016–2017). *Lov om nasjonal sikkerhet (sikkerhetsloven)*. Oslo: Forsvarsdepartementet, s. 99.
[41] NOU 2016: 19. *Samhandling for sikkerhet*, s. 262.
[42] Store norske leksikon. *Infrastruktur*. infrastruktur – Store norske leksikon (snl.no) [sist besøkt 05.12.22].
[43] Elstad, A.-K., Lund, K., Bloebaum, T. & Kristiansen, S. (2022). *Informasjonsdeling i Forsvarets beslutningsprosesser – kritiske suksessfaktorer*. FFI-rapport 22/00146. Kjeller: Forsvarets forskningsinstitutt, s. 43.

Cyber- er et prefiks som viser at det ordet prefikset benyttes sammen med (stammen av ordet) er relatert til noe i cyberdomenet, eksempler på bruk er *cyberangrep* eller *cybertrussel*.[44] Vi velger også å gjengi deler av en artikkel i Store norske leksikon som forklarer hva cyberdomenet er:[45]

> «Cyberdomenet, cyberspace, er et menneskeskapt globalt og stadig skiftende domene karakterisert av kombinert bruk av elektroner og det elektromagnetiske spektrum for det formål å generere, lagre, endre, utveksle, dele, hente og eliminere informasjon og ødelegge fysiske ressurser.
>
> Cyberdomenet består av fysisk infrastruktur som kopler sammen, trådløst eller med kabel: sambandssystemer; datasystemer med tilhørende programvare: nettverk mellom datasystemer (intranett); nettverk av nettverk mellom datasystemer (internett); knutepunkter for brukertilgang; og data som er latent til stede i systemene. Cyberdomenet er verken regulert eller kontrollert av noen enkeltinstans.»

I NATOs AJP-3.20 «Allied Joint Doctrine for Cyberspace Operations» defineres cyberdomenet (*cyberspace*) som:

> «The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.»[46]

Forsvaret forholder seg til NATOs terminologi, blant annet av hensyn til interoperabilitet mellom Norge og allierte nasjoner. Forsvaret benytter begrepet Communications and Information Systems (CIS) definert som «et fellesbegrep som omfatter materiell, metoder, prosedyrer og personell som er organisert for å oppnå informasjonsutveksling og -håndtering».[47] I henhold til Cyberforsvaret (2023) er IKT-systemer den norske ekvivalenten til CIS.[48]

Forsvarets fellesoperative doktrine har i tillegg følgende definisjoner: [49]

> «CIS-støtte: Etablere, drifte, sikre og opprettholde kommunikasjons- og informasjonssystemer for å tilgjengeliggjøre CIS-tjenester til støtte for militære operasjoner.
>
> CIS-tjeneste: En CIS-tjeneste støtter brukernes funksjonelle behov for å løse sine oppgaver. Fokuset er ikke på systemene som tilrettelegger for tjenesten, men på den effekt understøttelsen gir for å dekke brukerens behov.»

[44] Forsvaret (2019), *Forsvarets fellesoperative doktrine*, s. 228.
[45] Store norske leksikon. *Cyberdomenet*. cyberdomenet – Store norske leksikon (snl.no) [sist besøkt 08.07.22].
[46] NATO Standardization Office (2020). *AJP-3.20. Allied Joint Doctrine for Cyberspace Operations*. Ed. A Version 1, january 2020, s. 4. AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A) (publishing.service.gov.uk)
[47] Forsvaret (2019), s. 228.
[48] Cyberforsvaret (2023). *Cyberforsvarets koordineringsordre CCO 23-001*. Jørstadmoen, 9. januar 2023, s. 10. (BEGRENSET)
[49] Ibid, s. 228.

Denne rapporten er i tråd med ovenstående definisjoner av cyber og CIS, men vi velger å benytte det norske begrepet IKT-systemer med samme betydning.

## 2.3 Sikkerhet og IKT

Begrepene digital sikkerhet, cybersikkerhet, informasjonssikkerhet og IKT-sikkerhet brukes mange ganger om hverandre, og er delvis, men etter vårt syn ikke helt, overlappende. Digital sikkerhet, cybersikkerhet og IKT-sikkerhet er synonymer, mens informasjonssikkerhet innebærer noe mer.

Digital sikkerhet og cybersikkerhet er synonymer og handler om sikkerhet mot hendelser som skjer i og via cyberdomenet, og vi velger å benytte Forsvarets definisjon:

> «Cybersikkerhet: En ønsket tilstand hvor kommunikasjons- og informasjonssystemer kan motstå påvirkninger i cyberdomenet som kan kompromittere konfidensialiteten, integriteten og tilgjengeligheten til digitale tjenester og den informasjon som lagres, behandles eller overføres av disse systemene.»[50]

Konfidensialitet, integritet og tilgjengelighet er viktige begreper innen informasjonssikkerhet og blir beskrevet under. Disse omtales som de tre informasjonssikkerhetsegenskapene, i tråd med sikkerhetslovens bestemmelser for beskyttelse av skjermingsverdig informasjon.[51]

Den internasjonale standardiseringsorganisasjonen (International Organization for Standardization, ISO) definerer informasjonssikkerhet som «ivaretakelse av konfidensialitet, integritet og tilgjengelighet av informasjon» i tråd med de tre informasjonssikkerhetsegenskapene.[52]

I henhold til sikkerhetsloven er «informasjonssikkerhet» et videre begrep enn cybersikkerhet og inkluderer beskyttelse av informasjon i IKT-systemer og informasjon utenfor IKT-systemer, slik som papirer i en safe. Det handler om å sikre informasjon, både fysisk og digitalt, mot alle former for trusler og farer slik at informasjonen

- ikke blir kjent for uvedkommende (konfidensialitet),
- ikke blir endret utilsiktet eller av uvedkommende (integritet), og
- er tilgjengelig ved behov (tilgjengelighet).

[50] Forsvaret (2019), s. 229.
[51] Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven).
[52] Standard Norge (2020). *Informasjonsteknologi. Sikringsteknikker. Ledelsessystemer for informasjonssikkerhet. Oversikt og terminologi*. NS-EN ISO/IEC 27000:2020.

Digitaliseringsdirektoratet (Digdir) inkluderer sikring av informasjonssystemene som benyttes, inkludert digitale tjenester, IKT-systemer og komponenter som inngår i IKT-systemer, i sin bruk av begrepet informasjonssikkerhet.[53]

Sikkerhetsloven med forskrifter skiller derimot mellom informasjonssikkerhet, informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet. Dette er gjort fordi loven regulerer beskyttelse av informasjon, informasjonssystemer og objekter og infrastrukturer på ulike måter. I og med at sikkerhetslovens bestemmelser er utgangspunkt for det rammeverket vi foreslår, velger vi å forholde oss til begrepsbruk i tråd med sikkerhetsloven.

Imidlertid er det viktig å merke seg at FD i forarbeidene til sikkerhetsloven poengterer at skillet mellom informasjonssystemsikkerhet og infrastruktursikkerhet er utydelig, og at et helhetlig sikkerhetsperspektiv er målsettingen:

> «Det blir derfor på den ene siden nødvendig å se alle typer av infrastrukturer i en helhet, der både objekter og de nettstrukturene som knytter det hele sammen, ses på i et helhetlig sikkerhetsperspektiv. Her vil det imidlertid være et utydelig skille mellom informasjonssystemsikkerhet og infrastruktursikkerhet. Innenfor informasjonssystemsikkerhet skal det legges til grunn at all sikkerhet i skjermingsverdige informasjonssystemer skal håndteres helhetlig med hensyn til tilgjengelighet, integritet og konfidensialitet.
>
> Samtidig må det imidlertid tas hensyn til at informasjonssystemsikkerhet må ses i nær sammenheng med objekt- og infrastruktursikkerhet for å oppnå tilstrekkelig helhetlig sikkerhet, og dermed et forsvarlig sikkerhetsnivå. Hvordan de fysiske og logiske nettverkene er knyttet sammen i infrastrukturene, vil ha stor betydning for tilgjengeligheten i de fleste moderne informasjonssystemer. Sammenhengen mellom informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet er i særlig grad viktig for å sikre tilgjengeligheten i moderne distribuerte informasjonssystemer. […] Det kan i flere tilfeller være aktuelt å peke ut skjermingsverdige informasjonssystemer som skjermingsverdig objekt eller infrastruktur.»[54]

## 2.4 Analyseobjekt og systemer

For å vurdere risiko må man definere et analyseobjekt, det vil si et «fysisk eller organisatorisk system, enhet, fenomen eller aktivitet som omfattes av risikovurderingen».[55]

I denne rapporten refererer vi til analyseobjektet som et system, og beskrivelsen av analyseobjektet som en systembeskrivelse. Begrepet system brukes i veldig mange sammenhenger og forstås på mange måter.

[53] Digitaliseringsdirektoratet. *Informasjonssikkerhet*. Informasjonssikkerhet - en forutsetning for å nå virksomhetens mål | Digdir [sist besøkt 11.07.22].
[54] Prop. 153 L (2016–2017), s. 102–103.
[55] Standard Norge (2021).

Store norske leksikon definerer «system» som:

> «et sett eller gruppe av gjenstander eller deler som hører sammen eller er ment å virke sammen etter en bestemt plan.»[56]

Et system kan inneholde programvare samt mekanisk, elektrisk og elektronisk maskinvare og blir ofte styrt av mennesker (operatører). Systemdelene er avhengig av hverandre. Egenskapene og oppførselen til de enkelte systemdelene er bestemt av samspillet med de andre delene.

Å vurdere et sosioteknisk system betyr at en ser på systemet som et hele, bestående av to delsystemer, ett sosialt og ett teknisk system og forholdet mellom disse. Med det sosiale systemet forstår vi mennesker i organisasjonen og den kontakt, det samarbeid, samspill og samvær som foregår mellom dem. Med det tekniske systemet forstår vi alle fysiske deler, programvare og hvordan disse er koblet og fungerer sammen. Forsvarets bruk av IKT bør etter vårt syn ses på som sosiotekniske systemer i tråd med perspektivet prosess, teknologi og organisasjon (PTO-perspektivet).

Vi inkluderer også en definisjon av et cyberfysisk system fordi denne type systemer antas å bli stadig viktigere fremover, også for Forsvarets bruk av IKT, gitt fremveksten av tingenes internett, automatisering og bruk av autonome systemer.[57]

> «Med et cyberfysisk system mener vi smarte systemer som inkluderer konstruerte samhandlende fysiske og digitale komponenter.»[58]

Ulike former for kompleksitet kjennetegner mange systemer i dagens samfunn. Dette fører til utfordringer i å vurdere og håndtere risiko. Society for Risk Analysis sier at et system er komplekst dersom det ikke er mulig å etablere en korrekt prediksjonsmodell for systemet basert på kunnskap om de spesifikke funksjonene og tilstandene for systemets enkeltkomponenter.[59] Vi kommer nærmere inn på kompleksitet og komplekse systemer i kapittel 5.

[56] Store norske leksikon. *System*. system – Store norske leksikon (snl.no) [sist besøkt 08.07.22].
[57] Farsund, B. H., Søndrol, T., Nystuen, K.O., Hornfelt, L., Sellevåg, S.R. & Pham, V. (2022). *Utviklingen av nye IoT-baserte infrastrukturer i samfunnet – utfordringer for nasjonal sikkerhet* (revidert rapport). FFI-rapport 22/00631. Kjeller: Forsvarets forskningsinstitutt.
[58] Basert på definisjonen i National Institute of Standards and Technology (2017). *Framework for Cyber-Physical Systems. Volume 1, Overview*. Cyber-Physical Systems Public Working Group, Smart Grid and Cyber-Physical Systems Program Office Engineering Laboratory. Framework for Cyber-Physical Systems: Volume 1, Overview (nist.gov).
[59] Society for Risk Analysis (2018).

# 3 Sikkerhetsloven

Til grunn for risiko- og sikkerhetsarbeidet ligger en rekke lover og forskrifter, der den viktigste for Forsvarets virksomhet er sikkerhetsloven med forskrifter. Et krav til et rammeverk for risikobaserte vurderinger for Forsvarets bruk av IKT og IKT-sikkerhetsstyring, er at det skal utvikles i tråd med sikkerhetsloven med forskrifter. I dette kapittelet gir vi en oppsummering av den systematikken og de sentrale bestemmelsene i sikkerhetsloven med forskrifter som danner grunnlaget for vårt forslag til rammeverk.

## 3.1 Sikkerhetslovens formål og virkeområde

Det rammeverket vi foreslår i denne rapporten tar utgangspunkt i sikkerhetslovens formål § 1-1:

> «[…] bidra til
> a) å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser
> b) å forebygge, avdekke og motvirke sikkerhetstruende virksomhet
> c) at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.»

Figur 3.1 viser formålet med og virkeområdet for sikkerhetsloven og sammenhengen mellom nasjonale sikkerhetsinteresser, grunnleggende nasjonale funksjoner og virksomheter underlagt sikkerhetsloven.

De nasjonale sikkerhetsinteressene er inndelt i fem kategorier, inkludert «forsvar, sikkerhet og beredskap» (sikkerhetsloven § 1-5). FD presiserer at med dette menes «Forsvaret, den øvrige forsvarssektoren, med understøttende funksjoner i en totalforsvarssammenheng»[60]. Dagens forsvar er direkte avhengig av innsatsfaktorer fra offentlige og private totalforsvarsaktører, blant annet innen ekom og kraftforsyning. Slike infrastrukturer og tjenester er derfor avgjørende innsatsfaktorer for militær operativ evne.

Nasjonale sikkerhetsinteresser omfatter også «samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet» (sikkerhetsloven § 1-5). FD presiserer at det er behov for å inkludere infrastruktur og tjenester som ikke direkte understøtter Forsvaret, men som er avgjørende for at det sivile samfunnet skal fungere, og viktig for samlet beredskap og forsvarsevne.[61] Dette innebærer en «begrenset utvidelse av lovens virkeområde» sammenlignet med den forrige sikkerhetsloven.[62]

Departementene skal i henhold til sikkerhetslovens § 1-2 identifisere grunnleggende nasjonale funksjoner (GNF-er) innenfor sine ansvarsområder. GNF-er er «tjenester, produksjon og andre

[60] Prop. 153 L (2016–2017), s. 34.
[61] Ibid, s. 35.
[62] Ibid, s. 37.

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.» (Sikkerhetsloven § 1-5). Disse GNF-ene er styrende for å identifisere funksjoner i alle offentlige og private virksomheter som er underlagt sikkerhetsloven. En oversikt over alle departementenes utpekte GNF-er var til og med 2021 beskrevet i Justis- og beredskapsdepartementets (JD) budsjettproposisjon[63]. Hvert departement lister sine GNF-er i sin siste budsjettproposisjon. NSM har en oversikt over alle innmeldte GNF-er på sine hjemmesider, og oversikten oppdateres ved endringer.[64]


*Figur 3.1 Formålet og virkeområdet for sikkerhetsloven samt sammenhengen mellom nasjonale sikkerhetsinteresser, grunnleggende nasjonale funksjoner og virksomheter underlagt sikkerhetsloven.*[65]

FD har etablert følgende fem GNF-er: [66]

**GNF 1: Situasjonsforståelse.** Evnen til etterretning, situasjonsforståelse og rettidig varsling.

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

[63] Prop. 1 S (2021–2022). *For budsjettåret 2022*. Oslo: Justis- og beredskapsdepartementet, s. 130–132.
[64] Nasjonal sikkerhetsmyndighet (30.9.2022). *Oversikt over innmeldte grunnleggende nasjonale funksjoner.* Oversikt over innmeldte grunnleggende nasjonale funksjoner - Nasjonal sikkerhetsmyndighet (nsm.no) [sist besøkt 08.12.22].
[65] Prop. 153 L (2016–2017), s. 34.
[66] Prop. 1 S (2022–2023). *For budsjettåret 2023*. Oslo: Forsvarsdepartementet, s. 122.

**GNF 3: Kommando og kontroll.** Evnen til kommando og kontroll over norske og allierte styrker.

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

**GNF 5: FDs 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.

FD har også etablert underfunksjoner til de fem GNF-ene for sektoren. Disse er beskrevet i et brev til etatene i forsvarssektoren datert 4. desember 2020 om risikostyring for IKT-sikkerhet i forsvarssektoren.[67] Vedlagt til dette brevet er en beskrivelse av GNF-ene i sektoren og en veiledning. Vi kommer tilbake til disse underfunksjonene i kapittel 8.

## 3.2 Virksomhetens ansvar for forebyggende sikkerhetsarbeid

For en virksomhet som er underlagt sikkerhetsloven, har virksomhetens leder ansvaret for forebyggende sikkerhetsarbeid og for å etablere sikkerhetsstyring som en del av virksomhetens styringssystem (jf. sikkerhetsloven § 4-1). Videre setter sikkerhetsloven krav til vurdering av risiko. Det innebærer at virksomheten skal ha evne og kapasitet til kontinuerlig å kunne foreta helhetlige risikobaserte vurderinger. Disse må baseres på konsistente verdivurderinger og vil være grunnlag for ulike former for sikkerhetstiltak (jf. sikkerhetsloven § 4-2). Loven sier at:

> «Virksomheten skal gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet.» (sikkerhetsloven § 4-3)

Videre er det krav til at virksomheten regelmessig gjennomfører øvelser som ledd i å vurdere effekten av iverksatte sikkerhetstiltak (jf. sikkerhetsloven § 4-3). Virksomheten må kontinuerlig dokumentere hvilke risiko- og verdivurderinger som legges til grunn for å iverksette og gjennomføre ulike former for sikkerhetstiltak (jf. sikkerhetsloven § 4-4).

## 3.3 Risikobaserte vurderinger for å oppnå forsvarlig sikkerhetsnivå

Sikkerhetsloven setter krav til sikkerhetsarbeidet gjennom blant annet å kreve at risikobaserte vurderinger legges til grunn for å avgjøre hva som er et forsvarlig sikkerhetsnivå i en virksomhets funksjoner. Loven setter også et klart krav til at risikovurderinger skal være verdibaserte, ut fra at sikkerhet – og ikke minst kostnaden ved – sikkerhet til enhver tid skal være tilpasset den verdien et system har for brukerne eller eierne av systemet. Krav til beskyttelse av sikkerhetsgradert

[67] Forsvarsdepartementet (2020). *Risikostyring IKT-sikkerhet i forsvarssektoren*. FDs ref. 2020/50797-1/FD II 4/EKHB. BEGRENSET.

informasjon kan hevdes å bryte noe med sikkerhetslovens systematikk siden disse kravene oppfattes som absolutte.

I forarbeidene til sikkerhetsloven påpeker FD at forsvarlig sikkerhetsnivå er:

> «en rettslig standard som kun skal trekke opp de ytre rammene virksomhetene må forholde seg til, og gi virksomhetene mulighet til å se det totale omfanget av sikkerhetstiltak i sammenheng, også tiltak som ikke følger av sikkerhetsloven».[68]

Virksomhetsikkerhetsforskriften beskriver generelle krav til hvordan virksomheter skal vurdere og håndtere risiko for å beskytte sine skjermingsverdige verdier (virksomhetsikkerhetsforskriften § 12 og § 13).[69] Skjermingsverdige verdier er definert som skjermingsverdig informasjon, skjermingsverdige informasjonssystemer, skjermingsverdig infrastruktur og skjermingsverdige objekter (§ 2).

Virksomhetsikkerhetsforskriftens § 12 «Vurdering av risiko» sier:

> «Når en virksomhet vurderer risiko, skal den ta hensyn til
>
> a) hvilken betydning virksomhetens skjermingsverdige verdier har for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser
> b) hvilken sikkerhetstruende virksomhet de skjermingsverdige verdiene kan bli utsatt for
> c) sannsynligheten for at sikkerhetstruende virksomhet kan inntreffe
> d) hvilke sårbarheter som er knyttet til de skjermingsverdige verdiene
> e) konsekvensen av sikkerhetstruende virksomhet for de skjermingsverdige verdiene
> f) i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal.
>
> Behovet for å gjennomføre en ny helhetlig vurdering av risikoen skal vurderes årlig. Dersom det planlegges, gjennomføres eller inntreffer endringer som kan påvirke skjermingsverdige verdier i vesentlig grad, skal virksomheten vurdere hvilken risiko endringene medfører.»

Formålet med vårt forslag til rammeverk er at dette skal danne grunnlag for at Forsvaret skal kunne oppnå et forsvarlig sikkerhetsnivå for Forsvarets skjermingsverdige verdier innen IKT-området i tråd med sikkerhetslovens krav.

En moderne virksomhet med mennesker og andre fysiske og logiske produksjonsmidler, er i økende grad svært kompleks. Her må forsvarlig sikkerhetsnivå oppfattes som en dynamisk

[68] Prop. 153 L (2016–2017), s. 81.
[69] Forskrift 20. desember 2018 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften).

størrelse som raskt vil endres i takt med endringer i virksomhetens innhold og struktur, eksempelvis personell, IKT-systemer, tjenesteutsetting, og så videre.

Forsvarlig sikkerhetsnivå oppnås når risikoen med tilhørende usikkerheter kan vurderes å være på et akseptabelt nivå. Å identifisere hva et forsvarlig sikkerhetsnivå er, kan man kun oppnå ved å vurdere risiko med tilhørende usikkerheter. Risiko vil være tett koblet til virksomhetens verdiskapning, og igjen tett knyttet opp mot sårbarheter og trusler i virksomheten. Dette innebærer at man må kunne vurdere hva risikoen er (skjermingsverdige verdier, sårbarheter, trusler) og hvilke usikkerhetsfaktorer som er knyttet til vurderingen.

# 4 Standarder og veiledere

I tillegg til at rammeverket skal være i tråd med sikkerhetsloven, med krav beskrevet i kapittel 3, bør det også være i tråd med prinsipper og begrepsbruk i sentrale standarder innen risikostyring og sikkerhetsstyring. I tillegg støtter vi oss på ulike veiledere utarbeidet av offentlige myndigheter i utviklingen av rammeverket.

Å styre risiko og sikkerhet knyttet til anvendelsen av IKT-baserte funksjoner dreier seg om å forene prinsipper fra to standarder. Risikostyring er beskrevet i standarden ISO 31000. ISO har etablert en egen serie av standarder med anbefalinger for å styre sikkerhet innen informasjonsteknologi – ISO 27000-serien. Standardene er ganske generelle. Det betyr at det kan være krevende å operasjonalisere dem til bruk for konkrete virksomheter eller områder. Derfor har blant annet Nasjonal sikkerhetsmyndighet (NSM) og Digitaliseringsdirektoratet laget veiledere for virksomheter i Norge.

Rammeverket vi foreslår er i tråd med anerkjente standarder. I dette kapittelet oppsummerer vi kort relevant innhold fra standarder og veiledere som vi har benyttet terminologi og systematikk fra i utviklingen av rammeverket.

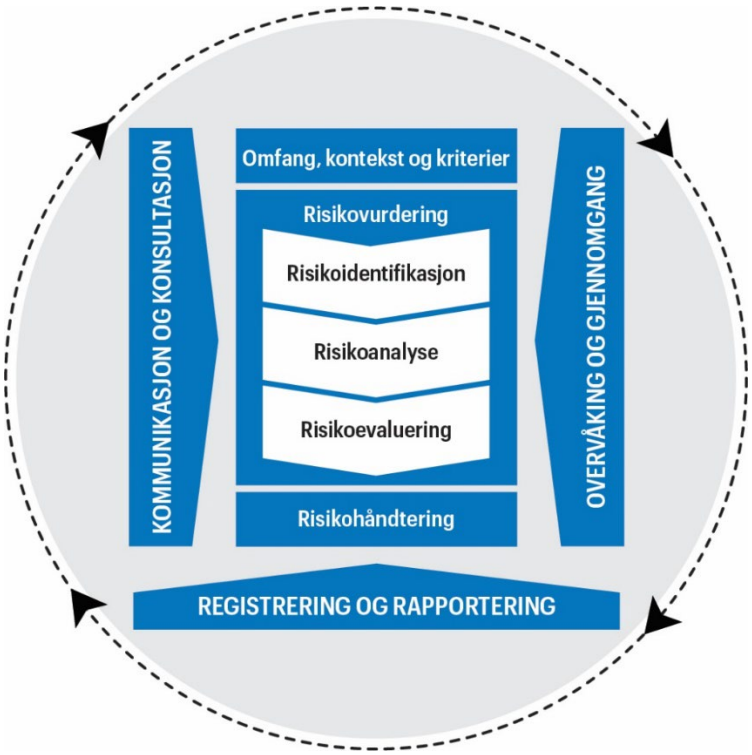
## 4.1 Risikostyring

Risikostyring defineres som «koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko».[70] ISO 31000 gir generelle retningslinjer for risikostyring.[71] Teksten i dette delkapittelet er basert på denne standarden.

Formålet med risikostyring er å skape og beskytte verdier og støtte oppnåelse av virksomhetens mål. Standarden fremhever virksomhetsleders ansvar for risikostyring og videre at slik styring skal være en integrert del av alle organisatoriske aktiviteter. ISO 31000 presenterer og anbefaler prinsipper, rammeverk og prosess for risikostyring. I henhold til standarden må risikostyring være en dynamisk prosess der vurderinger og tiltak oppdateres i tråd med endringer som påvirker risiko, og forbedres kontinuerlig gjennom læring og erfaring.

Figur 4.1 illustrerer elementene som inngår i helhetlig risikostyring, og som bør være en integrert del av ledelse, beslutningstaking og virksomhetsstyring, og integrert i organisasjonens struktur, drift og prosesser. Standarden presiserer at prosessen for risikostyring kan benyttes på ulike nivåer i virksomheten, det vil si på strategisk, operasjonelt, program- eller prosjektnivå. Hvert av elementene i figuren identifiserer områder der det er nødvendig å benytte og/eller utvikle hensiktsmessige metoder og fremgangsmåter.

[70] Standard Norge (2009); Standard Norge (2018a); Standard Norge (2020).
[71] Standard Norge (2018a).




*Figur 4.1 Risikostyringsprosessen i henhold til ISO 31000.*
*(Prosess fra NS-ISO 31000:2018 er gjengitt av Forsvarets forskningsinstitutt (FFI) med tillatelse fra Standard Online AS 3.12.2021. Standard Online er ikke ansvarlig for eventuelle feil i gjengitt materiale. Se www.standard.no.)*

Prosessen for risikostyring inkluderer følgende deler:

i. *Kommunikasjon og konsultasjon* har som formål å bringe inn ulik ekspertise for hvert element i prosessen, sikre at forskjellige synspunkter tas hensyn til ved fastsettelse av risikokriterier og risikoevaluering, gi tilstrekkelig informasjon, bygge forståelse og eierskap.

ii. *Omfang, kontekst og kriterier* har som mål å fastsette omfanget av prosessen, identifisere den interne og eksterne konteksten, målsettingene, fastsette risikokriterier, beskrive systemet og dets nøkkelressurser, strukturere prosessen, engasjere de nødvendige aktørene og definere nøkkelavgrensninger.

iii. *Risikovurdering* består av de tre trinnene (i) risikoidentifikasjon, (ii) risikoanalyse og (iii) risikoevaluering. Formålet er å gi det overordnede risikobildet og anbefalinger til beslutningstakere om hvordan risikoene bør håndteres.

iv. *Risikohåndtering* innebærer å formulere, velge og iverksette alternativer for å ta hensyn til risiko. Risiko kan ikke elimineres, men må behandles basert på ulike strategier – unngå, redusere, overføre eller akseptere risikoer. Trinnet består også i å vurdere virkningen av risikohåndteringen. Deretter besluttes om restrisikoen er akseptabel, og hvis den ikke er akseptabel, må ytterligere tiltak iverksettes.

v. *Overvåkning og gjennomgåelse* skal sikre og forbedre prosessen og bør skje på alle stadier av prosessen.

vi. *Registrering og rapportering* innebærer å dokumentere og rapportere prosessen og resultatene, der målet er å kommunisere med hele organisasjonen, gi informasjon til beslutningstakere, forbedre aktiviteter og fremme samhandling med ulike interessenter.

Risikostyringsprosessen er syklisk og bør gjentas med jevne mellomrom, eller tas opp igjen på grunn av viktige endringer som berører systemet, dets verdier, sårbarheter eller trusler. Risikostyringsprosessen i henhold til ISO 31000 er godt etablert og mye brukt. Sikkerhetslovens bestemmelser og ISO 31000 er kompatible, og standarden kan derfor brukes som utgangspunkt for vårt rammeverk for å vurdere risiko og sikkerhet for Forsvarets bruk av IKT i tråd med sikkerhetsloven.

Samlet sett omfatter risikostyring det å balansere innspill fra risikovurderinger med informasjon fra andre vurderinger slik som personvern, menneskerettigheter, kost-nytte, krigens folkerett, før det tas beslutninger om hvordan risikoer bør håndteres. Et forsvarlig sikkerhetsnivå skal oppnås, i tråd med sikkerhetslovens norm, men det kan være flere alternative mulige måter å gjøre det på.

IKT-baserte funksjoner, og særlig i form av IKT-infrastrukturer, blir stadig mer komplekse blant annet fordi de innehar mange eksterne og interne avhengigheter. Sammen med stadig mer sammensatte verdikjeder gir dette i mange tilfeller svært høy kompleksitet. For å kunne vurdere risiko og sikkerhet i dagens digitaliserte og komplekse virkelighet, er det derfor nødvendig med en strukturert og helhetlig tilnærming til risikostyring. Gitt de krevende omgivelsene og formålet med vårt rammeverk, er det etter vår vurdering viktig med en balansert og pragmatisk tilnærming til risiko og sikkerhet der enkeltdetaljene ikke tar overhånd.

ISO har etablert en egen standardserie for informasjonsteknologi, som Standard Norge også har gitt ut. Denne såkalte 27000-serien består av en rekke standarder som til sammen gir anbefalinger for et styringssystem for informasjonssikkerhet. Det er et prinsipp hos standardiseringsbyråene at standarder ikke skal være i motstrid. Terminologien[72] og risikostyringsprosessen for informasjonssikkerhet[73] er derfor i tråd med de øvrige standarder fra ISO.

[72] Standard Norge (2020).
[73] Standard Norge (2018b). *Informasjonsteknologi. Sikringsteknikker: Risikostyring for informasjonssikkerhet*. NS-ISO/IEC 27005:2018.

NSM har utgitt en veileder i sikkerhetsstyring som skal være til hjelp for virksomheter som skal etablere sikkerhetsstyring for forebyggende sikkerhet i samsvar med sikkerhetsloven. «Sikkerhetsstyring» defineres av NSM som «systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier.»[74]

Det amerikanske National Institute for Standards and Technology (NIST) utgir også en rekke standarder, rammeverk og veiledninger som kan være nyttige, herunder for eksempel NIST Cybersecurity Framework.[75]

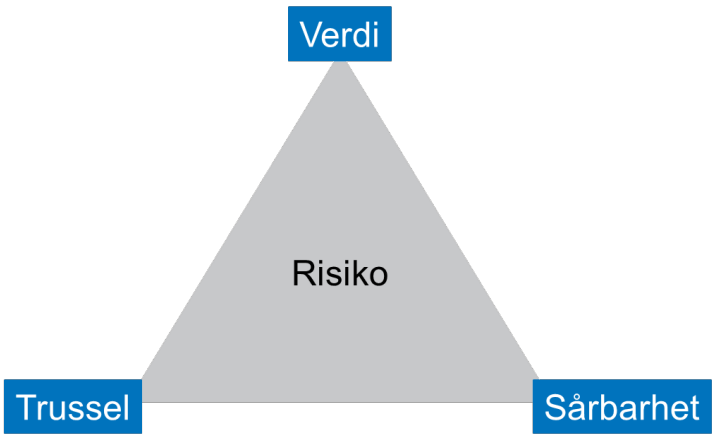
## 4.2 Risikovurdering

Det finnes en rekke ulike tilnærminger til risikovurderinger beskrevet i ulike standarder, veiledere, lærebøker og vitenskapelig litteratur. Vi begrenser oss her til to norske standarder.

Standardserien Norsk Standard (NS) 583X er etablert spesielt for å styre og vurdere risiko knyttet til tilsiktede uønskede handlinger, det vil si innenfor *security*. I NS583X dreier risiko seg, og dermed også risikostyring, om de tre faktorene verdi, trussel og sårbarhet. Som nevnt tidligere, definerer NS5830:2012 risiko som «forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifikke trusselen.». NS5832:2014 anbefaler en tilnærming til risikovurdering basert på denne definisjonen.[76] Alle tre faktorer er nødvendige i deler av risikovurderingen. Dette er illustrert i Figur 4.2, og prosessen som anbefales er illustrert i Figur 4.3. Mens faktoren verdi i stor grad må knyttes til bruken og brukeren av et system, vil sårbarhet i stor grad være knyttet til systemets eller infrastrukturenes egenskaper, både indre og eksterne. Sårbarhet vil også være knyttet til hvordan brukeren anvender systemet. Trusselen vil ofte i realiseres gjennom å utnytte sårbarheter for å angripe verdiene av systemet eller infrastrukturene.

Det er viktig å merke seg at infrastrukturbegrepet brukes om IKT-baserte funksjoner som benyttes av mange brukere. Dette er i motsetning til funksjonen til et enkelt system som ofte har en definert brukergruppe og dermed også enklere verdikjeder. Infrastruktur vil derimot ha ulik verdi for de ulike brukerne fordi hva de bruker infrastrukturen til, og dermed avhengigheten av infrastrukturen, kan variere. Verdikjedene knyttet til en infrastruktur blir dermed ofte svært sammensatt. Som påpekt i delkapittel 2.3, kan en infrastruktur bestå av ulike systemer, og skillet mellom systemer og infrastrukturer blir utydelig.

[74] NSM (ingen dato). *Veileder i sikkerhetsstyring*. Versjon 1.
[75] NIST (ingen dato). *Cybersecurity*. Cybersecurity | NIST [sist besøkt 19.01.23].
[76] Standard Norge (2012); Standard Norge (2014). *Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse*. NS 5832:2014.




*Figur 4.2 Risikotrekanten illustrerer risiko som forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifikke trusselen i tråd med definisjonen av risiko i NS5830:2012 (Standard Norge, 2012).*


*Figur 4.3 Elementer som inngår i prosessen for sikringsrisikoanalyse i henhold til NS5832:2014 (basert på Standard Norge, 2014).*

Én måte å gjennomføre en sikringsrisikovurdering på i henhold til NS5832:2014 er beskrevet av Busmundrud *et al.* (2015)[77], og er vist skjematisk i Figur 4.4. Analysetrinnene består av verdivurdering, trusselvurdering og valg av scenarioer og deretter en sårbarhetsvurdering. Sluttresultatet er en samlet vurdering av sikringsrisikoen for hvert av de valgte scenarioene basert på resultatet fra de tre analysetrinnene.

[77] Busmundrud, O., Maal, M., Kiran, J. H. & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. FFI-rapport 2015/00923. Kjeller: Forsvarets forskningsinstitutt.

| Analysetrinn | Delresultat | Samleresultat | Sluttresultat |
|---|---|---|---|
| **Verdivurdering** | Systematisk vurdering og rangering av de verdier virksomheten eier eller forvalter | Verdi (V) | Sikringsrisiko som en sammenstilling av V, T og S |
| **Trusselvurdering** | Identifisering av trusselaktører, deres intensjon og kapasitet og andre faktorer.<br>Valg av scenarioer (trusler som kan true verdiene) | Trussel (T) | |
| **Sårbarhetsvurdering** | Vurdering av i hvilken grad eksisterende barrierer kan forhindre den uønskede handling | Sårbarhet (S) | |

*Figur 4.4 Eksempel på analysetrinnene i en sikringsrisikovurdering i tråd med NS5832:2014.*

Etter en samlet vurdering og sammenstilling av sikringsrisikoen for hvert av de valgte scenarioene vurderes ulike strategier for å håndtere sikringsrisiko. NS5832:2014 presiserer at usikkerhet skal beskrives. Deretter vurderes ulike tiltak og disse vurderingene presenteres til beslutningstaker som skal avgjøre valg av tiltak.

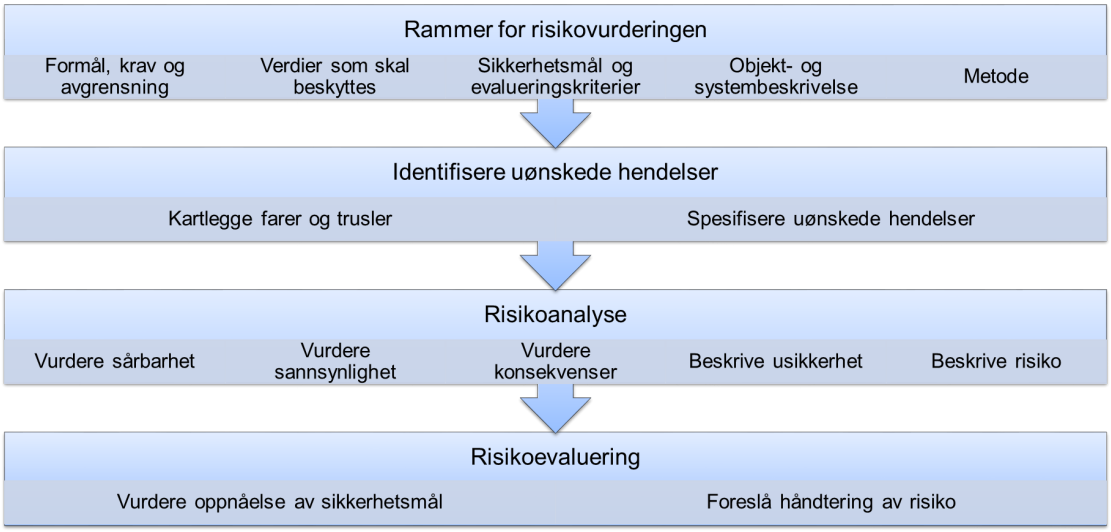
Standard Norge ga i 2021 ut en ny og oppdatert standard med krav til risikovurderinger: NS5814:2021.[78] Denne standarden tar høyde for, og har blitt oppdatert i tråd med, den utviklingen som har skjedd innen risikofaget siden forrige utgave ble utgitt i 2009. Spesielt er usikkerhets-dimensjonen i risikovurderinger vektlagt i denne nye versjonen. Videre inneholder standarden anbefalinger for å vurdere og kommunisere til beslutningstakere hvilken kunnskapsstyrke risiko-vurderingen bygger på. Kunnskapsstyrken som legges til grunn for risikovurderingen kan vurderes ut fra indikatorer slik som:[79]

- grad av forståelse av hendelsen, analyseobjektet og systemet.
- relevansen av kunnskap, erfaring og forskning på området.
- omfanget av datagrunnlag og involvering av fagkunnskap.

Usikkerhetsvurderinger og kommunikasjon av kunnskapsstyrke er viktige deler av en risiko-vurdering som må dokumenteres og kommuniseres til beslutningstakerne. Ulike kilder til usikker-het kommer vi mer inn på i neste kapittel.

[78] Standard Norge (2021).
[79] Standard Norge (2021), s. 9.

Figur 4.5 illustrerer skjematisk de fire trinnene som inngår i risikovurderingsprosessen i henhold til NS5814:2021.




*Figur 4.5 Analysetrinnene i risikovurderingsprosessen i henhold til NS 5814:2021 (basert på Standard Norge, 2021).*

NS5814:2021 er utviklet til bruk for både tilsiktede og utilsiktede hendelser. Standarden inneholder vedlegg som gir tre eksempler på hvordan standarden kan benyttes for ulike typer risikovurderinger. Ett av eksemplene er en risikovurdering i henhold til sikkerhetsloven, nemlig å vurdere risiko knyttet til terrorangrep mot et departement. De andre eksemplene er henholdsvis en risikovurdering for brann i tunnel og en risikovurdering av et vannforsyningsanlegg. Eksemplene er nyttige illustrasjoner av trinnene i en risikovurdering.

Som man ser av elementene som fremkommer i figurene 4.4 og 4.5, er det mange av de samme analysetrinnene som går igjen. Videre er beskrivelsene i standardene ganske generelle. I forslaget til rammeverk som presenteres i kapittel 8, har vi plukket ulike elementer fra de to standardene og satt disse sammen og tilpasset dette til problemstillingen i denne rapporten.

# 5 Usikkerhet og kompleksitet

Det er mange faktorer som bidrar til usikkerhet når vi skal vurdere risiko og sikkerhet for ulike systemer og infrastrukturer. Kompleksitet bidrar til usikkerhet. Både usikkerhet og kompleksitet kjennetegner de systemene vårt analytiske rammeverk skal utvikles for.

## 5.1 Usikkerhetsfaktorer

Det er viktig at usikkerhetsfaktorer er erkjent, og at disse blir vektlagt og kommunisert til beslutningstakerne som er ansvarlig for helhetlig sikkerhet. Usikkerhet henger også tett sammen med kompleksitet og begrenset rasjonalitet, som vi kommer tilbake til senere i kapittelet. Njå et al. (2020)[80] og NS5814:2021[81] deler usikkerhetsaspekter i tre tidskategorier; fortid, nåtid og fremtid, som tidligere nevnt.

Usikkerhet i historisk informasjon er knyttet til datamaterialet analysen bygger på, hvorvidt det finnes relevante og pålitelige data. Kunnskapsgrunnlaget består typisk av en kombinasjon av relevante data, gjerne historiske data, samt erfaringer. Det kan ligge eksperimenter og/eller modelldata til grunn for konsekvensvurderinger. Modeller kan være fraværende eller antas å gi dårlige resultater. Antakelsene som er gjort kan representere sterke forenklinger. Et ufullstendig eller skjevt datamateriale bidrar til usikkerhet.

Dersom analysen bygger på ekspertvurderinger, er det knyttet usikkerhet til i hvilken grad ekspertene har relevant bakgrunn og innsikt i historisk informasjon. Det å utarbeide et fullstendig kunnskapsgrunnlag som basis for rasjonelle beslutninger er en utopi, siden de som utarbeider dette grunnlaget møter ulike former for begrensinger innen oppmerksomhet, lagring og sammenstilling av informasjon. Mennesker har begrenset rasjonalitet, og utarbeidelsen av kunnskapsgrunnlaget vil være avhengig av hvilke deltakere som er med i utarbeidelsen.[82] Ulike deltakere vil gjøre forskjellige nyttevurderinger av det kunnskapsgrunnlaget som er tilgjengelig.[83] Det kan være større eller mindre grad av enighet, og ekspertvurderinger kan være subjektive og påvirkes av menneskelige faktorer, partiskhet og gruppedynamikk. Som påpekt i kapittel 4.2, er en vurdering av *kunnskapsstyrken* viktig å få frem slik at beslutningstakere er klar over analytikernes egen tiltro til analyseresultatet.

Usikkerhet i analysetidspunktet, nåtiden, handler blant annet om hvorvidt relevant og nødvendig informasjon er tilgjengelig og i hvilken grad analyseobjektet lar seg modellere. Analyseobjektets,

[80] Njå, O., Sommer, M., Rake, E. L. & Braut, G. S. (2020). *Samfunnssikkerhet. Analyse, styring og evaluering*. Oslo: Universitetsforlaget, s. 228–230.
[81] Standard Norge (2021), s. 14–17.
[82] Elstad, A.-K., Lund, K., Kristiansen, S. & Bloebaum, T. H. (2022). *Informasjonsdeling i Forsvarets beslutningsprosesser – Kritiske suksessfaktorer*. FFI-rapport 22/00146. Kjeller: Forsvarets forskningsinstitutt; Endregard, M. & Elstad, A.-K. (2021). «Beredskap i teori og praksis: Hvordan står det til?» I A. K. Larssen (Red.), *Beredskap og krisehåndtering - Utfordringer på sentralt, regionalt og lokalt nivå*. Oslo: Cappelen Damm AS, s. 23–45; March, J. (1994). *Primer on Decision Making: How Decisions Happen*. Simon and Schuster.
[83] March (1994).

eller systemets, egenskaper kan være kjennetegnet av ulike former for kompleksitet som gir ulike former for usikkerhet. Dette kommer vi tilbake til i neste delkapittel.

Usikkerhet knyttet til fortid og nåtid gjelder kunnskapsgrunnlaget for hele analysen, mens usikkerhet om fremtiden rett og slett skyldes at vi ikke kjenner fremtiden.[84] Det er usikkert hva som kan skje, og konsekvensene av hendelsene er usikre. Trusselbildet er dynamisk og kan endre seg raskt på grunn av ytre faktorer som virksomheten selv ikke kan kontrollere, slik som politisk klima, trusselaktørers intensjoner og evner, og nye sårbarheter som kan utnyttes. Som verktøy i risikovurderinger, etablerer vi gjerne et endelig sett av tenkbare hendelser, kalt scenarioer. Det er usikkerhet knyttet til hvor komplett og relevant et scenariosett er. Utvalget av scenarioer kan ha en tendens til å bli preget av nylige hendelser.

## 5.2 Kompleksitet som kilde til usikkerhet

Kompleksitet innebærer i henhold til definisjonen i kapittel 2.3 at det ikke er mulig å etablere en korrekt prediksjonsmodell for et system som helhet, basert på kunnskap om de spesifikke funksjonene og tilstandene for systemets enkeltkomponenter.

I henhold til Weinberg (1975) kan systemer deles inn i tre ulike kategorier – organisert linearitet, uorganisert kompleksitet og organisert kompleksitet – basert på graden av kompleksitet og graden av tilfeldighet.[85] Han laget en figur for å illustrere dette, og denne figuren har blitt gjengitt både av Leveson (2011)[86] og Njå et al. (2020)[87]. Vi gjengir også denne figuren for å illustrere ulike kategorier av systemer, se Figur 5.1.

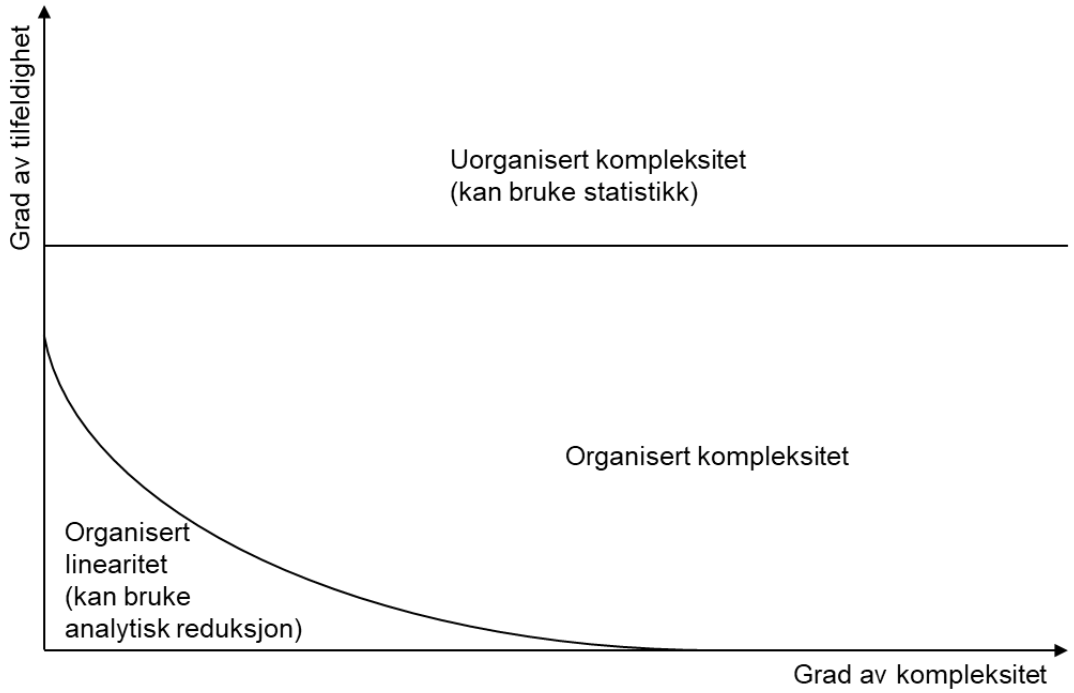
Området *organisert linearitet* inkluderer systemer med lav grad av tilfeldighet og kompleksitet. For slike systemer kan det etableres modeller som forklarer sammenhenger, og systemets helhet kan reduseres og beskrives ut fra subsystemer og enkeltkomponenter. Weinberg bruker eksempelet «maskiner» om slike systemer. Leveson (2011) påpeker at slike systemer ikke kjennetegnes av tilbakekoblingssløyfer og ikke-lineære interaksjoner, og at komponenter oppfører seg likt både når de opptrer alene og som del av systemet. Njå et al. (2020) trekker frem at bygningskonstruksjoner gjerne beskrives som enkle systemer. I en risikokontekst er dette en kategori der tradisjonell risikometodikk egner seg, det vil si der systemet lar seg modellere, og kausale årsaks- og konsekvenskjeder kan utledes. For systemer i kategorien organisert linearitet kan analytisk reduksjon benyttes.

For kategorien *uorganisert kompleksitet* er graden av tilfeldighet høy. Dette er systemer kjennetegnet av at det ikke er mulig å bryte ned systemet til enkeltkomponenter. Her kan statistiske modeller basert på observasjoner, etableres og benyttes. I en risikokontekst betyr det eksempelvis hendelser som oppstår med en viss frekvens. Det er mulig å etablere et datagrunnlag for å gjøre

[84] Endregard, M. & Elstad, A. K. (2021). «Beredskap i teori og praksis: Hvordan står det til?». I Larssen, A.-K. (red.) *Beredskap og krisehåndtering. Utfordringer på sentralt, regionalt og lokalt nivå*. Oslo: Cappelen Damm Akademisk, s. 23–45.
[85] Weinberg, G.M. (1975). *An Introduction to General Systems Thinking*. New York, NY: John Wiley & Sons, s. 26.
[86] Leveson, N. G. (2011). *Engineering a safer world.* The MIT Press, s. 62.
[87] Njå et al. (2020), s. 132.

meningsfulle beregninger av sannsynlighet og konsekvens på et aggregert nivå. Forekomst av trafikkulykker kan være et eksempel.

Kategorien *organisert kompleksitet* omfatter systemer som er for organiserte til at statistiske modeller kan benyttes, men likevel for komplekse for enkle modeller og analyser. Leveson påpeker at veldig mange menneskekonstruerte systemer, så vel biologiske som sosiale systemer faller inn i denne kategorien. Njå et al. gir eksempler som samfunnsviktige funksjoner og systemer som bygger på IKT-systemer, for eksempel kraftforsyning og vannforsyning. Systemteorien ble utviklet for dette området fordi klassiske analyseteknikker kom til kort for systemer med økende kompleksitet. Systemteorien fremhever at helheten i systemet alltid må være med. Vi kommer tilbake til systemteoretiske metoder i kapittel 6.




*Figur 5.1 Tre kategorier av systemer (basert på Weinberg (1975), Leveson (2011) og Njå (2020)).*

Definisjonen av et komplekst system er, som nevnt i kapittel 2.4, at det ikke er mulig å etablere en korrekt prediksjonsmodell for systemet basert på kunnskap om de spesifikke funksjonene og tilstandene for systemets enkeltkomponenter. Dette kjennetegner i økende grad den IKT-infrastrukturen og de IKT-systemene som Forsvarets operative evner er avhengig av. Disse systemene faller i økende grad inn i kategorien organisert kompleksitet fordi de er komplekse gjennom stadig lengre og mer komplekse verdikjeder. I tillegg er disse IKT-baserte funksjonene svært komplekse i seg selv. Kompleksitet er en form for sårbarhet det er vanskelig å beskytte seg mot. I risikobaserte vurderinger er det viktig å kunne kommunisere den usikkerhet som økt kompleksitet fører med seg. Beslutningstakerne må forstå den usikkerheten som følger av kompleksitet. Et eksempel kan være at ingeniørene vet at de ikke har full oversikt over deler av et IKT-system som

inngår i en sentral funksjon i et militært kommando- og kontrollsystem eller andre militære evner. De vurderinger som gjøres med hensyn til usikkerhet må være sporbare og etterprøvbare til enhver tid. Det er derfor viktig å forklare på hvilken måte systemene er komplekse for å kunne beskrive den usikkerheten som følger av ulike former for kompleksitet.

Det er flere aspekter som er viktig for å få en forståelse av kompleksiteten knyttet til IKT-systemer og -infrastrukturer, det vil si systemer som faller inn i kategorien organisert kompleksitet i Figur 5.1. Inspirert av arbeider av Leveson[88] og Perrow[89] har FFI tidligere strukturert ulike former for kompleksitet. De ulike formene for kompleksitet er dog ikke uavhengig av hverandre og kan delvis være overlappende, så noen egenskaper ved systemene og infrastrukturene vil passe inn i flere former for kompleksitet. FFI har i tidligere arbeider kommet frem til følgende former for kompleksitet som vi gjengir her:[90]

«**Samspillskompleksitet** beskriver hvordan avhengighetene er mellom og innad i informasjonssystemene og infrastrukturen. Her er det snakk om ulike avhengigheter:

- Interne avhengigheter kan betraktes som et sett med aktiviteter mellom elementer eller funksjoner i et system eller en infrastruktur. Et eksempel på dette kan være at en ruter er avhengig av en kontroller for å rute trafikk i et datasenter.

- Eksterne avhengigheter til andre (komplekse) systemer eller infrastrukturer, der en er avhengig av ressurser eller tjenester fra disse andre systemene eller infrastrukturene. Dette kan typisk være ekom, skytjenester, kraftforsyning og tidstjenester. En feil kan gjøre at mange ulike tjenester kan falle ut samtidig.

- Eksterne avhengigheter mellom systemer eller infrastrukturer fordi de bruker samme type maskinvare og/eller programvare eller trenger data fra hverandre. En sårbarhet som utnyttes her kan fort ramme mange ulike infrastrukturer. Bruk av eksempelvis skytjenester vil kunne føre til at samspillkompleksiteten øker. Det er mange interne avhengigheter mellom elementene i et datasenter. Datasentrene er også avhengig av kraftinfrastrukturer, og bruk av skytjenester fører som regel til en økt avhengighet av ekom. Deler av skyinfrastrukturen driftes og vedlikeholdes ofte fra utlandet. Det at ulike systemer og infrastrukturer bruker samme datasenter kan medføre at en tilsiktet eller utilsiktet hendelse som rammer skyinfrastrukturen kan gi en eller flere feil i andre systemer og/eller infrastrukturer. Disse kan gjerne være vanskelig å forutse, og i noen tilfeller vil konsekvensene kunne eskalere.

**Koplingskompleksitet** beskriver i hvilken grad sammenkoblingene eller tilbakekoblingene mellom elementer og funksjoner i IKT-systemer og organisatoriske elementer er tette eller

[88] Leveson, N. G. (2011).
[89] Perrow, C. (1999). *Normal Accidents: living with high-risk technologies*. New Jersey: Princeton University Press.
[90] Farsund, B. H., Søndrol, T., Nystuen, K. O., Hornfelt, L. Sellevåg, S. R. & Pham, V. (2022). *Utviklingen av nye IoT-baserte infratrukturer i samfunnet – utfordringer for nasjonal sikkerhet*. FFI-rapport 22/00631. Kjeller. Forsvarets forskningsinstitutt; Birkemo, G. A, Kristiansen P. & Farsund B. H. (2021). *Risiko ved strategisk samarbeid innen IKT – rammeverk og vurdering*. FFI-rapport 21/00527. Kjeller. Forsvarets forskningsinstitutt. (Unntatt offentlighet)

løse basert på tidskritikalitet. Ved tette koblinger vil en hendelse ett sted umiddelbart gi effekt et annet sted. Dette kan være fordi det er bestemt hvordan handlingen skal håndteres på forhånd, eller fordi det ikke er rom for fleksibilitet når handlingen skal håndteres. Tette koblinger tolererer ikke forsinkelser og tillater ikke slakk. Dette er i motsetning til løse koblinger som responderer saktere. Løse koblinger er dermed mer robuste med tanke på feilhåndtering, og vil fremstå som en slags buffer. Tette koblinger vil bidra til høy kompleksitet, mens løse koblinger vil bidra til det motsatte.

**Verdikompleksitet** beskriver hvordan et teknisk system eller et organisatorisk element bidrar oppover i verdikjeden. En verdi kan for eksempel være å medvirke til at et militært ledelseselement har et oppdatert og tilstrekkelig detaljert situasjonsbilde, eller at en militær styrke kan få kommunisert sin logistikkstatus. Hvis man har god oversikt over hvilke verdier infrastrukturen bidrar til, vil verdikompleksiteten være lav. Har man derimot liten oversikt over dette, fordi infrastrukturen blir brukt av mange aktører, både indirekte og direkte, vil verdikompleksiteten være høy. For strategisk partnerskap mellom forsvarssektoren og private aktører vil verdikompleksiteten øke. Som tidligere nevnt vil det ligge andre verdier i en skyinfrastruktur enn Forsvarets. Dette kan gjøre at Forsvaret kan bli rammet selv om ikke målet med et angrep var å ramme Forsvaret. Det samme gjelder for private aktører som kan bli utilsiktet offer for trusselaktørers handlinger. En (sky)tjeneste kan også fort bli brukt til mer enn først tenkt. Dette kan føre til at tjenester har større verdi enn man er klar over. En annen form for verdikompleksitet kan også oppstå fordi det forsvarssektoren ønsker å beskytte og regner som verdi, ikke samsvarer med det leverandøren regner som verdi. For eksempel vil private aktører gjerne ha økonomiske motiver når de vurderer sine verdier.

**Organisatorisk kompleksitet** sier noe om hvordan avhengighetene er mellom de involverte organisasjonene, organisasjonselementene og mellom de involverte organisasjonene og de tekniske systemene. Det kan være mange aktører involvert for å levere en tjeneste, for eksempel private virksomheter, offentlige etater og utenlandske virksomheter, og ofte en kombinasjon av disse. Det er i dag mange eksempler på at virksomheter splittes opp og/eller at deler av virksomheten tjenesteutsettes. Dette kan for eksempel utnyttes av en trusselaktør som ønsker å komme seg inn i en verdikjede. Organisatorisk kompleksitet kan blant annet gjøre det vanskelig å ha oversikt over hvor data havner, og kan gi uklare ansvarsforhold. Jo flere aktører som er involvert, jo større vil den organisatoriske kompleksiteten bli.

**Endringskompleksitet** (eller dynamisk kompleksitet) beskriver hvordan tekniske systemer, organisatoriske elementer og koblinger mellom disse endrer seg over tid. Disse endringene og dynamikken kan være knyttet til alt fra hvor ofte det skjer programvareoppdateringer, hvor ofte den fysiske infrastrukturen endres, hvor ofte det skjer endringer i hva infrastrukturen brukes til, til hvor ofte det skjer organisatoriske endringer, eksempelvis gjennom oppkjøp. Ved bruk av for eksempel kommersiell skyinfrastruktur som del av en IKT-basert funksjon vil forekomsten av slike endringer øke.»

Denne måten å bryte ned kompleksitet på i ulike faktorer og analysere disse, er én måte å vurdere og kommunisere ulike former for kompleksitet på til beslutningstakere i en risikovurdering. Dette

er en del av usikkerhetsvurderingen i vårt forslag til rammeverk for å vurdere risiko og forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT (se kapittel 8.4.4).

## 5.3 Begrenset rasjonalitet i beslutningsprosesser

Risiko- og sikkerhetsstyring innebærer beslutninger om hva som er et forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT. Basert på ulike forslag til handlingsalternativer skal det tas beslutninger om hvilke tiltak som må til for å oppnå et forsvarlig sikkerhetsnivå. I slike beslutningsprosesser er det viktig å være seg bevisst at slike prosesser ikke er fullt ut er rasjonelle, men kjennetegnet av det som i litteraturen kalles begrenset rasjonalitet.

Selve beslutningsprosessen består blant annet av innsamling, deling og behandling av informasjon, samt av handlinger og vurderinger som gjøres frem til valget av handlingsalternativ er tatt.[91] Rasjonalitet fremstår gjerne som et ideal i beslutningstakningsmodeller, der beslutningstakeren alltid tar den riktige beslutningen på bakgrunn av all tilgjengelig informasjon og avveininger for å oppnå maksimal nytte. I en slik ideell situasjon vil alltid beslutningstaker velge det beste handlingsalternativet, siden vedkommende har all informasjon tilgjengelig om alle mulige løsninger og konsekvenser av disse.

Konseptet om at beslutninger er rasjonelle har møtt kritikk siden mennesker har klare kognitive begrensninger knyttet til å håndtere objektivt den informasjonsmengden som kreves.[92] Rasjonalitet i beslutninger er en utopi, siden faktorer som tid, kognitive begrensninger og mangelfull informasjon vil ha innvirkning på beslutninger.[93] I tillegg kan opportunisme og uklare mål bidra til utfallet av beslutningsprosessen.[94] Videre vil også faktorer som følelser, usikkerhet, erfaring, situasjon og gruppedynamikk være faktorer som kan få innvirkning på utfallet av en beslutningsprosess.[95]

Samtidig møter beslutningstakerne begrensninger knyttet til oppmerksomhet, lagring av informasjon og sammenligning av informasjon. Ofte er det slik at en beslutningstaker har relevant informasjon, men feiler i å se at denne informasjonen er relevant. Et annet moment er at mennesker har begrenset kapasitet til å dele kompleks informasjon på tvers av kulturer og fagområder, noe som skyldes at de rammeverkene som benyttes for å forenkle verden, er forskjellig for ulike grupper.[96] Begrenset rasjonalitet er derfor kilde til usikkerhet i beslutningsprosesser, også innen risiko- og sikkerhetsstyring.

[91] Jacobsen, D. I. & Thorsvik, J. (2005). *Hvordan organisasjoner fungerer - Innføring i organisasjon og ledelse*. Fagbokforlaget Vigmostad og Bjørke.
[92] Fardal, H. & Elstad, A.-K. (2020). "Decision-making in crisis management of a serious digital incident: A garbage can approach." *Journal of Emergency Management 18*(6), s. 489–498.
[93] Simon, H. A. (1964). "On the concept of Organizational Goal." *Administrative Science Quarterly 9*(1), s. 1–22.
[94] Cyert, R. & March, J. G. (1992). *A behavioral theory of the firm*. Blackwell.
[95] Das, T. K. & Teng, B. S. (1999). "Cognitive biases and strategic decision processes: An integrative perspective." *Journal of Management Studies 36*(6), s. 757–778.
[96] March, J. (1994).

## 5.4 Ydmykhet som svar på begrenset kunnskap om komplekse teknologier

Sheila Jasanoff er en amerikansk professor som har vært sentral i å bygge opp teknologi- og vitenskapsstudier (*Science and Technology Studies*) til et eget fagfelt som forener naturfag med samfunnsfag og humaniora. Hun mener at vår evne til å utvikle ny teknologi har løpt fra vår evne til å kontrollere den og forutsi og dermed kunne hindre katastrofer. Eksempler på dette er ulykken med romfergen Challenger, Tsjernobyl-ulykken, kugalskap og menneskeskapte klimaendringer. Noe av det Jasanoff er mest kjent for er begrepet *technologies of humility*[97], som vi velger å oversette med «teknologier for ydmykhet». Med dette begrepet mener hun at vi må være ydmyke i forhold til stadig mer komplekse teknologier og hva de kan føre med seg, og at vi trenger «teknologier for ydmykhet» som et supplement til andre prediktive tilnærminger.

> 'Risk', on this account, is not a matter of simple probabilities, to be rationally calculated by experts and avoided in accordance with the cold arithmetic of cost-benefit analysis. Rather, it is part of the modern human condition, woven into the very fabric of progress. The problem we urgently face is how to live democratically and at peace with the knowledge that our societies are inevitably 'at risk'.[98]

Det motsatte av dette kaller hun *technologies of hubris* som vi kan oversette med teknologienes overmot, der men gjennom metoder som skal være objektive og etterprøvbare prøver å forutsi hva som kan skje og hva som virker. Eksempler på dette er risikovurderinger, kost-nytteanalyser og smittespredningsmodeller. Hun mener imidlertid at slike metoder skjuler den iboende usikkerheten som ofte kan være større enn det kan virke som. Hun mener videre at kritisk viktige spørsmål i risikostyring ikke kan bli besvart av teknologiske eksperter med tradisjonelle metoder. Slike spørsmål gjelder ikke bare om noe vil skje eller ikke, men hva som blir rammet og hvordan vi skal leve med denne usikkerheten.

Hun mener at vi nå prøver å kontrollere systemer med stadig større kompleksitet, med å øke kunnskapen. Selv om hun mener at det er bra å øke kunnskapen, mener hun samtidig at vi aldri vil få *tilstrekkelig* kunnskap. Kunnskapsnivået vårt vil bare gå mot dette optimale nivået asymptotisk.[99] Det vil si at vi aldri kommer til å nå dette nivået helt uansett hvor mye kunnskap vi tilegner oss.

«Ydmykheten handler om å anerkjenne at det er grenser for hva vi kan forutsi og kontrollere – og å være villige til å se på de verdimessige implikasjonene ved at vi ikke kjenner fremtiden.»[100] Vi må forholde oss til «den menneskelige forståelsens raggete utkanter – det ukjente, det usikre, det uklare og ukontrollerbare». For å møte dette peker hun på at det er viktig å inkludere flere ståsteder og erfaringer i beslutningsprosessene. I følge Jasanoff må det etableres «teknologier av

[97] Jasanoff, S. (2003). "Technologies of humility: Citizen participation in governing science". *Minerva 41*, s. 223–244.
[98] Jasanoff (2003).
[99] Jasanoff, S. (2007). "Technologies of humility". *Nature 450:*33.
[100] Time, J. K. (2022). *Advarer mot vitenskapens overmot, intervju med Sheila Jaasanoff*. Morgenbladet nr 14.

ydmykhet» for å synliggjøre muligheter for uforutsette konsekvenser, eksplisitt uttrykke normer og anerkjenne helt fra starten av at det er behov for mange ulike synsvinkler og kollektiv læring.[101]

## 5.5 Implikasjoner for utvikling av rammeverket

Både Forsvarets anvendelse av IKT-baserte funksjoner og sammensetningen av de IKT-baserte funksjonene i systemer og infrastrukturer er kompleks, og blir stadig mer kompleks. IKT-baserte funksjoner er integrert i så godt som all militær virksomhet. Dette gjør vurderinger av sikkerhet og risiko for Forsvarets bruk av IKT til krevende temaer, som det ikke uten videre finnes svar på i standarder.

Forsvaret blir stadig mer avhengig av sivile offentlige og private virksomheter innen totalforsvaret. I økende grad utvikles nært strategisk samarbeid med private aktører. Dette bidrar til å øke den samlede kompleksiteten knyttet til Forsvarets militære evner og virksomhet. På sikt gir dette økt usikkerhet og uforutsigbarhet for Forsvarets viktige oppgaver knyttet til nasjonal sikkerhet.

Analyseobjektet, det vil i vårt tilfelle si Forsvarets bruk av IKT, består av sosiotekniske systemer med mennesker/operatører, organisatoriske forhold og teknologiske systemer med integrerte fysiske og digitale komponenter. Videre er systemene gjerne i endring og avhengig av leveranser og funksjonalitet fra eksterne aktører eller systemer. Det er krevende å sikre en god nok system-forståelse og oversikt over interne og eksterne avhengigheter og koblinger.

Kompleksitet, og den usikkerheten som følger av kompleksitet, gjør at tradisjonelle risiko-vurderinger basert på sannsynlighet og konsekvens, eller grovanalyser basert på den såkalte trefaktormodellen, ikke lenger alene kan være grunnlaget for å styre risiko og sikkerhet for Forsvarets bruk av IKT. Det må i større grad tas hensyn til usikkerhet og kompleksitet. De nevnte tradisjonelle statiske risikovurderingene må komplementeres med utvikling av nye dynamiske tilnærmingsmåter for risiko- og sikkerhetsstyring. I utviklingen av rammeverket har vi latt oss inspirere av ulike tilnærminger for å håndtere usikkerhet og kompleksitet, herunder system-teoretiske tankesett basert på nyere risikofaglig forskning. Dette presenterer vi i neste kapittel.

[101] Jasanoff (2007).

# 6 Systemteoretisk tilnærming til risiko og sikkerhet

Forsvaret er en sammensatt virksomhet som har ansvar for å utføre en rekke ulike operasjoner og oppgaver. Å vurdere risiko og sikkerhet for Forsvarets bruk av IKT krever bruk av forskjellige tilnærminger og metodiske verktøy. I dette kapittelet legger vi mest vekt på systemteoretiske tilnærminger til risiko og sikkerhet utviklet for komplekse systemer. Slike tilnærminger kan derfor ha overføringsverdi til helhetlig risiko- og sikkerhetsstyring for Forsvarets bruk av IKT.

## 6.1 Behov for ulike metoder, verktøy og tilnærminger

For å vurdere risiko og sikkerhet på en helhetlig måte, er det hensiktsmessig å kombinere flere ulike metoder, verktøy og tilnærmingsmåter til en sammensatt fremgangsmåte. Valget av fremgangsmåte må tilpasses formålet, konteksten og kriteriene for vurderingen, inkludert også det tidsperspektivet og de ressursene som er tilgjengelige for oppdraget. Det finnes et betydelig antall metoder, verktøy og tilnærminger utviklet for ulike typer virksomheter og operasjoner, som det kan velges fra. Disse er beskrevet i standarder, veiledere, bøker og vitenskapelig litteratur.

ISO har etablert standarden NS-ISO 31010 der ulike metoder som kan inngå i en risikostyringsprosess, er kort beskrevet med referanser til utdypende litteratur.[102] Eksempler på metoder som er beskrevet, er analyse ved hjelp av sløyfediagram (*Bow-tie analysis*), årsaks-virkningsanalyse, scenarioanalyse, feiltre-analyse, konsekvens-sannsynlighet-matrise og mange flere. Metodenes styrker og svakheter er kort beskrevet. Videre er det gitt en oversikt der de ulike metodene er koblet til ulike deler av risikostyringsprosessen vist i Figur 4.1. Standarden har også vurdert anvendbarheten av hver av metodene i ulike deler av risikostyringsprosessen. NS-ISO 31010, og andre standarder og veiledere (se kapittel 4), kan være nyttig for å finne frem til egnede metoder og verktøy for å gjennomføre risikovurderinger. I vårt anbefalte rammeverk i kapittel 7 benytter vi blant annet sløyfediagram som hjelpemiddel.

Til grunn for utviklingen av rammeverket ligger også en gjennomgang av risikofaglig vitenskapelig litteratur. I kapittel 5 beskrev vi kilder til usikkerhet, spesielt som følge av kompleksitet. Hvordan kan vi styre risiko når usikkerheten og kompleksiteten er høy?

Aven argumenterer for at når usikkerheten er høy, er tradisjonelle risikovurderinger alene ikke tilstrekkelig.[103] Ifølge Aven er det tre strategier for å styre risiko:

- *Risikoinformert strategi* som bygger på risikovurderinger, og basert på disse vurderingene håndteres risiko gjennom å unngå, redusere, overføre eller akseptere risikoer.

[102] Standard Norge (2019). *Risikostyring – Metoder for risikovurdering (Risk management – Risk assessment techniques).* NS-IEC 31010:2019.
[103] Aven, T. (2015). "Implications of black swans to the foundations and practice of risk assessment and management". *Reliability Engineering and Systems Safety 134*, s. 83-91.

- *Forsiktighetsstrategi*, det vil si en strategi av robusthet og resiliens som legger vekt på konstant overvåkning og økt kunnskap gjennom forskning og utvikling for å identifisere alternative måter å oppnå robusthet og resiliens.

- *Diskursiv strategi* for å bygge tillit og troverdighet gjennom å redusere usikkerhet, klargjøre fakta, involvere berørte mennesker, foreta avveininger og ansvarliggjøring.

Kompleksiteten og usikkerheten tilsier at det bør legges økt vekt på resiliens, det vil si å iverksette tiltak for å heve systemers motstandsdyktighet, redundans og tilpasningsevne for å redusere sårbarheter. Denne innfallsvinkelen er noe Hollnagel argumenterer for innenfor *resilience engineering* for å øke systemers evner til å justere sin funksjon før, under eller etter endringer og forstyrrelser, slik at systemene kan opprettholde nødvendige operasjoner under både forventede og uventede forhold.[104]

For komplekse systemer kan sikkerhet ikke utledes basert på de enkelte komponentenes pålitelighet. Sikkerhet må ses på som en egenskap på systemnivå. Sikkerhet er uløselig knyttet til systemet som helhet, inkludert systemets avhengigheter, koblinger og samvariasjon mellom enkeltdeler og subsystemer. En slik tilnærming finner vi i systemteori anvendt innenfor risiko og sikkerhet. Rammeverket er derfor inspirert av systemteoretisk teori og metoder samt ovenfor nevnte strategier. De neste delkapitlene presenterer to relevante systemteoretiske tilnærminger til risiko og sikkerhet som rammeverket er inspirert av. Metoden som presenteres i kapittel 6.3 er en videreutvikling av metoden i kapittel 6.2.

## 6.2 Systemteoretisk prosessanalyse for *security*

Leveson har utviklet en systemteoretisk prosessanalyse til sikkerhet,[105] primært for *safety*, men hun mener at det også er en nyttig tilnærming på *security*-området.[106] Tilnærmingen for security kaller hun *Systems-Theoretic Process Analysis for Security* (STPA-Sec), eller systemteoretisk prosessanalyse for security. Den er utviklet for å sikre komplekse systemer mot cyberhendelser. Young og Leveson argumenterer for å endre perspektiv og startpunkt i sikkerhetsanalyser. I stedet for tilnærminger som vektlegger å analysere *trusler* som årsak til tap og uønskede konsekvenser, anbefales heller å vektlegge de sosiotekniske *sårbarhetene* som tillater forstyrrelser å forplante seg i systemet. Argumentet er at ondsinnede handlinger er utenfor sikkerhetsanalytikernes kontroll, og derfor bør det heller legges vekt på å kontrollere systemets sårbarheter. Et overordnet mål for sikkerhetsarbeidet er derfor å identifisere sårbarheter og begrense systemet fra å komme i sårbare tilstander som kan gi negative konsekvenser.

Trusselbaserte tilnærminger egner seg best ved tilgang på god etterretningsinformasjon, der årsak og virkning er tett koblet i tid og rom, samt at mulige trusselaktørers virkemidler, motiver og

[104] Hollnagel, E., Paries, J., Woods, D. D & Wreathall J. (2011). *Resilience engineering in practice: A guidebook*. Farnham, UK: Ashgate.
[105] Leveson, N.G. (2011).
[106] Young, W. & Leveson, N. (2013). *Systems thinking for safety and security*. In Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13). ACM, New York, NY, USA, s. 1-8.

evner er godt kjent og mulige handlemåter kan forutses. En trusselbasert tilnærming kan være nyttig for å identifisere og motstå sikkerhetstrusler mot en veldefinert og godt forstått systemverdi eller komponent. Imidlertid vil en slik tilnærming ha begrenset nytte for å sikre komplekse, koblede infrastrukturer og systemer mot avanserte trusselaktører.

Skade på og bortfall av IKT-baserte funksjoner i moderne organisasjoner der IKT er en integrert faktor, er gjerne et resultat av komplekse vekselvirkninger mellom ulike sosiotekniske system-komponenter. Skade eller tap skyldes ikke nødvendigvis at enkeltkomponenter feiler, men som vekselvirkninger i hele systemet. Det er derfor ikke tilstrekkelig å bryte systemet ned i enkelt-komponenter og sørge for at disse ikke feiler, selv om dette fortsatt vil være viktig. For å sikre komplekse sosiotekniske systemer mot tap, mener Leveson at det er nødvendig med en *top-down* analyseprosess der en tverrfaglig gruppe kan identifisere og iverksette begrensninger (*constraints*) for å unngå at systemet settes i sårbare tilstander som fører til tap. En slik analyseprosess er kun mulig med en tverrfaglig gruppe med risiko- og sikkerhetsfaglig kompetanse og dyp innsikt i operasjonelle forhold samt domenekompetanse. Vi velger å oversette ordet constraint med beskrankning[107].

Begrepet *control* er sentralt i modellen til Leveson. Standard Norge oversetter control med kontroll, og definerer kontroll som «tiltak som modifiserer risiko».[108] En nyere definisjon fra Standard Norge og ISO er «tiltak som opprettholder og/eller modifiserer risiko».[109] Det bemerkes at «kontroller inkluderer, men er ikke begrenset til, enhver prosess, policy, plan og praksis eller andre forhold og/eller ordninger som opprettholder og/eller modifiserer risiko» samt at «[d]et er ikke alltid at kontroller har den antatte modifiserende virkningen».[110]

De systemteoretiske tilnærmingene vi presenterer i dette kapitlet, kombinerer systemteori med kontrollteori. I denne sammenhengen benyttes begrepene kontroll og kontrollhandling om funksjoner og handlinger som setter beskrankninger for systemet på ulike måter.

STPA-Sec består av fire analysetrinn:[111]

1. **Etablere grunnlaget for analysen, systemforståelse og kontrollstruktur**

Analysen starter med å etablere organisatoriske formål og målsettinger for selve analysen. Dette steget krever at ledelsen også involveres i tillegg til sikkerhetsfaglig og annen ekspertise i en analysegruppe. Første oppgave er å identifisere de tapene, det vil si de negative konsekvensene, som anses å være uakseptable for virksomheten.

[107] Beskrankning er et ord brukt blant annet i matematikkfaget i betydningen avgrensning, skranke eller vilkår.
[108] Standard Norge (2009).
[109] Standard Norge (2018a).
[110] Standard Norge (2018a).
[111] Beskrivelsen av de fire trinnene er basert på Young & Leveson (2013).

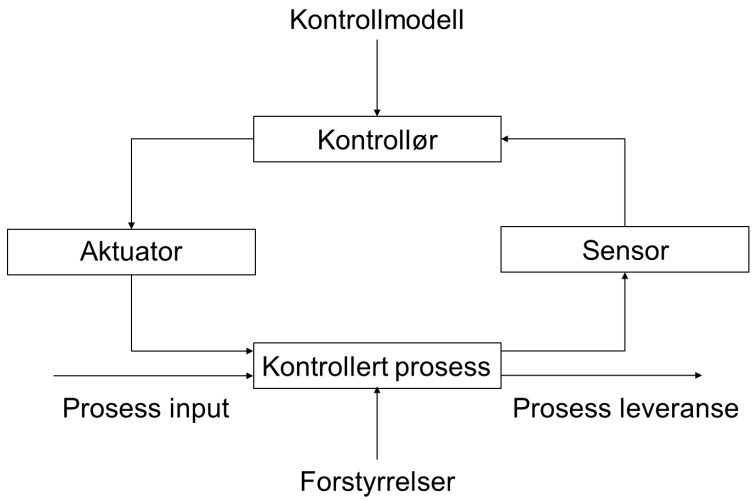
Spørsmålene analysegruppen søker svar på innledningsvis er:

- Hvilke essensielle funksjoner og tjenester må sikres mot forstyrrelser?
- Hva representerer uakseptable tap?
- Hvordan kan uønskede hendelser skje?

Analysegruppen legger seg på et overordnet virksomhetsnivå, og foretar en top-down analyse basert på virksomhetens mål, og i hvilken kontekst systemet skal fungere. Det advares mot å vektlegge motstandere og trusler for tidlig i prosessen.

En virksomhet må sikre at de kritiske funksjonene og tjenestene som IKT-systemer og -infrastrukturer leverer, opprettholdes selv om de utsettes for påkjenninger og forstyrrelser. Ved å identifisere og kontrollere sårbarheter, kan systemet beskyttes mot forstyrrelser som skyldes både kjente og ukjente trusler. Trusler adresseres først etter at det er etablert en dypere systemforståelse og kunnskap om hvilke situasjoner og kontekst trusselaktører kan operere i, og hvilke angrep fra dem som faktisk gir kritiske tap eller degradering.

Modellen for årsakssammenhenger (kausalitet) i STPA-Sec er basert på kontroll og hierarki. I stedet for å attribuere et tap til en enkelthendelse eller hendelseskjede, er formålet med STPA-Sec å utvikle og bevare kontroller for systemet som helhet. Som en del av første trinn etableres en overordnet kontrollstruktur (High Level Control Structure). Dette er en oversikt over hensyn, aspekter og funksjonelle kontroller, både tekniske og organisatoriske, som overvåker og setter beskrankninger for systemet. Den overordnede kontrollstrukturen bygges opp av én eller flere kontrollsløyfer (*control loop*). Figur 6.1 viser en forenklet modell for en slik kontrollsløyfe.




*Figur 6.1 Forenklet kontrollsløyfe i en overordnet kontrollstruktur. Figuren er basert på Young & Leveson (2013) og Njå et al. (2020, s. 135).*

2. **Identifisere usikre kontrollhandlinger**

Kontrollinformasjon flyter gjennom systemet og regulerer hvordan systemet oppfører seg. En fordel ved Young og Leveson sin tilnærming er at den søker å identifisere og kontrollere systemets sårbare tilstander som kan føre til tap på systemnivå, i stedet for kun å unngå svikt eller tap for enkeltkomponenter.

Usikre kontrollhandlinger er ifølge Young og Leveson:

- En kontrollhandling fører til en fare eller at sårbarheter kan utnyttes.
- Å ikke utføre en kontrollhandling fører til en fare eller at sårbarheter kan utnyttes.
- Å utføre kontrollhandlinger for sent, for tidlig eller i feil rekkefølge fører til en fare eller at sårbarheter kan utnyttes.
- Å stoppe en kontrollhandling for tidlig eller å utføre kontrollhandlingen for lenge fører til en fare eller at sårbarheter kan utnyttes.

3. **Utvikle sikkerhetskrav og beskrankninger**

Dette trinnet består i å benytte de usikre kontrollhandlingene til å utvikle sikkerhetskrav og beskrankninger.

4. **Identifisere utløsende scenarioer**

Det siste trinnet består i å analysere den eksisterende fysiske og logiske infrastrukturen for å bestemme hvordan sikkerhetskrav og beskrankninger kan bli brutt. Basert på dette identifiseres et sett med scenarioer som kan føre til tap.

Disse scenarioene benyttes deretter som utgangspunkt for å identifisere beskyttelsestiltak for å hindre at tapsscenarioer forekommer, eller, hvis dette ikke er mulig, å identifisere tiltak som begrenser skadeomfanget av uønskede hendelser (tapsscenarioer).

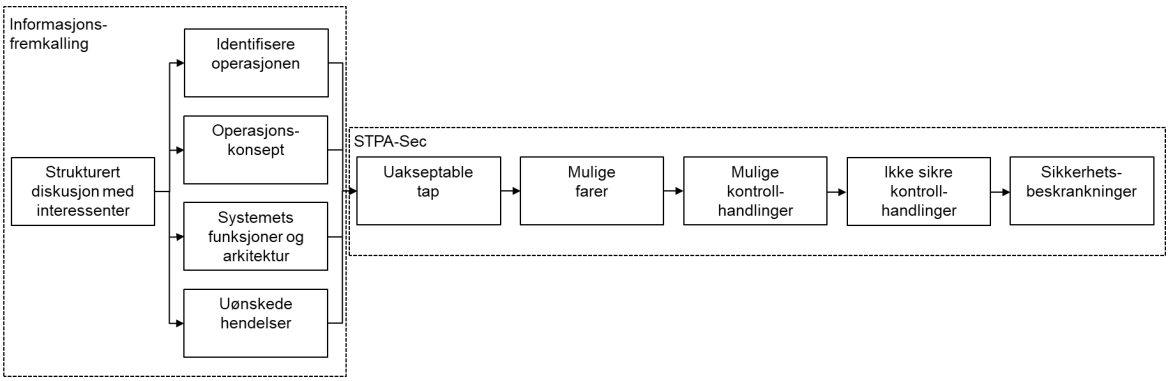
## 6.3 Systemtilnærming til risiko og sikkerhet for cyberfysiske systemer

Rammeverket for å vurdere risiko for Forsvarets bruk av IKT skal kunne benyttes for å utlede IKT-sikkerhetskrav ut fra hvordan IKT understøtter nasjonal sikkerhet, og mer spesifikt hvordan IKT inngår i og understøtter Forsvarets operasjoner. Hvilke sikkerhetskrav og -tiltak som settes til IKT avhenger av hva systemet brukes til og hvor viktig det er for brukerne. Carter et al. (2018) legger vekt på en slik operasjons- og verdisentrisk tilnærming og har videreutviklet STPA-Sec spesielt for sikkerhetsvurderinger for militære anvendelser av cyberfysiske systemer[112] slik som

[112] Som nevnt i kapittel 2.4, er cyberfysiske systemer smarte systemer som inkluderer konstruerte samhandlende fysiske og digitale komponenter.

for eksempel droner.[113] Carter et al. (2018) legger stor vekt på sammenhengen mellom de operasjonelle målene og selve systemet. Dette passer bra med systematikken i sikkerhetsloven. Vårt rammeverk er inspirert av og bygger på Carter et al. (2018) sin tilnærming.

Carters tilnærming består av to hoveddeler, henholdsvis informasjonsfremkalling[114] (*information elicitation*) og STPA-Sec. Vi gjengir innholdet i tilnærmingen i Figur 6.2 og i påfølgende tekst, slik Carter et al. (2018) beskriver den. I utviklingen av vårt rammeverk må vi tilpasse tilnærmingen til vårt formål, det vil si å oppnå et forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT.




*Figur 6.2 Konsept for hvordan informasjonsfremkalling understøtter STPA-Sec-analysen (basert på Carter et al. (2018)).*

**Trinn 1: Informasjonsfremkalling**

Formålet med informasjonsfremkallingen er å samle så mye data som mulig om den aktuelle operasjonen og bruken av systemet, inkludert operasjonens mål, suksesskriterier, hva som trengs for å gjennomføre operasjonen og systemets rolle i operasjonen. En analysegruppe leder diskusjonen med relevante interessenter, eksempelvis systemdesignere, militære ledere, operasjonelt personell, teknikere og annet relevant personell. Analysegruppen stiller spørsmål for å skaffe nok informasjon for senere å kunne lage en modell av systemet og bruken av det i operasjoner.

Basert på informasjonsinnhentingen utarbeides en detaljert beskrivelse av operasjonen, et operasjonskonsept for systemet som studeres, en liste over funksjoner eller komponenter som er kritiske for at operasjonen skal lykkes og innsikt om uakseptable, farlige og uønskede hendelser eller utfall av operasjonen. Analysegruppen bør ha en god forståelse av basisarkitektur, funksjon og formålet for operasjonen og systemet.

Basert på informasjonen som er utarbeidet, settes det opp en liste over operasjonens målsettinger, delmål, suksesskriterier, årsaker til at operasjonen kan feile og hva som kan utgjøre et

[113] Carter, B. T, Bakirtzis, G., Elks, C. R. & Fleming, C. H. (2018). "A systems approach for eliciting mission-centric security requirements." *IEEE*. . IEEE Xplore Full-Text PDF [sist besøkt 13.07.22]
[114] Vi velger å benytte informasjonsfremkalling selv om det er et litt spesielt og uvanlig ord på norsk.

uakseptabelt resultat av operasjonen. Deretter lages en oversikt over kritiske funksjoner, mål og handlinger for operasjonen. Analysegruppen utfordrer interessentenes rutiner, forventninger og erfaringer og undersøker ulike situasjoner som kan oppstå og hvordan interessentene håndterer dem.

Det totale resultatet av første trinn er en stor mengde data som må organiseres og systematiseres for å kunne benyttes i resten av analysen.

**Trinn 2: STPA-Sec**

Først etableres en systemteoretisk modell av operasjonen og systemet. Målet er å kunne etablere en modell fra overordnede målsetninger for operasjonen hele veien ned til programvare og fysiske komponenter slik at en får top-down og *bottom-up* sporbarhet i modellen. Hensikten er å kunne vurdere kaskadeeffekter ved endringer på ulike nivåer i modellen og effekter for operasjonens mål. Deretter skal man kunne identifisere og vurdere sårbare områder i systemet for å kunne ta grep for å håndtere sårbarhetene ved å enten dempe, akseptere eller eliminere dem.

Å konstruere modellen består av følgende trinn:

- Definere uakseptable utfall eller tap for operasjonen.
- Definere et sett scenarioer som potensielt kan resultere i uakseptable utfall.
- Skissere et funksjonelt hierarki og kontrollhandlinger som kan gjøres på hvert nivå under operasjonen (nivåene kan for eksempel være operasjonsplanlegger, systemoperatør og cyberfysisk system).
- Definere kontrollhandlinger for de ulike nivåene i det funksjonelle hierarkiet representert ved kontrollsløyfer.
- Representere kontrollhandlingene og funksjonsnivåene i et flytskjema som viser planlagt rekkefølge i en operasjon, noe som hjelper analytikerne å etablere en basis slik at avvik senere kan identifiseres og vurderes.
- Definere situasjoner der visse kontrollhandlinger ikke er sikre.

Å bruke modellen innebærer følgende handlinger:

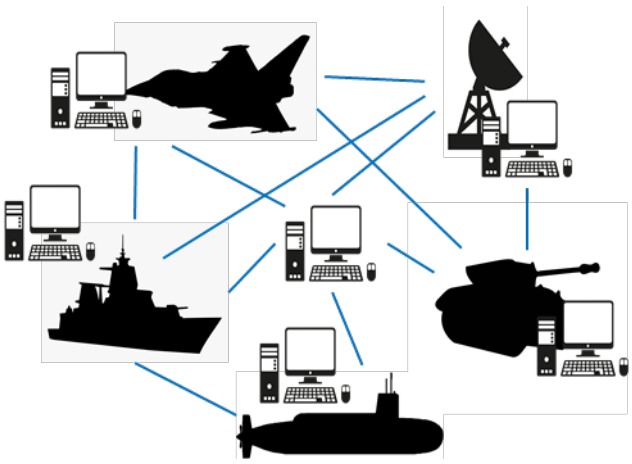
- Identifisere og prioritere uakseptable tap for operasjonen.
- Identifisere hvordan disse uakseptable tapene kan oppstå, og deretter hvordan disse tapene kan unngås eller dempes.
- Utlede sikkerhetskrav og beskrankninger for systemets oppførsel.
- Identifisere tapsscenarioer ved bruk av tilgjengelig informasjon for å bestemme hvordan uakseptable tap kan oppstå.
- Bestemme de mest sannsynlige eller mest skadelige måter mulige sikkerhetsbrudd kan oppstå på, og identifisere de mest kritiske komponentene, egenskapene og funksjonaliteten for systemet med hensyn på operasjonens suksess.
- Bruke resultatene av hele analysen for å velge hvilke IKT sikkerhetstiltak som bør implementeres.

# 7 Rammeverkets formål og forutsetninger

I denne rapporten presenterer vi et rammeverk som kan benyttes som hjelpemiddel for å vurdere og styre risiko og sikkerhet for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT. I dette kapitlet presenterer vi formålet med og forutsetningene for utviklingen av rammeverket, samt anbefalinger knyttet til kompetanse for gjennomføringen av denne type risikobaserte vurderinger.

## 7.1 Formål

Formålet med rammeverket er å etablere en systematikk og et forslag til tilnærming for funksjonsbaserte risikovurderinger som kan inngå i et beslutningsgrunnlag for styring av risiko og sikkerhet for Forsvarets bruk av IKT. Forsvaret er en sammensatt organisasjon som er avhengig av IKT-baserte funksjoner i væpnet konflikt, krise og fred. IKT-systemene og -infrastrukturen kan ses på som integratorer som bidrar på ulike måter til Forsvarets operative evner. Forsvaret er avhengig av IKT-basert infrastruktur for å kommunisere og utveksle informasjon mellom hovedkvarterer, kampplattformer som fregatter og kampfly, landstridsavdelinger og sensorer (se Figur 7.1 for en enkel illustrasjon av dette). IKT-systemene kan være integrert direkte i materiellet, de kan være i form av konvensjonell maskin- og programvare som brukerne vekselvirker med, eller IKT-systemene kan være en del av autonome og semi-autonome forsvarskapabiliteter. Fordi Forsvarets IKT-virksomhet er kompleks og omfattende, er det ikke hensiktsmessig eller mulig å ha ambisjon om én altomfattende og helhetlig analyse av risiko og sikkerhet. Det er nødvendig å gjøre avgrensninger, men uten at viktige aspekter ved helheten mistes av syne. I utviklingen av vårt rammeverk konsentrerer vi oss om Forsvarets bruk av IKT på et mer overordnet nivå, ikke primært om IKT som er integrert i materiell.



*Figur 7.1 Forsvarets bruk av IKT er en forutsetning for felles kommando og kontroll (K2) og synkroniserte militære operasjoner. IKT er også en integrert del av sensorer og våpenplattformer som fregatter, ubåter og kampfly.*

Forsvarsjefen (FSJ) er etatsleder for Forsvaret og har dermed ansvaret for å etablere og opprettholde et forsvarlig sikkerhetsnivå i etaten, inkludert for IKT-virksomheten.[115] Dette innebærer beslutninger knyttet til hvilket IKT-sikkerhetsnivå og hvilke IKT-sikkerhetstiltak som er tilstrekkelig for de IKT-baserte funksjonene Forsvaret er avhengig av, samt hvilken risiko som kan aksepteres, eller det som også kalles risikoappetitt. I henhold til sikkerhetsloven skal et forsvarlig sikkerhetsnivå etableres basert på risikobaserte vurderinger.

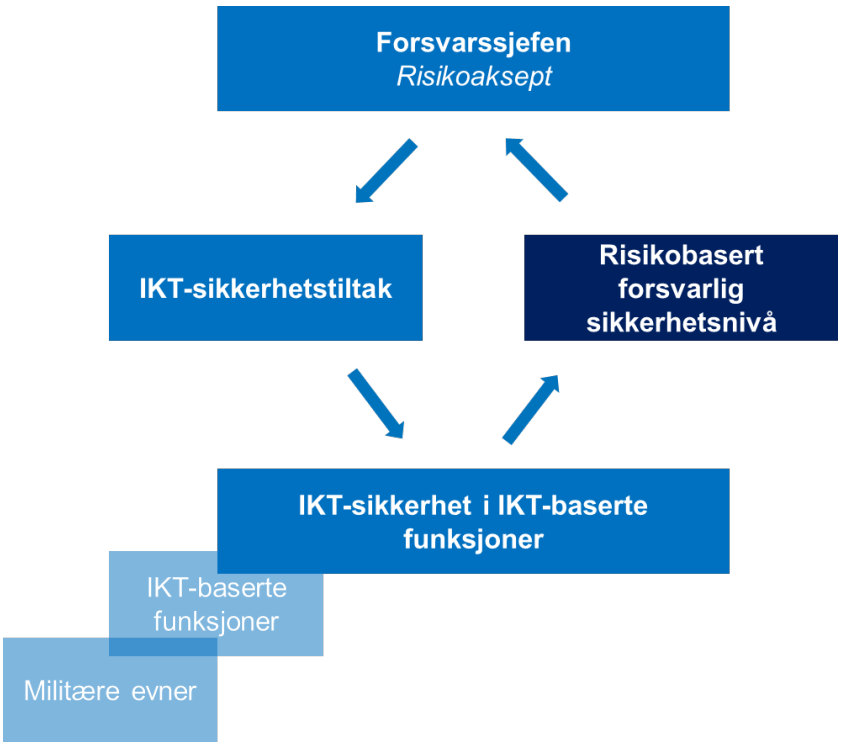
Formålet med funksjonsbaserte risikovurderinger er at FSJ skal ha et tilstrekkelig analyseunderlag og dokumentasjon for å kunne ta konsistente og helhetlige beslutninger, basert på forslag til en strategi og en handlings- og tiltaksplan. FSJ beslutter deretter å iverksette strategi og tiltak for å oppnå et forsvarlig sikkerhetsnivå. Fordi IKT-området kontinuerlig endres, og andre forhold og rammebetingelser også endres, må denne beslutningsprosessen være dynamisk og evne å ta inn utvikling og endring. Prosessen og elementene som inngår i beslutningsprosessen, er illustrert i Figur 7.2.

For å sette FSJ i stand til å ta beslutninger om hva som er et forsvarlig sikkerhetsnivå for de ulike delene av Forsvarets bruk av IKT, og hvilke tiltak som må til for å oppnå et slikt sikkerhetsnivå, må det først etableres en oversikt – en systeminnsikt. Dette bør være en strukturert og funksjonelt basert systeminnsikt over dagens IKT-systemer og -infrastrukturer, det vil si IKT-baserte funksjoner, som understøtter og inngår i Forsvarets militære evner. Detaljeringsnivået bør være hensiktsmessig, det vil si ikke for detaljert, slik at det egner seg for beslutningstakere strategisk nivå, men samtidig detaljert nok til å være et nyttig grunnlag for veivalg og beslutninger.

Vårt forslag til rammeverk for risikobaserte vurderinger av Forsvarets anvendelse og avhengighet av IKT-baserte funksjoner legger til grunn en top-down tilnærming. Risikovurderinger må baseres på tilstrekkelig forståelse av de ulike evnene og funksjonene som samlet utgjør Forsvarets evner for å kunne gjennomføre oppgaver i hele spennet fra væpnet konflikt, krise og fred. Å etablere en formålstjenlig systeminnsikt for en så sammensatt virksomhet som Forsvaret, er en krevende del av risikobaserte vurderinger. Det må derfor gjøres avgrensninger.

Basert på avgrensningen som er valgt, og en systeminnsikt er neste steg å vurdere risiko og sikkerhet for IKT-baserte funksjoner. Beslutningsgrunnlaget bør inneholde en verdibasert vurdering av risiko og eksisterende status for IKT-sikkerheten for de IKT-baserte funksjonene Forsvaret er avhengig av. Det må deretter vurderes i hvilken grad eksisterende IKT-sikkerhet er tilstrekkelig for et forsvarlig sikkerhetsnivå. Dersom det ikke er tilstrekkelig, må beslutningsgrunnlaget beskrive hva som bør til for å oppnå et forsvarlig sikkerhetsnivå, og eventuelt alternative løsninger i et forslag til handlings- og tiltaksplan.

[115] FD har fra 1. januar 2021 gitt FSJ «Ansvar, myndighet og funksjon for å utøve og videreutvikle den strategiske IKT-styringen i sektoren […]» (jf. FDs tildelingsbrev for Forsvaret 2021, ref. 2020/50888-1/FD III 3/TOHAB, s. 21). I denne rapporten fokuserer vi på Forsvarets bruk av IKT. Rammeverket kan imidlertid også benyttes av de øvrige etatene i sektoren for risikobaserte vurderinger innen IKT-området.




*Figur 7.2* *Forsvarssjefen er ansvarlig for å ta beslutninger om hvilket IKT-sikkerhetsnivå og hvilke IKT-sikkerhetstiltak som er tilstrekkelig for å ivareta et forsvarlig sikkerhetsnivå for Forsvarets IKT-baserte funksjoner og hvilken risiko som kan aksepteres, det vil si risikoappetitt.*

Formålet med rammeverket er todelt:

1. Utvikle en hensiktsmessig metodisk tilnærming og systematikk – et verdihierarki – for å utlede hvilke IKT-baserte funksjoner som inngår i ulike militære evner, og som understøtter de nasjonale sikkerhetsinteressene.

2. Foreslå en metodisk tilnærming for å vurdere risiko for IKT-baserte funksjoner som grunnlag for beslutninger om IKT-sikkerhetstiltak for å oppnå og opprettholde et forsvarlig sikkerhetsnivå.

## 7.2 Forutsetninger

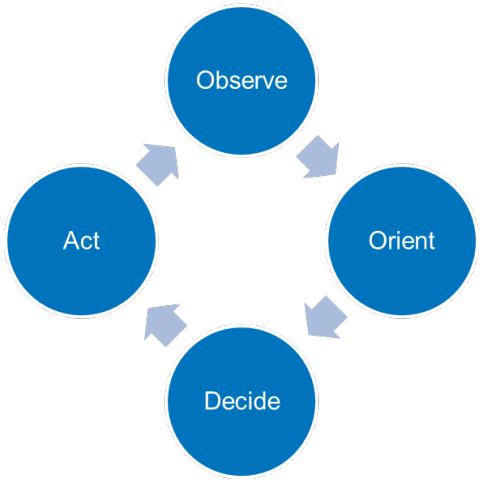
Et krav er at rammeverket skal være i tråd med sikkerhetsloven og virksomhetsikkerhetsforskriften, jf. kapittel 3. Videre har vi valgt å bygge på standarder og veiledere (se kapittel 4). En tredje forutsetning er at rammeverket skal være i tråd med systematikken og innretningen til Digital reguleringsplan (DRP) for forsvarssektoren.

### 7.2.1 Risiko som en dynamisk størrelse avhengig av kontekst

Vurderingen av risiko må knyttes til Forsvarets behov for og bruk av IKT i sin virksomhet, både i væpnet konflikt, krise og fred. Det er den funksjonaliteten IKT utgjør for Forsvaret i ulike situasjoner som er viktig, det vil si hvilke operative evner som IKT-baserte funksjoner bidrar til, både direkte og indirekte.

En militær operasjon utvikler seg dynamisk. Utviklingen og situasjonen avhenger av handlinger og effekter initiert av militære beslutningstakere med militær sjef øverst, eller hvis situasjonen krever det, beslutninger fattet på øverste politiske nivå, det vil si regjeringen. Videre er operasjonen avhengig av en eventuell motstanders og andre aktørers handlinger og respons på det som skjer. Nye beslutninger tas hele tiden, tilpasset situasjonen. Dette utgjør en kontinuerlig beslutningsprosess – en beslutningssløyfe.

Et eksempel på en beslutningssløyfe benyttet i militær sammenheng, er en OODA-løkke.[116] Løkken består av fire prosesser som ofte inngår i det å ta en beslutning og utføre en handling, henholdsvis observere (*observe*), orientere (*orient*), beslutte (*decide*) og handle (*act*). Direktoratet for samfunnssikkerhet og beredskap (DSB) har oversatt dette til OBBO på norsk der en ledelsessløyfe (beslutningssløyfe) består av å observere, bedømme, beslutte og gi ordre.[117] I en OODA-sløyfe er de fire prosessene bundet sammen av utveksling av informasjon representert med piler (se Figur 7.3). Figuren er svært forenklet, og ifølge Richards mente Boyd heller ikke at den nødvendigvis er sekvensiell slik som figuren kan gi inntrykk av.[118]

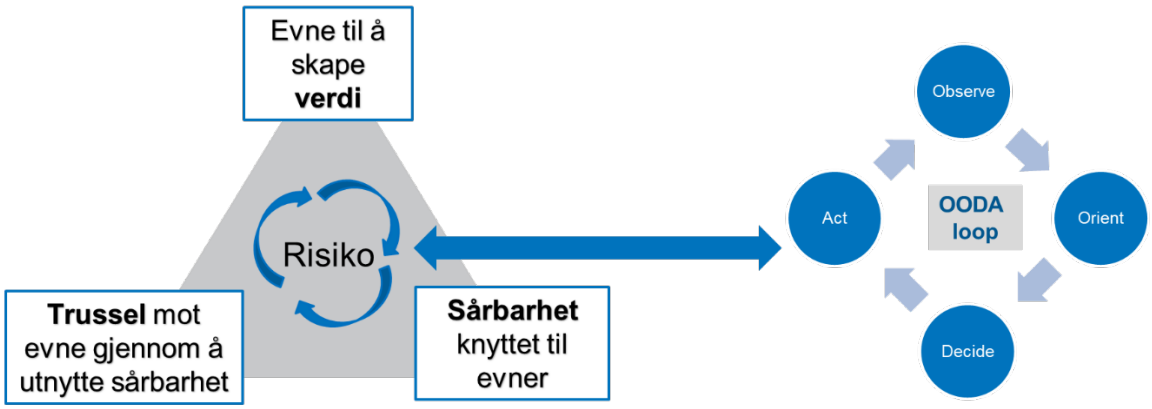



*Figur 7.3 En OODA-løkke er en beslutningssløyfe benyttet i militær sammenheng.*

[116] Richards, C. (2020). «Boyd's OODA loop». *Necesse 5*, nr. 1.
[117] DSB (2011). *Veileder om Enhetlig ledelsessystem (ELS).* veileder-om-enhetlig-ledelsessystem-els.pdf (dsb.no) [sist besøkt 15.07.22].
[118] Richards (2020).

Det sentrale aspektet vi ønsker å fremheve ved å vise til OODA-løkken, er at i militære operasjoner må beslutninger tas om og om igjen på ulike måter, og hele tiden tilpasses omskiftelige situasjoner og omgivelser. Hvor kritiske ulike IKT-baserte funksjoner er for militære evner, avhenger for det første av hvilke operative evner som er avgjørende i den konkrete militære operasjonen det er snakk om. For det andre avhenger dette av trusselbildet, hvor i krisespekteret man er og en rekke andre eksterne forhold. Behovet for IKT-baserte funksjoner, og hvor kritisk behovet er, bestemmes derfor av operativ kontekst.

Risikotrekanten illustrerer tre av faktorene som inngår i risiko, det vil si verdier, trusler og sårbarheter (se Figur 4.2). I utgangspunktet fremstår risikotrekanten som en statisk modell. Imidlertid, når behovet for IKT-baserte funksjoner endrer seg, endres også verdiene av de IKT-infrastrukturene, de IKT-systemene og den informasjonen som inngår i disse funksjonene. Truslene endrer seg avhengig av en motstanders intensjon og virkemidler. Videre kan IKT-baserte funksjoner i seg selv endres gjennom oppdateringer, feilretting eller konfigurering og så videre, og dermed endres også tilhørende sårbarheter. Dynamiske militære operasjoner medfører og påvirker i stor grad risiko, som derfor også er en dynamisk størrelse. Dette illustrerer vi i Figur 7.4.




*Figur 7.4 Dynamisk beslutningssløyfe for militære operasjoner representeres av en OODA-løkke (til høyre) som kontinuerlig påvirker evnen til å skape verdi, og dermed bidrar til en dynamisk risiko. Militære operasjoner medfører og påvirker risiko.*

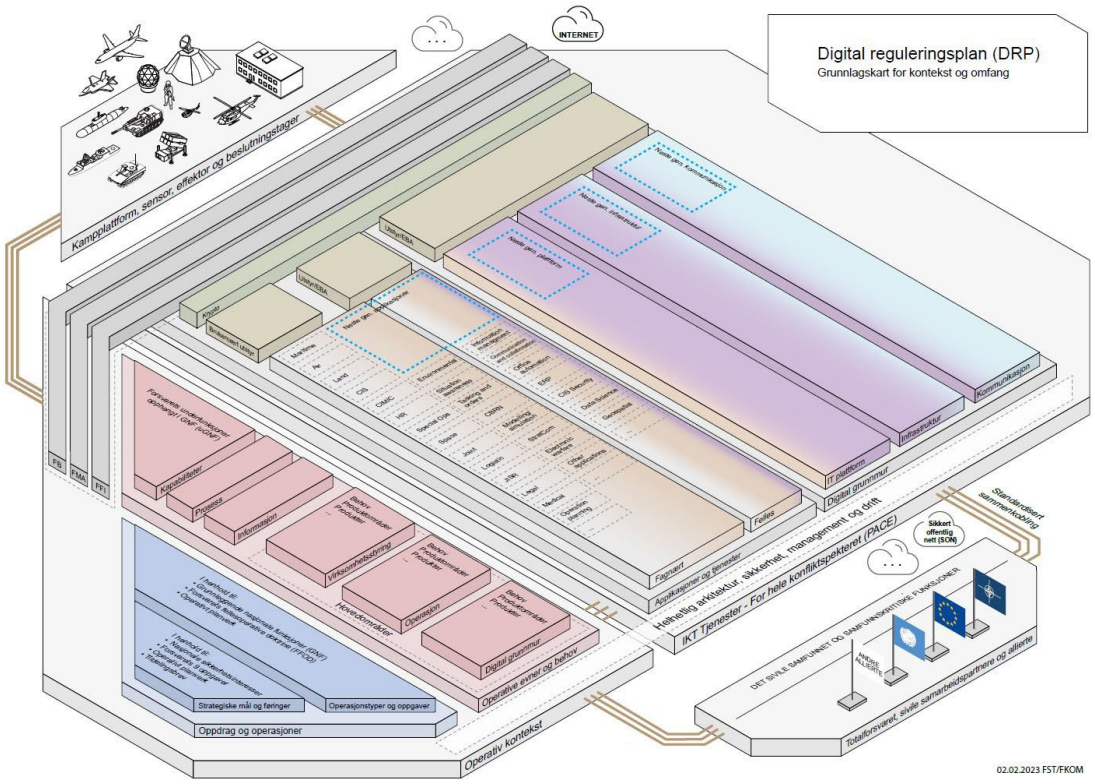
### 7.2.2 Digital reguleringsplan og NATOs C3-taksonomi

I tråd med Forsvarets IKT-strategi er det etablert en digital reguleringsplan (DRP)[119] for forsvarssektorens IKT-virksomhet med det formål å angi retning og regulere forsvarssektorens IKT. DRP setter rammer for utvikling, forvaltning og drift av IKT.[120]

En forutsetning er at vårt rammeverk i størst mulig grad skal være i tråd med Forsvarets styrende dokumenter. Dette gjelder i særdeleshet DRP da denne er førende for begrepsbruk, strukturering

[119] Se vedlegg i Forsvaret (2021).
[120] Forsvaret (2023b). *Digital reguleringsplan*. (BEGRENSET)

og utvikling innen Forsvarets IKT-virksomhet. Grunnlagskartet for DRP er vist i Figur 7.5, og en lesbar versjon er lagt ved i vedlegg A. Det fremstiller helheten i IKT-virksomheten og øvrig virksomhet i en lagvis platemodell. Kartet består av fire koblede hovedplater, henholdsvis «operativ kontekst og behov», «kampplattform, sensor, effektor og beslutningstager», «totalforsvaret og allierte» og «IKT-tjenester – for hele konfliktspekteret (PACE[121])». Denne siste platen viser applikasjons- og teknologiarkitekturen, og består av en digital grunnmur, applikasjoner og tjenester samt tilhørende utstyr.




*Figur 7.5 Grunnlagskartet for kontekst og omfang i henhold til Digital reguleringsplan (gjengitt med tillatelse fra Forsvaret, 2023).*

Forsvaret deler den digitale grunnmuren inn i IT-plattformer, infrastruktur og kommunikasjon, jf. DRP:

- «IT-plattformer vil si felles programvare og maskinvare som skaper kjøremiljø til applikasjonstjenestene. Heri ligger også operativsystemet, annen programvare og nødvendig infrastruktur som sikrer informasjon, funksjonalitet, drift og overvåking samt orkestrering.

- Infrastruktur vil si maskinvare for prosessering, lagring, brannmurer og datasenter.

[121] PACE står for *Primary, Alternate, Contingency, Emergency*, og er et prinsipp Forsvaret følger for å sikre tilstrekkelig redundans for Forsvarets bruk av IKT-tjenester.

- Kommunikasjon er overføring av data mellom applikasjoner og tjenester.»[122]

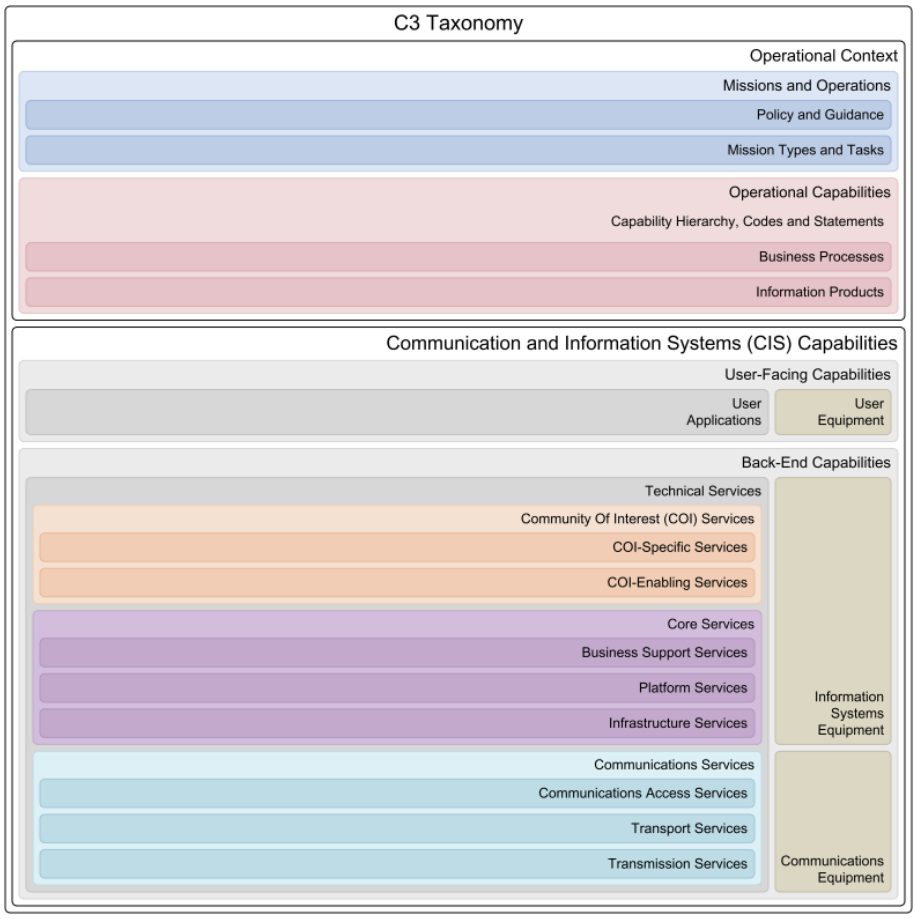
Grunnlagskartet for DRP bygger på NATOs taksonomi for kapabiliteter innen *Consultation, Command and Control* (C3).[123] C3-taksonomien er betydelig mer detaljert enn beskrivelsen i DRP. Det er derfor hensiktsmessig for vår studie å benytte den lagdelte inndelingen fra C3-taksonomien for å illustrere IKT-applikasjoner, -tjenester og -infrastruktur i rammeverket. Samtidig er målet å være tro mot strukturering og tenkningen bak DRP. Den lagdelte C3-inndelingen lar seg på en hensiktsmessig måte kombinere med den systemteoretiske tilnærmingen beskrevet i kapittel 6.

NATOs C3-taksonomi er et verktøy, felles språk og begrepsapparat med det formålet å synkronisere alle C3-kapabiliteter i NATO. Den knytter sammen NATOs strategiske konsept og politiske føringer, via NATOs prosess for forsvarsplanlegging ned til arkitektur og design av CIS-kapabiliteter (*Communication and Information Systems Capabilities*). C3-taksonomien omfatter både den operative konteksten (*Operational Context)* og CIS-kapabiliteter.[124] Den operative konteksten inneholder oppdrag og operasjoner (*Missions and Operations)* som støttes av operative evner (kapabiliteter) (*Operational Capabilities*).

I et lag under den operative konteksten finner man IKT-kapabilitetene som understøtter de operative evnene (kapabilitetene). Dette laget inneholder en kategorisering av funksjonaliteten man finner i NATOs informasjonsinfrastruktur. Øverst finner man brukerapplikasjonene (*User Applications*) som er den delen av IKT-kapabilitetene de operative brukerne ser og forholder seg til. Disse er tilpasset ulike domener og interessefellesskap gjennom ulike *Community of Interest (COI)*-tjenester.

Under brukerapplikasjonene finner man kjernetjenester (*Core Services*) og kommunikasjonstjenester (*Communications Services*). Kjernetjenestene består av mer generell maskinvare og programvare som leverer funksjonalitet til brukerapplikasjonene, mens kommunikasjonstjenestene sørger for å flytte informasjon mellom brukere og/eller noder i nettverket. Strukturen for NATOs C3-taksonomi er vist i fFigur 7.6.

[122] Forsvaret (2023a).
[123] NATO (2021). *C3 Taxonomy baseline 5.0*. Consultation, Command and Control Board (C3B).
[124] På norsk IKT-kapabiliteter.



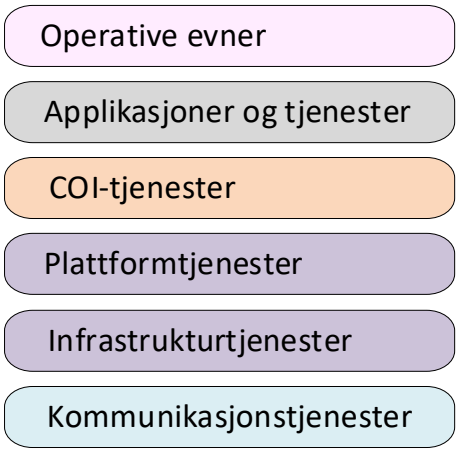

*Figur 7.6 Strukturen for NATOs C3-taksonomi (NATO, 2021 s. 8).*

Som vi ser av grunnlagskartet i DRP (vedlegg A), inngår ikke COI-tjenester direkte som en egen plate, men er en del av fagnært og felles på platen «applikasjoner og tjenester». I vårt eksempel i kapittel 7.5, og med den vinklingen vi har valgt, kommer vi heller ikke direkte inn på COI-tjenester. Vi har likevel tatt med COI-tjenester i laginndelingen fordi slike tjenester sannsynligvis er viktigere i andre konkrete eksempler og militære kontekster enn den vi kommer inn på i denne rapporten.

For vårt formål er det hensiktsmessig å systematisere IKT-systemer som inngår i Forsvarets IKT-baserte funksjoner i henhold til en lagdeling som illustrert i Figur 7.7. Denne inndelingen benytter vi senere i kapittelet når vi kommer inn på det konkrete eksempelet i kapittel 7.5. Øverst er operativ evne som innebærer aktiviteter for å oppnå overordnede mål, og for vår problemstilling er dette å ivareta nasjonal sikkerhet.

Brukeren av IKT forholder seg til applikasjoner og tjenester, det vil si de brukernære tjenestene, for å realisere operative evner. Applikasjoner og tjenester kan være alt fra enkle telefonitjenester, taleradio, forvaltningssystemer, fagspesifikke tjenester som meteorologitjenester til komplekse

beslutningsstøtteverktøy. COI-tjenester er tekniske tjenester som understøtter både felles og fagnære applikasjoner og tjenester.




*Figur 7.7 Lagdeling som forslaget til rammeverk benytter for å knytte operative evner til IKT-applikasjoner, -systemer og -infrastruktur som benyttes for å oppnå operativ effekt.*

Plattformtjenester består av den maskinvaren og programvaren som skal til for å levere nødvendig funksjonalitet til applikasjonene og tjenestene på lagene over. Et eksempel på en plattform er FISBasis B. En plattform kan bestå av flere datamaskiner i et større system. Da vil en ofte ha et datadistribusjonslag med overføring av informasjon internt innen plattformen.

Funksjonalitet i plattformene knyttes sammen av infrastrukturtjenester og kommunikasjonstjenester. Disse sørger for den funksjonaliteten som hver plattform har tilgjengelig for å formidle informasjon mellom brukerne, inkludert formidling av informasjon i nettverk.

## 7.3 Kompetansebehov

En god risikovurderingsprosess bør utføres av en tverrfaglig sammensatt analysegruppe. Det krever at flere kompetanseområder bringes inn og aktivt deltar. Med kompetanse menes her både kunnskap, ferdigheter og holdninger, som bygger både på utdanning og erfaring.[125] Følgende kompetanse er nødvendig:

- Domenekompetanse om det sosiotekniske systemets mål, prosesser og funksjonalitet, det vil i vårt tilfelle si:
    - Kompetanse om militære operasjoner på de nivåer av operativ virksomhet som skal inkluderes i analysen. I vårt eksempel er dette kompetanse både på operasjonelt, taktisk og sub-taktisk nivå i Forsvaret.

[125] Lai, L. (2011). Kompetansemobilisering og egenmotivasjon. *Magma 3*, s. 50–55; Lai, L. (2013). *Strategisk kompetanseledelse* (3. utgave). Fagbokforlaget.

- Kompetanse om IKT-systemene, det vil si detaljert kompetanse om oppbygning, drift og vedlikehold av IKT-systemene, funksjonalitet og IKT-sikkerhetsmekanismer og sårbarheter.

- Trusselfaglig kompetanse om motstanders intensjoner, midler og mulige angrepsscenarioer, det vil i vårt tilfelle si:
  - Etterretningskompetanse – herunder kompetanse om IKT-angrep og cyberoperasjoner.
  - Annen relevant trusselkompetanse – herunder kunnskap om ulike angrepsvektorer.

- Risiko- og sikkerhetsfaglig kompetanse, det vil si:
  - Metodekompetanse – for å kunne skreddersy bruk av egnede tilnærminger og metoder til analysens formål samt tid og ressurser tilgjengelig.
  - IKT-sikkerhetsfaglig kompetanse – for å kunne vurdere IKT-sikkerhetskrav og -tiltak.
  - Prosesskompetanse – for å kunne tilrettelegge og gjennomføre en egnet risikovurderingsprosess.

Vi anbefaler at det legges til rette for en tverrfaglig gruppeprosess, og at informasjonsinnhenting til analysen ikke kun baseres på at risikoanalytikere foretar intervjuer. Erfaringsmessig er det viktig at det etableres en arena for å sikre dynamikk, tverrfaglige diskusjoner og iterasjoner, samt felles kvalitetssikring. Samtidig vil dette bidra til forankring av analyseresultatet i relevante miljøer.

# 8 Forslag til rammeverk

I dette kapitlet presenterer vi et forslag til rammeverk og tilnærming for funksjonsbaserte risikovurderinger som kan inngå i et beslutningsgrunnlag for styring av risiko og sikkerhet for Forsvarets bruk av IKT. Formålet med rammeverket er å etablere et grunnlag for beslutninger om IKT-sikkerhetstiltak for å oppnå og opprettholde et forsvarlig sikkerhetsnivå. Som tittelen på rapporten presiserer, er dette en innledende studie, og rammeverket må utvikles videre og testes før det kan tas i bruk i Forsvaret.

I kapittel 8.1 presenterer vi rammeverkets struktur. Kapittel 8.2 presenterer et verdihierarki for nasjonal sikkerhet for forsvarssektoren i tråd med sikkerhetsloven og andre føringer. Som presisert i kapittel 7.2.1, er risiko en dynamisk størrelse som er avhengig av kontekst. I den resterende delen av rammeverket bruker vi derfor ett av Forsvarets oppdrag for å illustrere tilnærmingen. Kapittel 8.3 tar for seg hvordan informasjonsfremkallingen om operativ kontekst og operasjonskonsept kan beskrives. I kapittel 8.4 presenterer vi momenter som inngår i risikovurderinger og risikostyring.

## 8.1 Rammeverkets struktur

Rammeverket har en hierarkisk struktur som søker å lage en sammenheng og sporbarhet mellom overordnede målsettinger, nasjonale sikkerhetsinteresser og militære operative evner ned til det teknologiske nivået og forsvarlig sikkerhetsnivå for de IKT-systemene, IKT-infrastrukturen og informasjonen som skal sørge for militær operativ evne. Vi har valgt å dele rammeverkets struktur inn i tre nivåer og kaller nivåene premiss, informasjonsfremkalling og risiko. Strukturen er vist i Figur 8.1.

I tråd med sikkerhetslovens bestemmelser skal de overordnede nasjonale sikkerhetsinteressene, de fem grunnleggende nasjonale funksjonene (GNF-ene) for forsvarssektoren og underfunksjonene som er definert av FD for hver av disse GNF-ene, ligge til grunn for å vurdere risiko for å oppnå et forsvarlig sikkerhetsnivå. I tillegg har myndighetene gitt politiske føringer og besluttet hvilke oppgaver Forsvaret skal løse. Samlet utgjør dette et overordnet premiss i rammeverket, og vi har utviklet et verdihierarki for nasjonal sikkerhet for forsvarssektoren som kan benyttes som utgangspunkt for vurderinger av risiko og forsvarlig sikkerhet i sektoren, ikke kun begrenset til bruk av IKT.

For å vurdere risiko for Forsvarets bruk av IKT, er det nødvendig å sette bruken av IKT inn i en operativ kontekst. Det er den funksjonaliteten IKT gir Forsvaret i ulike situasjoner som er viktig, det vil si direkte og indirekte bidrag til operative evner. Bruken og avhengigheten av IKT-baserte funksjoner for operativ evne er avgjørende for hvor viktig en funksjon er, og dermed også hvor viktig det er å sikre IKT-funksjonen, og informasjonens konfidensialitet, tilgjengelighet og integritet. Sikkerhetskrav på IKT-systemnivå må utledes ut fra hva Forsvaret bruker IKT til. Derfor har vi benyttet et konkret eksempel for å utvikle og illustrere tilnærmingen for å vurdere risiko og forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT. Vi har valgt et av Forsvarets

oppdrag innen luftoperativ virksomhet i fredstid – «hurtig reaksjonsvarsel» – *quick reaction alert* (QRA).[126] Videre viser vi hvordan oppdraget QRA kan brytes ned i oppgaver og IKT-baserte funksjoner slik at det er mulig å identifisere hvilke IKT-systemer, IKT-infrastruktur og informasjon som inngår i disse IKT-baserte funksjonene. Å innhente og systematisere informasjon om operativ kontekst utgjør informasjonsfremkalling i rammeverket. Innholdet er inspirert av Carter *et al.* (2018) (se Figur 6.2).


*Figur 8.1 Rammeverk for risikobasert vurdering av forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT.*

Det neste nivået i rammeverket er den risikobaserte vurderingen knyttet til Forsvarets avhengighet og bruk av IKT-baserte funksjoner for å oppnå den ønskede militære evnen og utføre oppdraget. I slike vurderinger er det en rekke kilder til usikkerhet, som beskrevet i kapittel 5. Usikkerhet, inkludert den usikkerhet som følger av kompleksitet, er særlig viktige utfordringer i utviklingen av risikovurderinger og forståelsen av forsvarlig sikkerhet, og må derfor inkluderes. I kapittel 5 er kilder til usikkerhet beskrevet, herunder kompleksitet. Basert på den militære målsettingen og vurdering av kritikalitet for de IKT-baserte funksjonene defineres forsvarlig sikkerhetsnivå for de IKT-baserte funksjonene som inngår.

[126] Forsvaret (2023a). *Dette er QRA – Quick Reaction Alert*. Dette er QRA – Quick Reaction Alert - Forsvaret. [sist besøkt 09.01.23].

Å vurdere risiko som grunnlag for å oppnå forsvarlig sikkerhetsnivå, kan utføres på mange måter og gjerne ved en kombinasjon av ulike verktøy og metoder, for eksempel veiledere som presentert i kapittel 4.2, eller ved systemteoretiske tilnærminger (se kapittel 6). I risikodelen av rammeverket anbefaler vi å bruke en kombinasjon av hensiktsmessige metoder og fremgangsmåter som er tilpasset formålet og problemstillingen (kapittel 3) og tenkesett som er i tråd med relevante standarder og veiledere (kapittel 4). Vi mener en systemteoretisk tilnærming til risiko og sikkerhet kan være nyttig, og derfor bør utforskes videre. Slike tilnærmingsmåter er kort beskrevet i kapittel 6, men det har ikke vært innenfor denne studiens rammer å utforske dette i praksis. Dette foreslår vi derfor for videre studier.

## 8.2 Verdihierarki for nasjonal sikkerhet

Som presisert i kapittel 7.1, er ett av to formål med rammeverket å utvikle en metodisk tilnærming – et verdihierarki – for å utlede hvilke IKT-baserte funksjoner som inngår i militære evner, som så understøtter de nasjonale sikkerhetsinteressene. Dette utgjør et premiss i rammeverket, det vil si den øverste delen i rammeverkets struktur (se Figur 8.1).

I dette kapitlet presenterer vi hvordan en top-down systematikk i sikkerhetsloven med utgangspunkt i forsvars- og sikkerhetspolitikkens formål og de overordnede nasjonale sikkerhetsinteressene kan brukes for å identifisere underliggende verdier.

Moderne sikkerhet må være forankret i tilstrekkelig innsikt i virksomhetens overordnede verdier, det vil si de verdier som utvikles og forvaltes som resultat av virksomhetens kjerneaktiviteter. Dette er det som kalles en verdisentrisk tilnærming. For Forsvarets del er de overordnede verdiene operative evner, det vil si at Forsvaret er i stand til å utføre sine militære oppgaver når det trengs for å beskytte nasjonal sikkerhet.

IKT-sikkerhet har ofte blitt håndtert som en taktisk utfordring med vekt på best å beskytte IKT-nettverk og informasjon mot trusselaktører. Dette er viktig, men det kan føre til at det helhetlige målet mistes av syne, nemlig beskyttelse av kjerneaktiviteter og -verdier. For Forsvarets del er det overordnede målet å beskytte IKT ut fra hvordan IKT bidrar til Forsvarets ivaretakelse av statssikkerhet og nasjonale sikkerhetsinteresser. I praksis betyr dette å etablere en sammenheng mellom nasjonal sikkerhet, Forsvarets operative evner og IKT-baserte funksjoner, det vil si å etablere et verdihierarki. Dette innebærer det vi kan kalle en strategisk, helhetlig og top-down tilnærming i tråd med en systemteoretisk tilnærming til risiko og sikkerhet.

Sikkerhetslovens formål er, som beskrevet i kapittel 3.1, å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser, heretter omtalt som å ivareta «nasjonal sikkerhet». Politiske myndigheter presiserte i langtidsplan for forsvarssektoren (LTP) at «[s]ikkerhets- og forsvarspolitikkens formål er å verne om statssikkerheten og sette

Norge i stand til å svare på utfordringer i hele krisespekteret, fra alvorlige trusler og episodehåndtering i fred, via sikkerhetspolitisk krise til væpnet konflikt».[127] Å ivareta nasjonal sikkerhet, og sikkerhets- og forsvarspolitikkens formål, er det øverste nivået i verdihierarkiet.

I LTP poengterer myndighetene at «Norge trenger et forsvar for å ivareta det grunnleggende og tidløse ansvaret det er å skape sikkerhet for staten, befolkningen og samfunnet.».[128] Forsvaret er derfor en etat hvis overordnede oppdrag er å ivareta nasjonal sikkerhet. Neste nivå i vårt verdihierarki er derfor politiske myndigheters oppdrag til Forsvaret. Stortinget har gjennom vedtak av nåværende og tidligere langtidsplaner besluttet at Forsvaret har følgende ni oppgaver, hvorav de sju første skal være dimensjonerende for Forsvarets struktur og innretning:[129]

1. Sikre troverdig avskrekking med basis i NATOs kollektive forsvar.

2. Forsvare Norge og allierte mot alvorlige trusler, anslag og angrep, innenfor rammen av NATOs kollektive forsvar.

3. Avverge og håndtere episoder og sikkerhetspolitiske kriser med nasjonale ressurser, herunder legge til rette for alliert engasjement.

4. Sikre et nasjonalt beslutningsgrunnlag gjennom overvåking og etterretning.

5. Hevde norsk suverenitet og suverene rettigheter.

6. Ivareta myndighetsutøvelse på avgrensede områder.

7. Delta i flernasjonal krisehåndtering, herunder fredsoperasjoner.

8. Bidra til internasjonalt samarbeid på det sikkerhets- og forsvarspolitiske området.

9. Bidra til ivaretakelse av samfunnssikkerhet og andre sentrale samfunnsoppgaver.

I henhold til sikkerhetsloven skal hvert sektordepartement, identifisere sine GNF-er, det vil si «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser». [130] FD har utpekt fem GNF-er (se kapittel 3.1). FD har operasjonalisert disse i underfunksjoner,[131] og dermed etablert et verdihierarki for forsvarssektorens kjernevirksomhet. Figur 8.2 viser dette verdihierarkiet. I denne rapporten gjengir vi ikke listen over underfunksjoner da listen er unntatt offentlighet i henhold til offentleglova § 21.

[127] Prop. 14 S (2020–2021). *Evne til forsvar – vilje til beredskap. Langtidsplan for forsvarssektoren*, s. 19.
[128] Prop. 14 S (2020–2021), s. 7.
[129] Prop. 14 S (2020–2021), s. 11.
[130] Sikkerhetsloven.
[131] Forsvarsdepartementet (2020).

Verdihierarkiet gjelder generelt for forsvarssektoren. Det viser imidlertid ikke avhengigheter som forsvarssektorens GNF-er og underfunksjoner har til andre sektorers GNF-er. Eksempler på slik avhengighet er til GNF «Posisjonsbestemmelse, navigasjon og tidsbestemmelse» innmeldt av Justis- og beredskapsdepartementet, GNF «Evne til å ivareta grunnleggende internettilgang» identifisert av Kommunal- og distriktsdepartementet og GNF «Nasjonal kraftforsyning» identifisert av Olje- og energidepartementet.[132] I risikovurderinger er det viktig at slike avhengigheter kartlegges.

I den videre utviklingen av rammeverket velger vi å avgrense til de fire GNF-ene som gjelder for Forsvarets operative virksomhet og tilhørende underfunksjoner. De 21 underfunksjonene til de 4 GNF-ene er dekkende for bredden av Forsvarets oppgaver for å understøtte de overordnede nasjonale sikkerhetsinteressene og utføre de oppgavene politiske myndigheter har besluttet for Forsvaret.

Verdihierarkiet vist i Figur 8.2 er et avgjørende premiss for å sikre sammenheng og en tilnærming til verdisentrisk risikovurdering i tråd med sikkerhetsloven. For å illustrere rammeverkets neste del, informasjonsfremkalling, bygger vi videre på og benytter verdihierarkiet for nasjonal sikkerhet i forsvarssektoren for det konkrete eksempelet hurtig reaksjonsvarsel (QRA).

[132] Nasjonal sikkerhetsmyndighet (30.09.22). *Oversikt over innmeldte grunnleggende nasjonale funksjoner*. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/grunnleggende-nasjonale-funksjoner/oversikt-over-innmeldte-grunnleggende-nasjonale-funksjoner/ [sist besøkt 08.12.22].


*Figur 8.2 Verdihierarki for nasjonal sikkerhet i forsvarssektoren. I figuren har vi uthevet de viktigste momentene på hvert nivå.*

## 8.3 Operativ kontekst

Formålet med rammeverket er at dette kan benyttes for å vurdere risiko for Forsvarets bruk av IKT og anbefale IKT-sikkerhetstiltak for å oppnå et forsvarlig sikkerhetsnivå. En hensiktsmessig tilnærming er å beskrive Forsvarets bruk av IKT gjennom et sett av IKT-baserte funksjoner som er nødvendige for operative evner i ulike militære operasjoner der IKT er viktig. På denne måten

kan IKT-baserte funksjoner kobles opp til verdihierarkiet for nasjonal sikkerhet. Samtidig vil det sikre en funksjonsbasert tilnærming.

Formålet med andre del av rammeverket i Figur 8.1 – informasjonsfremkalling – er å innhente og systematisere informasjon om operativ kontekst, selve operasjonen og identifisere et funksjonelt hierarki (se kapittel 6.3). For å identifisere et sett med IKT-baserte funksjoner, og deretter koble disse til GNF-er og underfunksjoner, må vi først identifisere hvilke IKT-kritiske militære evner operasjonen krever. Når reelle vurderinger skal utføres, anbefaler vi at denne delen gjennomføres ved at en analysegruppe innhenter bred relevant informasjon fra en gruppe interessenter. Målsettingen er å etablere en cyberfysisk og sosioteknisk modell for den militære konteksten og operasjonen.

Strukturen og systematikken i rammeverket er som nevnt delt i tre hoveddeler: premiss, informasjonsfremkalling og risiko. Premisset er det overordnede verdihierarkiet for nasjonal sikkerhet og koblingen til forsvarssektorens GNF-er og underfunksjoner. Kontekst og dynamikk er avgjørende for en funksjonsbasert vurdering av risiko. For å utvikle og illustrere rammeverket har vi derfor benyttet eksempelet «hurtig reaksjonsvarsel» (QRA).[133] Det presiseres at eksempelet kun baserer seg på åpen informasjon fra Forsvaret. Vår bruk av eksempelet er svært forenklet og ikke basert på en reell vurdering av QRA og evner som inngår. Det sosiotekniske systemet som er vårt analyseobjekt (jf. kapittel 2.4) består av alle systemer, sosiale og tekniske, som skaper evnen hurtig reaksjonsvarsel. Dette er også i tråd med DRP som har et såkalt PTO-perspektiv, der PTO står for personell, teknologi og organisasjon.

QRA er et beredskapsoppdrag som Forsvaret utfører på vegne av NATO. Oppdraget forutsetter at Forsvaret kontinuerlig overvåker norsk luftrom og tilstøtende områder, noe Forsvaret gjør hele tiden også av nasjonale hensyn. I henhold til QRA står to norske kampfly hele tiden klare til å ta av fra Evenes flystasjon på 15 minutters varsel. Dette kan skje dersom ukjente luftfartøy er på vei mot norsk luftrom. Kampflyenes oppgave er da å finne, identifisere og dokumentere de ukjente flyene, samt å hindre at luftfartøyer tar seg ulovlig inn i norsk luftrom.

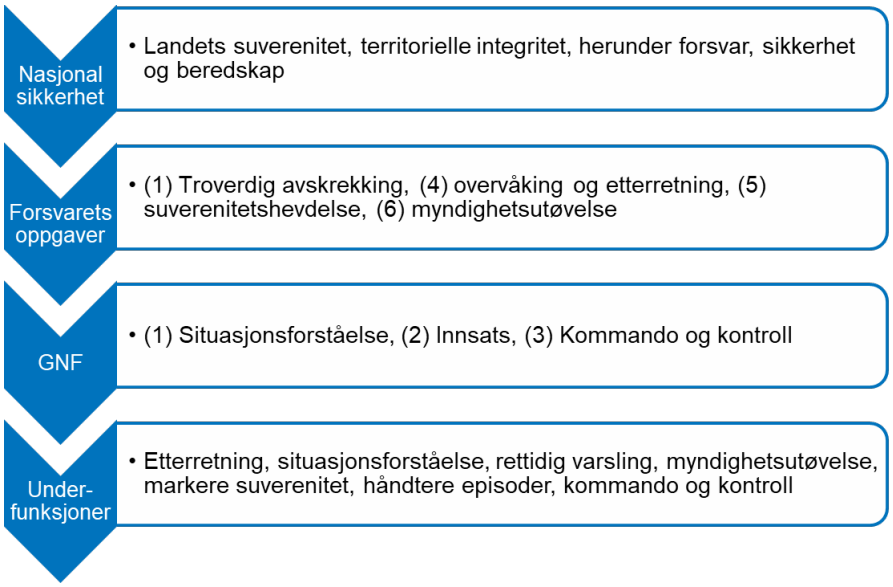
Det er kan generelt være krevende å identifisere IKT-kritiske evner, og ulike tilnærminger kan hjelpe. Én mulig tilnærming for å gå gjennom Forsvarets ulike evner/kapabiliteter slik de er benyttet i FFIs støtte til Forsvarets langtidsplanlegging,[134] og å vurdere kapabilitetenes avhengighet av IKT, er utviklet i FFI-prosjektet «Forsvarets bruk av det digitale og elektromagnetiske rom».[135] Denne tilnærmingen har blitt testet for to caser.[136]

[133] Forsvaret (2023a). *Dette er QRA – Quick Reaction Alert*. Dette er QRA – Quick Reaction Alert - Forsvaret. [sist besøkt 09.01.23]
[134] Vatne, D. F, Køber, P. K., Guttelvik, M. S., Arnfinnsson, B. & Rise, Ø. R. (2020). *Norwegian long-term defence analysis – a scenario- and capability-based approach*. FFI-rapport 20/02367. Kjeller: Forsvarets forskningsinstitutt.
[135] Farsund, B. H., Thuv, Aa. & Hansen, B. J. (2022). *Hvordan håndtere IKT i Forsvarets langtidsplanlegging*. FFI-rapport 22/01569. Kjeller: Forsvarets forskningsinstitutt.
[136] Farsund, B. H., Thuv, Aa. & Hansen, B. J. (2022). *Hvordan håndtere operativ IKT i Forsvarets langtidsplanlegging? – et innspill med testcaser;* FFI-rapport 22/01703. Kjeller: Forsvarets forskningsinstitutt. (BEGRENSET)

### 8.3.1 Verdihierarki for eksempelet hurtig reaksjonsvarsel

Først identifiserer vi hvordan QRA bidrar til Forsvarets GNF-er og nasjonale sikkerhetsinteresser. Formålet med QRA er å ivareta nasjonal sikkerhet, herunder landets suverenitet og territorielle integritet. QRA inngår i nasjonale sikkerhetsinteresser kategori b) forsvar, sikkerhet og beredskap i Figur 3.1. Av Forsvarets ni oppgaver bidrar QRA til troverdig avskrekking ved at Norge og NATO klart markerer luftherredømme. Det bidrar til overvåking og etterretning gjennom kontinuerlig overvåking av luftrommet og andre lands aktiviteter i våre nærområder. Det bidrar til suverenitetshevdelse og myndighetsutøvelse ved at ukjente luftfartøy oppdages og hindres i å ulovlig ta seg inn i norsk luftrom.

Av Forsvarets fire GNF-er bidrar QRA til evnen situasjonsforståelse (GNF 1), evnen til innsats (GNF 2) og evnen til kommando og kontroll (GNF 3). Flere underfunksjoner under GNF 1, 2 og 3 er viktige for den militære evnen QRA, herunder evner innen etterretning, situasjonsforståelse, rettidig varsling og så videre. Disse er ikke listet her, da forsvarssektorens underfunksjoner er unntatt offentlighet. Den øverste delen av verdihierarkiet for den militære evnen QRA er vist i Figur 8.3.




*Figur 8.3 Verdihierarki for eksempelet for hurtig reaksjonsvarsel (QRA). Underfunksjonene er unntatt offentlighet, og derfor ikke spesifisert, kun omtalt på et overordnet nivå.*

### 8.3.2 Konkretisering av oppgaver for eksempelet hurtig reaksjonsvarsel

Forsvaret har på et overordnet nivå beskrevet hvilke oppgaver den militære evnen QRA består av:[137]

1. **Overvåke luftrom**. Luftforsvarets kontroll- og varslingssenter, CRC Sørreisa, overvåker og holder oversikt over lufttrafikken i og nær det norske luftrommet kontinuerlig hele døgnet og hele året. Til overvåkingen benytter CRC Sørreisa data fra en rekke radarer og samarbeider med sivile luftfartsmyndigheter.

2. **Oppdagelse**. Dersom CRC Sørreisa oppdager et ukjent luftfartøy meldes dette til Nasjonalt luftoperasjonssenter (National Air Operations Centre, NAOC) i Bodø og til NATOs CAOC (Combined Air Operations Centre) i Uedem i Tyskland.

3. **Ordre**. Sjefen i operasjonsrommet ved CAOC avgjør om det skal gis oppdrag om QRA til kampflyene.

4. **Avgang**. Fra ordre er gitt, klargjøres fly og kampflyene er i luften etter maksimalt 15 minutter.

5. **Identifisering**. Pilotene kommuniserer med CRC Sørreisa underveis. CRC Sørreisa benytter gradert radiosamband, link[138] og radarer for å planlegge manøvrering. Pilotene overtar navigeringen når de ser det ukjente luftfartøyet.

6. **Avskjæring, eventuelt eskortering**. Ved behov kan pilotene eskortere flyet til en utpekt flyplass eller ut av norsk luftrom. Ved en eventuell kapring av sivilt fly er det vanligvis sivile myndigheter ved politiet som håndterer hendelsen. Da vil NATO i så fall overføre myndigheten over QRA-flyene til sivile myndigheter.

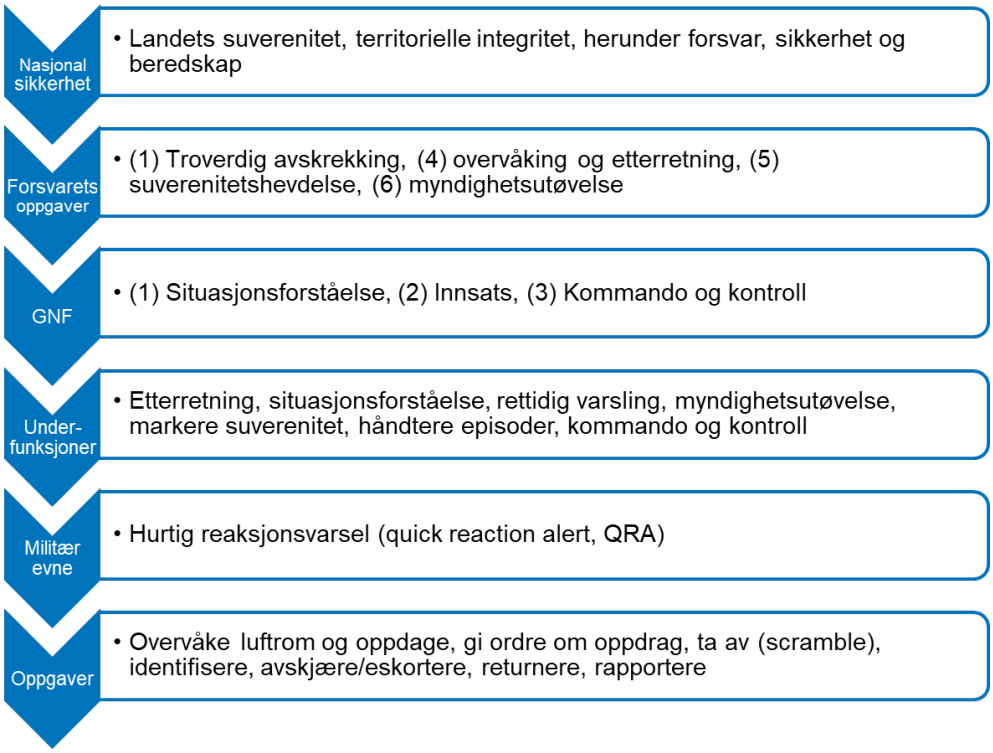
7. **Retur**. Etter utført oppdrag returnerer kampflyene til Evenes flystasjon.

8. **Rapportering**. Etter at hele operasjonen er fullført, sender Luftforsvaret en rapport til CAOC.

Den militære evnen QRA er avhengig av evnen til å utføre disse oppgavene. Det utgjør fortsettelsen av verdihierarkiet (se Figur 8.4).

Verdihierarkiet er så langt ikke knyttet direkte til bruk av IKT. Fremgangsmåten så langt kan derfor etter vårt syn være utgangspunkt for mange typer vurderinger knyttet til risiko og sikkerhet for Forsvarets operative evner og virksomhet som understøtter disse. I neste trinn identifiseres behov for IKT-kritiske evner for å løse oppgavene, i tråd med rammeverkets struktur.

[137] Forsvaret (2023b).
[138] Link er system for overføring av informasjon mellom kampfly og landbasert infrastruktur.




*Figur 8.4 Verdihierarkiet for den militære evnen hurtig reaksjonsvarsel (QRA). Fordi underfunksjonene er unntatt offentlighet, er disse ikke spesifisert i denne rapporten.*

### 8.3.3 Behov for IKT-kritiske evner for eksempelet hurtig reaksjonsvarsel

De påfølgende vurderinger knyttet til QRA er fiktive, kun foretatt av forfatterne for å illustrere det foreslåtte rammeverket. Som et praktisk grunnlag velger vi derfor å benytte et fiktivt, forenklet land og kun forenklede beskrivelser for bruk av rammeverket.

Den fiktive hendelsen som inntreffer i eksempelet, er at et ukjent luftfartøy, for eksempel et kampfly fra en annen nasjon, har kurs mot landets luftrom. Dette blir fanget opp av nasjonens luftovervåkingssensorer, og det gis deretter ordre om at det utenlandske kampflyet skal avskjæres fordi det vurderes å være på vei inn i nasjonalt luftrom.

La oss relatere vårt luftoperative eksempel til OODA-løkken (se figur 7.3), og skissere hvilke kommandosentre og elementer som inngår i beslutningsprosessene. Prosessen «observere» tilsvarer at en sensor, i vårt eksempel en radar, detekterer et objekt. Registrerte data prosesseres slik at objektet identifiseres som et ukjent fly, med en gitt posisjon, hastighet og retning. Videre skjer en prediksjon av flyets fremtidige bevegelser basert på hastighet og retning, det vil si at det antas at flyet vil nå nasjonens territorielle grense et gitt sted til en gitt tid. Denne informasjonen formidles deretter fra radaren til et taktisk luftkontrollsenter som er ansvarlig for neste prosess i beslutningssløyfen.

Prosessen «orientere» skjer i Taktisk luftkontrollsenter og innebærer å behandle mottatt varsel om innkommende utenlandsk kampfly og vurdere dette varselet opp mot annen informasjon og den situasjonsforståelsen som er tilgjengelig i kontrollsenteret. Annen informasjon kan være relevant informasjon fra andre sensorer på bakken, i luften eller på satellitter, både militære og sivile. Prosessen innebærer videre å utarbeide beslutningsgrunnlag for alternative luftoperative handlemåter basert på tilgjengelige kapabiliteter, det vil i dette tilfellet si egne kampfly på beredskap. Denne informasjonen formidles til Taktisk luftkommando, som kontakter Alliert luftkommando utland, og samtidig til kampflybasen.

Prosessen «beslutte» innebærer at det tas en beslutning om håndtering av episoden. I vårt tilfelle antar vi at beslutningen er å sende opp to kampfly for å avskjære det utenlandske kampflyet før det når nasjonens luftrom. Denne beslutningen tas i vårt eksempel av Alliert luftkommando i samråd med Taktisk luftkommando. Fellesoperativt hovedkvarter varsles også. Beslutningen om å sende opp to kampfly kommuniseres tilbake til Taktisk luftkontrollsenter og samtidig til kampflybasen.

Prosessen «handle» innebærer at to kampfly tar av fra kampflybasen tidsnok til å avskjære flyet før det når nasjonens luftterritorium, og innenfor responstiden på 15 minutter fra varselet kommer. I vårt tilfelle antar vi at avskjæring skjer, og at innkommende utenlandsk kampfly bøyer av og fortsetter i internasjonalt luftrom for deretter å returnere til eget luftrom. Hele tiden har de nasjonale kampflyene kontakt med Taktisk luftkontrollsenter. Handlingen avsluttes ved at kampflyene returnerer til basen. Til slutt rapporteres det i henhold til kommandolinjer til Taktisk luftkontrollsenter og videre til Taktisk luftkommando, Fellesoperativt hovedkvarter og Alliert luftkommando. Etter dette starter en ny runde i beslutningssløyfen, nemlig å observere og følge utenlandsk kampfly samt overvåking av all annen luftfart. Dette er en kontinuerlig pågående prosess.

Alle delene av OODA-løkken, både prosessene og informasjonsutvekslingen mellom prosessene, er avhengig av IKT-baserte funksjoner. Informasjonsutveksling mellom prosessene er avgjørende for å etablere et beslutningsgrunnlag, ta beslutninger og handle i en militær operasjon. Selve prosesseringen som foretas av radarsystemet krever også IKT. Prosessene i kontrollsenteret og kommandosentrene skjer ved hjelp av digitale systemer og programvare. Informasjonen mellom prosessene formidles ved hjelp av IKT-baserte funksjoner (eksempelvis dataoverføring på linksystemer og taleradio) på én eller flere IKT-plattformer (for eksempel sikker plattform) som er knyttet sammen av en kommunikasjonsinfrastruktur (fysisk og logisk infrastruktur).

Figur 8.5 illustrerer skjematisk hvilke lokasjoner som er involvert, og samhandlingen og relasjonene mellom dem, for dette generiske eksempelet. Denne type kartlegging er viktig for å forstå hvordan operasjonen foregår og for å kunne identifisere hvordan IKT brukes i operasjonen. Vi inkluderer implisitt både personell, teknologi og organisering for å utføre oppgavene i vår omtale av lokasjoner. De røde linjene i figuren er antatt informasjonsflyt. Vi kaller denne illustrasjonen samhandlings- og relasjonslaget. Luftoperasjonene ledes av en Taktisk luftkommando, samlokalisert med et Fellesoperativt hovedkvarter. Den taktiske luftkommandoen gir ordre innen luftoperasjoner til et Taktisk luftkontrollsenter. En slik ordre kan inneholde hvilke effekter som skal oppnås, prioritering av tilgjengelige luftstyrker, hvilke mål som skal tas ut og/eller forsvares samt retningslinjer for bruken av luftstyrker. Den taktiske luftkommandoen koordinerer også med

Alliert luftkommando i utlandet, samt at luftoperasjonene må ledes og koordineres med operasjoner i andre militære domener av Fellesoperativt hovedkvarter.

Taktisk luftkontrollsenter overvåker nasjonens og tilstøtende luftrom døgnkontinuerlig og utvikler et luftbilde basert på informasjon fra ulike sensorer og annen informasjon, for eksempel kontakt med sivile luftfartsmyndigheter. I tillegg utøver Taktisk luftkontrollsenter kontroll og varsling av hendelser i nasjonens luftterritorium, og hevder nasjonens suverenitet i luftrommet, det vil si innehar taktisk kontroll over kampflyene. I eksempelet inngår i tillegg kampfly og kampflybaser. For å kommunisere med kampflyene brukes i hovedsak taleradio- eller datalinktjenester. Både taleradio- og datalinktjenester inkluderer også en bakkeinfrastruktur.

Deretter identifiseres hvilke IKT-kritiske evner som inngår i QRA basert på QRA-oppgavene. For vårt QRA-eksempel er bruk av IKT en integrert del av alle oppgavene. Vi skiller mellom det å beskrive oppgavene og å identifisere IKT-kritiske evner fordi det, for andre eksempler enn QRA, ikke nødvendigvis er slik at IKT inngår i alle oppgaver. For vårt formål definerer vi følgende IKT-kritiske evner for QRA:

1. Evne til å overvåke luftrom og oppdage ukjente luftfartøy. Denne IKT-kritiske evnen stiller særlige krav med tanke på tilgjengelighetsaspektet ved informasjonssikkerhet.

2. Evne til å koordinere, ta beslutning og gi ordre om at to kampfly skal ta av.

3. Evne til å klargjøre kampfly og avgang.

4. Evne til å identifisere ukjent luftfartøy.

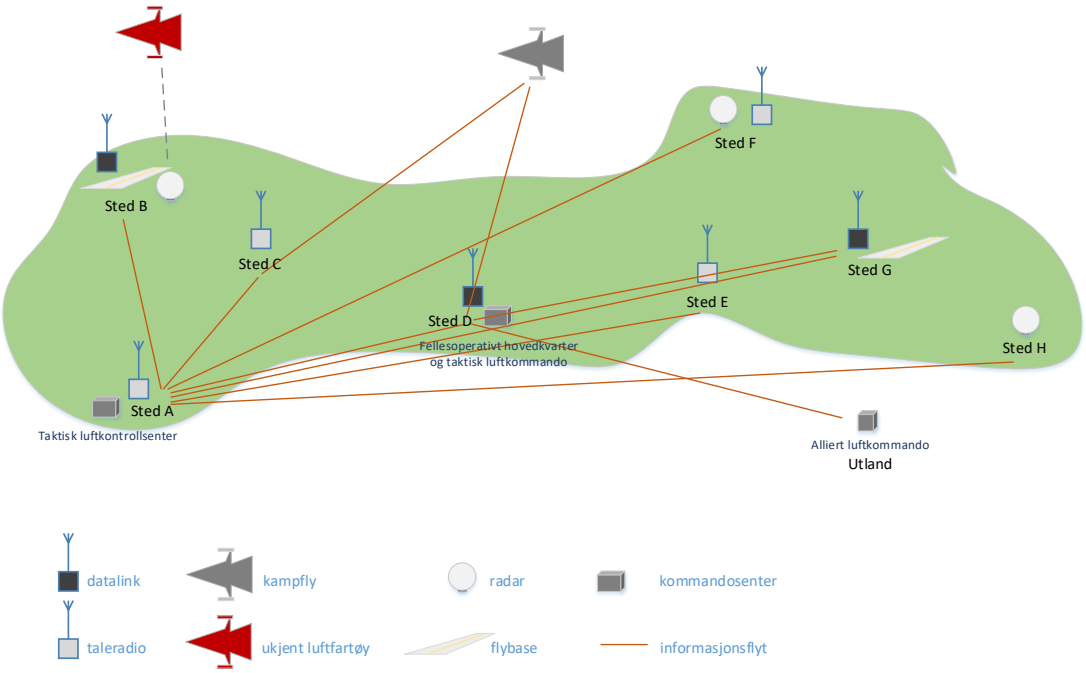
5. Evne til å avskjære, eventuelt eskortere fly.

6. Evne til retur.

7. Evne til rapportering.

På hvilket detaljeringsnivå og hvordan disse IKT-kritiske evnene formuleres, er avhengig av konteksten og formålet med analysen. Dette trinnet vil ofte innebære prøving og feiling i en iterativ prosess før en finner frem til den mest hensiktsmessige formuleringen av evner som egner seg for analysen.

Vi velger primært å konsentrere oss om evnen til å overvåke luftrom og oppdage ukjente luftfartøy videre i dette eksempelet. Dette er fordi formålet vårt er å illustrere systematikken, ikke utføre en nedbrytning av alle de IKT-kritiske evnene som inngår i QRA.




*Figur 8.5 Samhandlings- og relasjonslaget – det fiktive landet med de ulike lokasjonene og antatt informasjonsflyt mellom dem.*

### 8.3.4 IKT-baserte funksjoner for evnen til å overvåke luftrom og oppdage ukjente luftfartøy i eksempelet

IKT-applikasjoner og -tjenester gir i seg selv ikke operativ effekt. Det er hva disse benyttes til for å realisere konkrete evner som gir effekt. Dersom systemene ikke virker slik de skal, degraderes eller hindres operativ effekt. En viktig del av informasjonsinnhentingen, og grunnlaget for å vurdere risiko, er derfor å identifisere hvilke applikasjoner og plattformer som benyttes, og hva de benyttes til. For å beskrive hva IKT brukes til i en konkret kontekst identifiserer vi derfor hvilke IKT-baserte funksjoner som skal til for å løse oppdraget og kartlegger hvilke IKT-systemer som inngår i disse funksjonene.

For å illustrere hva vi mener med dette, ser vi på den første IKT-kritiske evnen i vårt eksempel – Evne til å overvåke luftrom og oppdage ukjente luftfartøy. Vi antar at følgende IKT-baserte funksjoner benyttes i evnen til å overvåke luftrom og oppdage ukjente luftfartøy:

1. Detektere, behandle og formidle data fra sensorer i radarkjeden til Taktisk luftkontrollsenter
    - Funksjon avhengig av datalink, K2-system A eller B, sikker plattform A, militær kommunikasjonsinfrastruktur

2. Etablere, presentere og formidle luftbilde fra Taktisk luftkontrollsenter til Taktisk luftkommando og Alliert luftkommando
    - Funksjon avhengig av datalink, K2-system A eller B, sikker plattform A, militær kommunikasjonsinfrastruktur

3. Kontakt med og innhenting av informasjon fra sivile luftfartsmyndigheter
    - Funksjon avhengig av internett, plattform U, sivil kommunikasjonsinfrastruktur

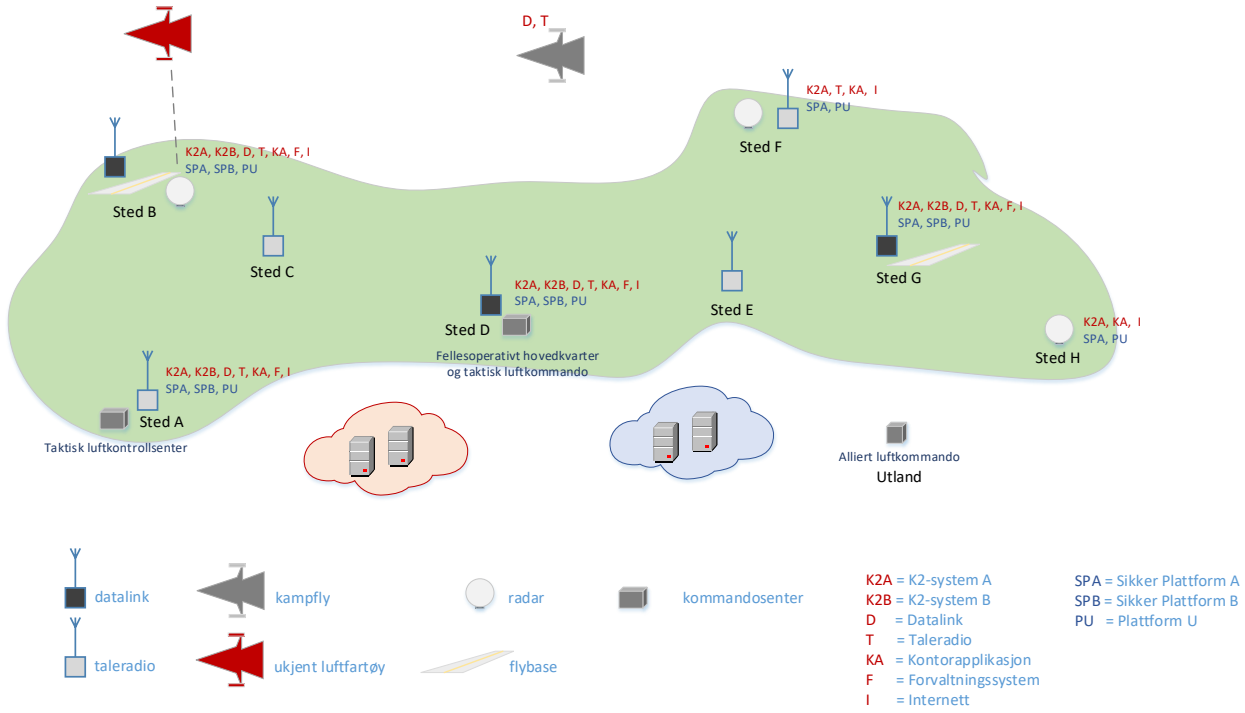
Da vi her kun ser på én av de IKT-kritiske evnene, vil ikke alle applikasjoner og tjenester som benyttes i operasjonen som helhet, fremkomme. Ved de ulike lokasjonene har brukerne en rekke applikasjoner og plattformtjenester tilgjengelig, herunder systemer for kommando og kontroll, datalink, taleradio, kontorapplikasjon, forvaltningssystem og internett. Disse applikasjonene er tilgjengelig på ulike plattformer, noen via internett på ugradert plattform og de andre applikasjonene på sikkerhetsgraderte plattformer.

Figur 8.6 gir en fiktiv skjematisk oversikt over de brukernære systemene, det vil si applikasjons- og plattformtjenestene som benyttes av brukerne ved de ulike lokasjonene i operasjonen samlet sett. Vi kaller dette applikasjons- og plattformlaget. En slik illustrasjon kan være et nyttig hjelpemiddel for å illustrere hvilke IKT-systemer og IKT-infrastruktur som brukes og ved hvilken lokasjon.

Av figuren fremkommer at tre plattformtjenester benyttes: ugradert plattform (PU) og sikre plattformer (SPA og SPB). Applikasjonene, det vil si de brukernære tjenestene, omfatter systemer for kommando og kontroll (K2A og K2B), datalinktjeneste (D), taleradio (T), kontorapplikasjon (KA), forvaltningssystem (F) og internett (I). Servere er også inkludert i figur 8.6 fordi applikasjoner, data og plattformer i mange tilfeller ligger på servere som ikke er samlokalisert med brukerne. Slike servere kan for eksempel være en forutsetning for tynnklientløsninger eller programvare og/eller databaser som er en del av et forvaltningssystem.

Militær og sivil kommunikasjonsinfrastruktur utgjør til sammen det nettverket som muliggjør overføring av data mellom lokasjoner. Datalink bakkestasjoner sørger for at det er mulig å overføre data mellom mobil plattform (kampfly) og stasjonære lokasjoner (kampflybase og/eller Taktisk kontrollsenter) via en *downlink*/*uplink* til en stasjonær kommunikasjonsinfrastruktur.

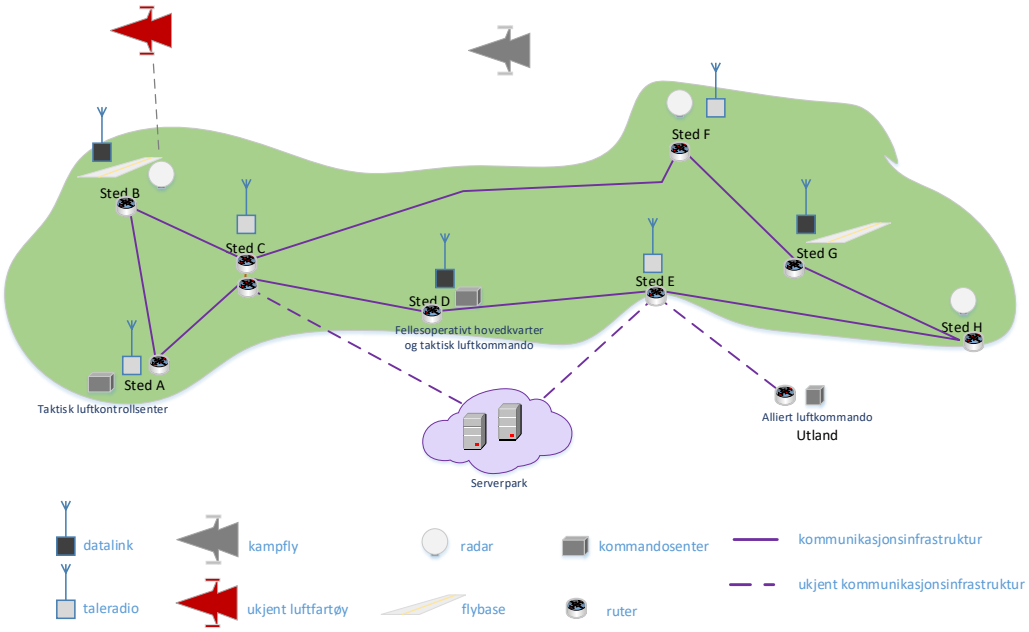
Det kan være mange måter å beskrive IKT på, men som forklart tidligere velger vi en lagdeling inspirert av DRP og C3-taksonomien (se Figur 7.7). For andre formål, kan det være mer formålstjenlig med en annen beskrivelse og systematisering av den IKT som brukes.



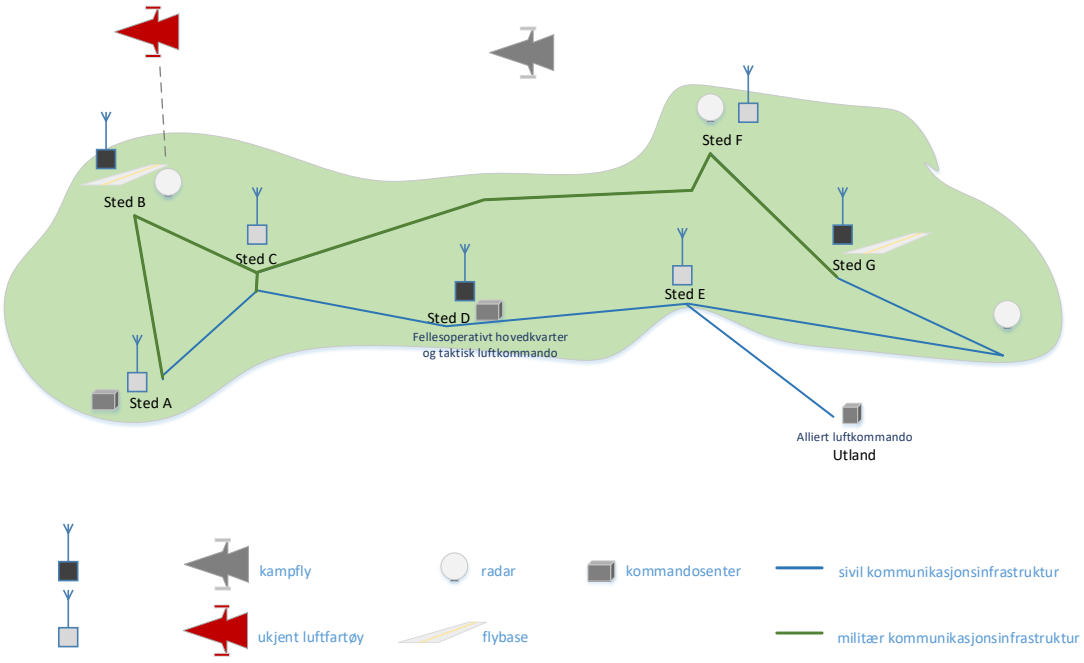

*Figur 8.6 Applikasjons- og plattformlaget – en oversikt over de applikasjoner (rød tekst) og plattformtjenester (blå tekst) som benyttes og dermed muliggjør den militære operasjonen.*

I vårt forenklede QRA-eksempel velger vi å beskrive deler av IKT som et infrastrukturlag. Infrastrukturlaget består av rutere, lagring, prosessering og brannmur (både maskinvare og programvare) som er del av en bakkebasert stasjonær kommunikasjonsinfrastruktur som sørger for å distribuere informasjon mellom lokasjoner (se Figur 8.7). I vårt eksempel antar vi at deler av denne infrastrukturen leveres av sivile tilbydere. Skillet mellom infrastrukturlaget og det underliggende kommunikasjonslaget er uklart. I tillegg kan det være slik at noe av infrastrukturen kan være delvis ukjent for Forsvaret, for eksempel fordi den avhenger av sivile tilbydere. For sivil infrastruktur er detaljert informasjon om hvordan infrastrukturen er konfigurert og oppfører seg, ikke nødvendigvis tilgjengelig for Forsvaret. Dette er illustrert med stiplede linjer i figur 8.7. Videre kan det være usikkerhet omkring hvor serverparker er plassert.

Kommunikasjonslaget sørger for overføring av data mellom applikasjoner og tjenester og består av høyhastighets transportnett (fiber og radiolinje), satellittkommunikasjon, radiosystemer og 4G (se Figur 8.8). Både taleradio og datalinktjenester er systemer som både har et brukergrensesnitt, men som samtidig har en underliggende funksjonalitet helt ned til kommunikasjonslaget.



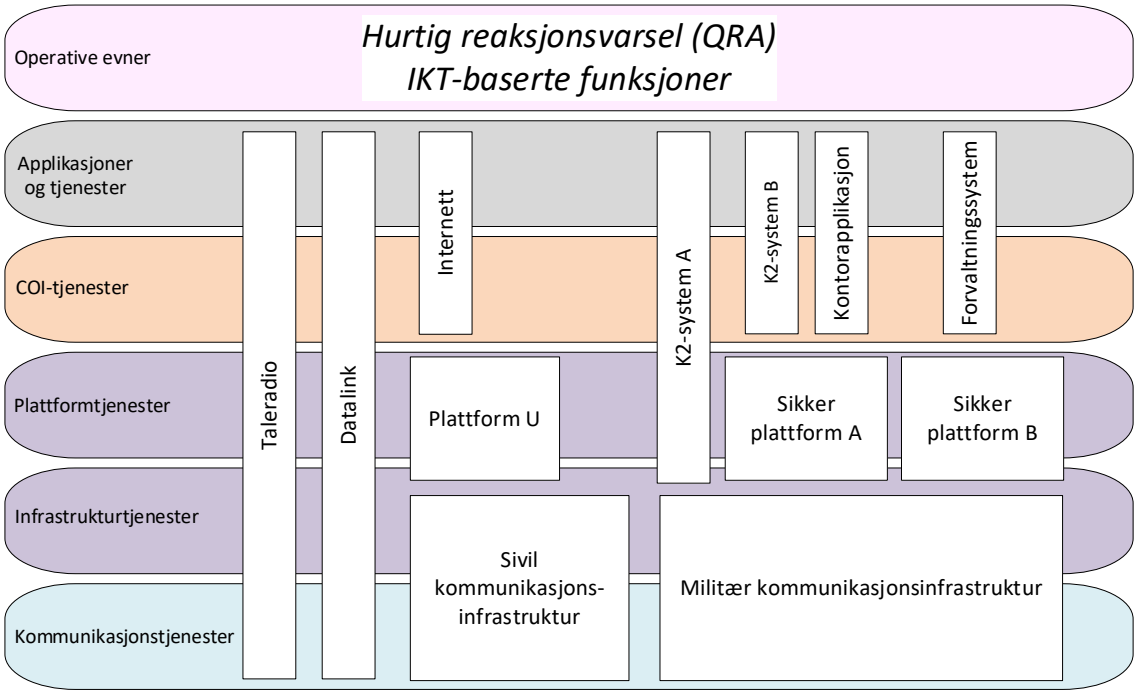

*Figur 8.7 Infrastrukturlaget – en oversikt over rutere (både maskinvare og programvare) som del av en bakkebasert stasjonær kommunikasjonsinfrastruktur samt noe infrastruktur som er ukjent.*




*Figur 8.8 Kommunikasjonslaget – en oversikt over den sivile og militære kommunikasjonsinfrastrukturen som muliggjør informasjonsflyt mellom lokasjonene.*

I Figur 8.9 systematiserer vi applikasjoner og tjenester, plattform-, infrastruktur- og kommunikasjonstjenester som er i bruk i vårt eksempel, i henhold til vår lagdelte inndeling inspirert av C3-taksonomien og DRP. Denne oversikten kombinert med informasjon og behov knyttet til bruk av IKT, gjør det mulig å beskrive det Carter et al. (2018) kaller «systemets funksjoner og arkitektur». For et reelt case ville dette, dersom det er hensiktsmessig, inkludert å innhente mer detaljert informasjon om hvordan IKT-systemene og -infrastrukturen er bygget opp. Dette krever relevant IKT-fagekspertise samt kunnskap om de aktuelle systemene. Derfor må personell som har ansvar for styring, drift, vedlikehold og sikkerhet for systemene, involveres.

Som del av denne detaljeringen, er det også viktig å kartlegge avhengigheter til eksterne innsatsfaktorer. Det kan særlig være ekstern sivil infrastruktur slik som strømforsyning og elektroniske kommunikasjonstjenester (ekom).




*Figur 8.9 Applikasjoner og tjenester, plattform-, infrastruktur- og kommunikasjonstjenester som benyttes i vårt forenklede QRA-eksempel, systematisert i henhold til C3-taksonomien.*

### 8.3.5 Uønskede hendelser

En viktig siste del av informasjonsfremkallingen er å identifisere uønskede hendelser med utgangspunkt i operasjonen og de IKT-baserte funksjonene som operasjonen er avhengig av. Dette er det siste punktet av informasjonsfremkallingen (se Figur 6.2). Uønskede hendelser er bortfall, degradering eller bevisste forstyrrelser av de IKT-kritiske evnene som realiserer den overordnede militære evnen, samt uautorisert tilgang til, tukling med eller tap av sensitiv informasjon som igjen kan skade militær evne direkte, indirekte eller i fremtidige operasjoner.

Tabell 8.1 skisserer eksempler på slike uønskede hendelser. De uønskede hendelsene kan benyttes i verdivurderingen for å identifisere og rangere skjermingsverdige verdier basert på en skadevurdering (se neste kapittel).

*Tabell 8.1 Eksempler på uønskede hendelser knyttet til operasjonen og IKT-baserte funksjoner for forenklet QRA-eksempel.*

| IKT-basert funksjon | Uønskede hendelser |
|---|---|
| Detektere, behandle og formidle data fra sensorer i radarkjeden til Taktisk luftkontrollsenter (TLKS) | – TLKS mottar ikke radardata<br>– TLKS mottar ukorrekte data<br>– Radar mister funksjonalitet for å detektere luftfartøyer<br>– Radar mister evne til å behandle data<br>– Radar mister evne til å sende data<br>– … |
| Etablere, presentere og formidle luftbilde fra Taktisk luftkontrollsenter til Taktisk luftkommando og Alliert luftkommando | – TLKS mister kommunikasjon med Taktisk luftkommando<br>– Taktisk luftkommando mister kommunikasjon med Alliert luftkommando<br>– TLKS sine K2-systemer for presentasjon og formidling av luftbilde virker ikke<br>– … |
| Kontakt med og innhenting av informasjon fra sivile luftfartsmyndigheter | – TLKS mister internettforbindelsen og dermed tilgang til informasjon fra sivile luftfartsmyndigheter<br>– Sivile luftfartsmyndigheters informasjon er ikke korrekt<br>– … |
| … | … |

## 8.4 Forsvarlig sikkerhetsnivå

Siste del av rammeverket er selve vurderingen av risiko og usikkerhet knyttet til risikoen, inkludert å kommunisere disse vurderingene til beslutningstakere. Formålet med en risikovurdering er å analysere risiko på IKT-systemnivå for å vurdere om IKT-sikkerhetsnivået er forsvarlig. Dersom et forsvarlig sikkerhetsnivå ikke er ivaretatt, må det anbefales alternative strategier og nødvendige IKT-sikkerhetstiltak. En samlet vurdering av risiko, usikkerhet og forsvarlig sikkerhetsnivå skal derfor gi et beslutningsgrunnlag til beslutningstakere knyttet til sikkerhetstiltak.

Gjennom informasjonsfremkallingen er det etablert innsikt i operasjonen og et funksjonelt hierarki, det vil si en utledning av IKT-baserte funksjoner og systeminnsikt for disse. Vi anbefaler at en vurdering av risiko tar utgangspunkt i slike IKT-baserte funksjoner og disses betydning for

de IKT-kritiske evnene som inngår i en militær evne realisert i en operativ kontekst. På den måten kan det skapes sammenheng og sporbarhet mellom den militære operative evnen og operasjonens formål og kravene til IKT-sikkerhet på teknisk nivå for å oppnå et forsvarlig sikkerhetsnivå.

Som presisert i presentasjonen av rammeverkets struktur i kapittel 8.1, kan risikovurderinger som grunnlag for å oppnå forsvarlig sikkerhetsnivå utføres på mange måter og med fordel gjennom en kombinasjon av ulike verktøy og metoder. Formålet med denne rapporten er å skissere et rammeverk, ikke foreta en reell vurdering av risiko og sikkerhet for én konkret militær evne. En detaljert beskrivelse av militær evne og Forsvarets avhengighet av IKT-systemer, ville raskt blitt sensitiv. Derfor har vi ikke gått inn i detaljer i denne siste delen av rammeverket som omhandler forsvarlig sikkerhetsnivå. I stedet har vi har valgt å vektlegge noen sentrale momenter som kan inngå i en risikovurdering. Vi refererer til QRA-eksempelet, men benytter det ikke spesifikt som i forrige del. Fremstillingen er ikke uttømmende.

I den videre inndelingen av risiko som den siste delen av rammeverket, har vi holdt oss til strukturen gitt i standarden NS 5832:2014 (se kapittel 4.2), med en verdivurdering, trusselvurdering, sårbarhetsvurdering og en samlet risikovurdering etterfulgt av risikoevaluering. I tillegg har vi hentet momenter fra NS 5814:2021.

### 8.4.1 Verdivurdering

Verdier som skal beskyttes, fremkommer på ulike nivåer. I kapittel 8.3.2 utledet vi et verdihierarki som knytter den militære evnen QRA opp til de overordnede verdiene nasjonale sikkerhetsinteresser (se Figur 8.4). De oppgavene som inngår i QRA, er igjen avhengig av IKT-kritiske evner og IKT-baserte funksjoner. Avslutningsvis i kapittel 8.3.4 etablerte vi en oversikt over Forsvarets bruk av IKT-systemer i vårt eksempel (se Figur 8.9). De underliggende verdiene som skal beskyttes, er derfor disse IKT-systemene samt den skjermingsverdige informasjonen som utveksles og foreligger på disse systemene.

Formålet med verdivurderingen er å identifisere, beskrive og rangere de underliggende verdiene (IKT-systemene) ut fra hvor viktige de er for operasjonen. Det bør også fremkomme hvilken sikkerhetsegenskap som er viktigst av henholdsvis tilgjengelighet, integritet og konfidensialitet, og hvilke sikkerhetskriterier som gjelder. Resultatet av verdivurderingen gir grunnlag for en prioritering av de mest relevante truslene og sårbarhetene.

### 8.4.2 Trusselvurdering

Formålet med trusselvurderingen er å identifisere mulige trusler, herunder sikkerhetstruende virksomhet, som kan skade verdiene. Det vil i dette tilfellet si de delene av Forsvarets IKT-virksomhet som muliggjør den militære evnen. Trusselvurderingen bør i tillegg til å spenne ut et mulighetsrom, også beskrive hvordan trusselscenarioer kan utspille seg, inkludert en vurdering av hvor mulige scenarioene er, det vil si en vurdering av sannsynligheter.

En såkalt morfologisk analyse kan være nyttig for å spenne ut utfallsrommet av tilsiktede uønskede handlinger som kan ramme IKT-virksomheten, og dermed Forsvarets bruk av IKT.

Farsund og Enemo (2018) har utført en slik analyse av mulige tilsiktede uønskede hendelser mot Forsvarets informasjonsinfrastruktur, som kan være et nyttig utgangspunkt.[139] Rapporten ser både på angrep utført i programvare (cyberdomenet) og fysiske angrep. Trusselscenarioer bør etableres ut fra en angripers perspektiv, det vil si intensjon, enkelhet, kostnader og forutsigbarhet med tanke på effekt. For eksempel kan et fysisk angrep på infrastruktur, eller påvirkning av de menneskelige prosessene rundt IKT-virksomheten, være enklere enn et angrep utført med programvare. Denne type vurderinger bør fremkomme i trusselvurderingen.

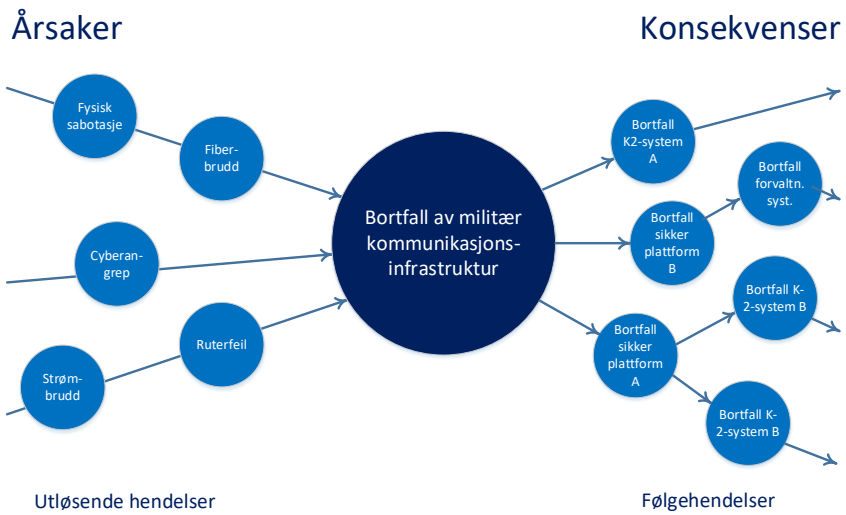
### 8.4.3 Sårbarhetsvurdering

Å vurdere sårbarheter krever tilstrekkelig innsikt i IKT-systemene, slik at sårbarheter kan ses i sammenheng med både fysiske og logiske trusselscenarioer. Dette er nært koblet til verdivurderingen. Dersom en morfologisk analyse benyttes for å identifisere realiserbare trusler, kan den morfologiske matrisen også benyttes som utgangspunkt for analyse av sårbarheter for programvare og maskinvare, menneskelige sårbarheter på de ulike komponentene samt fysiske sårbarheter.

Bruk av et sløyfediagram kan også være et nyttig hjelpemiddel for å analysere årsaks- og konsekvenskjeder av uønskede hendelser. Det gjelder både bortfall (tilgjengelighetsbrudd), uautorisert tilgang (konfidensialitetsbrudd) eller kompromittering (integritetsbrudd) for IKT-systemer og den informasjon som behandles på disse. Et generelt enkelt eksempel er vist i Figur 8.10.

I en sårbarhetsvurdering er det viktig å inkludere eksisterende barrierer i systemet som kan redusere sannsynligheten for at en uønsket hendelse skjer samt barrierer som bidrar til å redusere konsekvensene av den uønskede hendelsen. Barrierer bidrar til at årsakskjeder eller konsekvenser reduseres eller ikke manifesterer seg. Det kan være redundans i systemet som fører til at selv om én eller flere rutere ikke fungerer, så rutes datatrafikken andre veier i infrastrukturen. Det kan være at det eksisterer reservestrømløsninger som bidrar til at strømbortfall må vare lenge før det får negativ effekt for infrastrukturen.

[139] Farsund, B. H. & Enemo, G. (2018). *En morfologisk analyse av tilsiktede uønskede handlinger rettet mot Forsvarets informasjonsinfrastruktur.* FFI-rapport 18/00466. Kjeller: Forsvarets forskningsinstitutt.



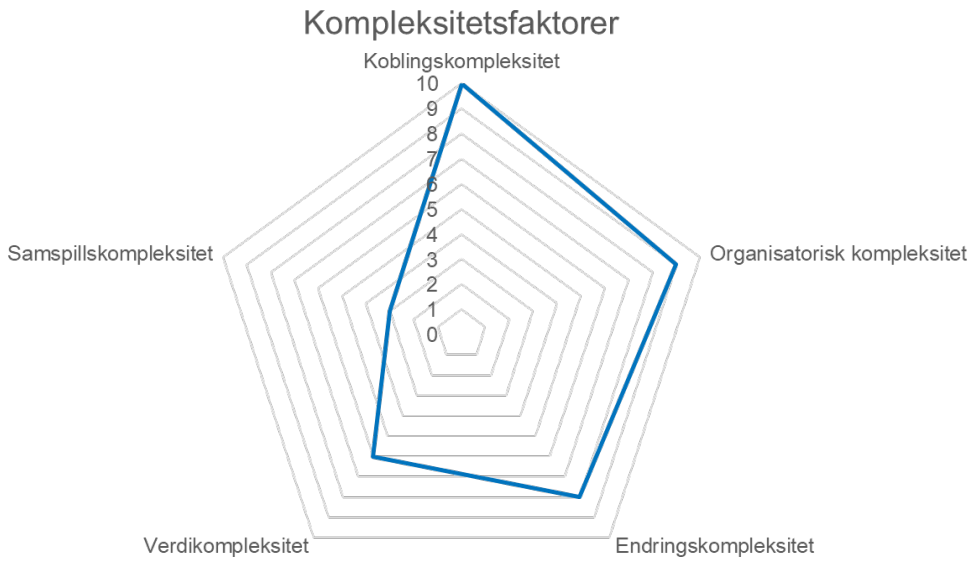

*Figur 8.10 Enkelt eksempel på sløyfediagram.*

### 8.4.4 Vurdering og kommunikasjon av usikkerhet som følge av kompleksitet for QRA-eksempelet

Som det fremgår av rammeverket (Figur 8.1) må vurdering av risiko, forsvarlig sikkerhet og usikkerhet ses i tett og dynamisk sammenheng. En viktig del av en helhetlig risikovurdering er å forstå Forsvarets avhengighet til integrerte IKT-baserte funksjoner og hvordan de inngår i militære evner og operasjoner. Både risikovurderingen og forsvarlig sikkerhetsnivå er beheftet med usikkerhet. Usikkerhet vil i økende grad være viktig når Forsvaret tar i bruk ny teknologi innenfor IKT-baserte systemer og infrastrukturer.

Ulike former for kompleksitet er en kilde til usikkerhet (se kapittel 5.2). Vi mener at usikkerhet må vurderes og kommuniseres eksplisitt til beslutningstakere som del av en helhetlig vurdering av risiko og forsvarlig sikkerhetsnivå. Ved å kommunisere usikkerhet eksplisitt kan det beskrives strukturelle uklarheter som ikke er mulig å komme til bunns i med rimelig innsats og tilgjengelig kunnskap. Denne type usikkerhet er det viktig at beslutningstakerne blir gjort oppmerksom på.

I kapittel 5.2 ble fem ulike kompleksitetsfaktorer forklart: koblingskompleksitet, organisatorisk kompleksitet, endringskompleksitet, verdikompleksitet og samspillskompleksitet. Et forslag for hvordan å kommunisere vurderinger av usikkerhet som følge av kompleksitet, er å benytte et spindelvevdiagram. I vårt eksempel (QRA) vil det kunne fremkomme slike usikkerheter knyttet til de ulike IKT-systemene og IKT-infrastrukturene. De fem kompleksitetsfaktorene gis en score for eksempel fra 0 til 10.




*Figur 8.11 Eksempel på illustrasjon av kompleksitetsfaktorer som kilder til usikkerhet.*

Følgende type argumentasjon kan være en del av en kompleksitetsvurdering for vårt QRA-eksempel (merk at vurderingene her er fiktive, og ikke knyttet til faktiske militære forhold):

- Koblingskompleksitet kan vurderes som høy. Bakgrunnen for det er at det er høy grad av tidskritikalitet og høy grad av avhengighet til at informasjon, for eksempel radarbilder, er tilgjengelig. Forsinkelser vil være kritisk for situasjonsforståelsen og kunne få alvorlige negative konsekvenser for gjennomføring av oppdraget.

- Organisatorisk kompleksitet kan vurderes som høy. Det er mange enheter som må samhandle og kommunisere, både internt i Forsvaret, med NATO og sivile myndigheter. For at denne samhandlingen skal kunne skje, er det avhengighet til både militær og sivil (for eksempel Telenors) infrastruktur og til en rekke samhandlingsverktøy (applikasjoner og tjenester).

- Endringskompleksiteten er potensielt ganske høy innen IKT-baserte funksjoner da det kan skje teknologiske endringer, for eksempel ved nye rutere, endringer i Telenors infrastruktur og oppdateringer av applikasjoner. Muligens introduseres nye algoritmer, og det kan skje strukturelle endringer i sammenhengen mellom systemer, eksempelvis ved å erstatte radiolinjer med fiber.

- Verdikompleksiteten er ikke så høy, da IKT-systemene (verdiene) skal støtte Forsvarets militære evner, ikke andre aktører.

- Samspillskompleksiteten kan vurderes som lav. Systemet er ganske homogent for Forsvarets del.

I Figur 8.11 har vi vist et fiktivt diagram for QRA-eksempelet. Dersom ulike alternative konsepter og innretninger av tekniske løsninger skal sammenlignes, kan slike figurer også illustrere interessante ulikheter, og understøtte anbefalinger og veivalg.

### 8.4.5 Risikovurdering og -evaluering

I QRA-eksempelet har vi introdusert forslag til vurderinger som vi mener kan inngå i en risiko-basert vurdering. En helhetlig beskrivelse av risiko er en samlet vurdering av verdiene, truslene og sårbarhetene fra de foregående delkapitlene. Følgende spørsmål bør adresseres:

- Hva er de viktigste IKT-baserte funksjonene?
- Hva er absolutte krav til disse funksjonene og dermed krav til IKT-systemene?
- Er forsvarlig sikkerhetsnivå i virksomheten oppnådd?
- Hvis ikke? Hvilke tiltak kan anbefales?
- Hvilke sårbarheter er det viktig å gjøre noe med?
- Er det behov for ytterligere vurderinger og analyser av risiko og usikkerhet innfor deler av virksomheten og dennes IKT-baserte funksjoner?

Risikoevaluering innebærer å utforme forslag til strategier for å oppnå og ivareta forsvarlig sikkerhetsnivå. Dette innebærer også å gjøre kost/nytte-vurderinger som ofte er krevende.

# 9 Oppsummering

Forsvaret er helt avhengig av IKT-baserte funksjoner for å lede og gjennomføre militære operasjoner, samhandle, etablere og dele oppdaterte situasjonsbilder. Dette gjelder både Forsvarets egne enheter, og samhandlingen og koordineringen med allierte styrker og sivile totalforsvarsaktører. IKT er også en integrert del av Forsvarets våpenplattformer og sensorer og også helt nødvendig for logistikk og administrative prosesser. IKT-baserte funksjoner inngår i stadig større grad som en svært viktig integrator i Forsvarets virksomhet og påvirker dermed alle former for risiko og sikkerhet i Forsvaret.

Formålet med dette forskningsarbeidet har vært å foreslå et rammeverk for risikobaserte vurderinger for Forsvarets bruk av IKT. Rammeverket skal kunne benyttes for å utarbeide et risikobasert beslutningsgrunnlag og anbefalinger for å sikre et forsvarlig sikkerhetsnivå for forsvarssektorens IKT-infrastruktur, IKT-systemer og informasjon. Rammeverket skal være egnet for Forsvarets virksomhet i fred, krise og krig, i nært samvirke med allierte nasjoner.

Begrepet forsvarlig sikkerhetsnivå er en rettslig standard som trekker opp rammene for hvilket handlingsrom Forsvaret har for etablering av sikkerhetstiltak. Virksomheten er gjennom virksomhetens leder, det vil si Forsvarssjefen, ansvarlig for at virksomheten innehar et forsvarlig sikkerhetsnivå.

Rammeverket har en klar top-down tilnærming, der verdien av ulike funksjoner, sikkerhet og risiko er knyttet til hva funksjonene brukes til og hvordan de bidrar til nasjonale sikkerhetsinteresser, i tråd med sikkerhetslovens systematikk. Imidlertid legges det også til grunn at detaljert kunnskap om forhold som militære funksjoner og innsikt i systemer og teknologier, er nødvendig, det vil si en bottom-up tilnærming. Gjennom rammeverket søkes det å strukturere og sette sammen svært mange former for informasjon og kunnskap, i hele spennet fra teknologi og teknologirealisering i systemer og infrastrukturer, til risikofaglig kunnskap og militær og sivil domeneforståelse.

Rammeverket er basert på erfaringer fra risiko- og sårbarhetsvurderinger i komplekse sivile og militære funksjoner, og legger særlig vekt på vår innsikt i nyere sikkerhets- og risikoforsking. Rammeverket vektlegger at en helhetlig tilnærming er nødvendig, for å unngå sub-optimalisering. Videre fremheves at kompleksitet og usikkerhet må analyseres og kommuniseres.

Rammeverket har tre deler, og i det følgende oppsummeres delene kort. Som et premiss etableres et verdihierarki for nasjonal sikkerhet for forsvarssektoren. Gjennom en informasjonsfremkalling etableres en operativ kontekst og kunnskap om operasjonens oppgaver og hvordan bruk av IKT inngår. I siste del av rammeverket er formålet å etablere et forsvarlig sikkerhetsnivå basert på en funksjons- og risikobasert vurdering.

I tråd med sikkerhetslovens bestemmelser skal de overordnede nasjonale sikkerhetsinteressene, de fem grunnleggende nasjonale funksjonene (GNF-ene) for forsvarssektoren og underfunksjonene som er definert av FD for hver av disse GNF-ene, ligge til grunn for å vurdere risiko for å

oppnå et forsvarlig sikkerhetsnivå. I tillegg har myndighetene gitt politiske føringer og besluttet hvilke oppgaver Forsvaret skal løse. Samlet utgjør dette et overordnet premiss i rammeverket. Vi har utviklet et verdihierarki for nasjonal sikkerhet for forsvarssektoren som kan benyttes som utgangspunkt for vurderinger av risiko og forsvarlig sikkerhet i sektoren, ikke kun begrenset til bruk av IKT.

For å vurdere risiko for Forsvarets bruk av IKT, er det nødvendig å sette bruken av IKT inn i en operativ kontekst. Det er den funksjonaliteten IKT utgjør for Forsvaret i ulike situasjoner som er viktig, det vil si hvilke operative evner som IKT-baserte funksjoner bidrar til, både direkte og indirekte. Det er bruken og avhengigheten av IKT-baserte funksjoner for operativ evne som er avgjørende for hvor viktig en IKT-funksjon er, og dermed også hvor viktig det er å sikre IKT-funksjonen, inkludert informasjonens konfidensialitet, tilgjengelighet og integritet. Sikkerhetskrav på IKT-systemnivå må derfor utledes ut fra hva Forsvaret bruker IKT til. Derfor har vi benyttet et konkret eksempel for å utvikle og illustrere tilnærmingen for å vurdere risiko og forsvarlig sikkerhetsnivå for Forsvarets bruk av IKT. Vi har valgt ett av Forsvarets oppdrag innen luftoperativ virksomhet i fredstid, nemlig «hurtig reaksjonsvarsel» (*quick reaction alert)* (QRA). Eksempelet er benyttet for å vise hvordan et oppdrag kan brytes ned i oppgaver. Videre identifiseres IKT-kritiske evner som igjen brytes ned i IKT-baserte funksjoner. Dette gjør det mulig å identifisere hvilke IKT-systemer, IKT-infrastruktur og informasjon som inngår i disse IKT-baserte funksjonene. Å innhente og systematisere informasjon om operativ kontekst utgjør andre trinn, informasjonsfremkalling, i rammeverket.

Den siste delen av rammeverket er den risikobaserte vurderingen knyttet til Forsvarets avhengighet og bruk av IKT-baserte funksjoner for å oppnå den ønskede militære evnen og utføre oppdrag. Usikkerhet, inkludert den usikkerhet som følger av kompleksitet, er særlig viktige utfordringer i utviklingen av risikovurderinger og forståelsen av forsvarlig sikkerhet, og må derfor inkluderes. Å vurdere risiko som grunnlag for å oppnå forsvarlig sikkerhetsnivå, kan utføres på mange måter og gjerne ved en kombinasjon av ulike verktøy og metoder. Vi anbefaler å bruke en kombinasjon av hensiktsmessige metoder og fremgangsmåter som er tilpasset formålet og problemstillingen og tenkesett som er i tråd med relevante standarder og veiledere. Vi mener en systemteoretisk tilnærming til risiko og sikkerhet kan være nyttig, og anbefaler å utforske dette i videre arbeid.

For å sikre et forsvarlig sikkerhetsnivå, er det gjennomgående behov for kontinuerlig kunnskapsutvikling og kunnskapsforvaltning innen ferdigheter, rammeverk, verktøy, metoder, med mer, tilpasset kontekst. Dette innebærer en evne til å utvikle strukturert systeminnsikt, det vil si utvikling av en hensiktsmessig form for systemforståelse av relevante systemer og infrastrukturer og anvendelsen av disse i operative kontekster. Dette omfatter til dels detaljert innsikt i teknologi- og samfunnsutviklingen, så vel som utvikling av hensiktsmessige risiko- og sikkerhetsfaglige metoder. Videre krever dette evne til å kunne utvikle, planlegge og ta beslutninger i gjennomføringen av aktiviteter i komplekse omgivelser i stadige endringer, omfattet av stor grad av usikkerhet og tvetydighet. Dette omfatter evne til å omsette strukturert systeminnsikt inn i en relevant aktivitetsinnsikt, og gjøre robuste vurderinger av risiko og legge grunnlaget for beslutninger om risikoaksept. Avslutningsvis er det viktig med evne til å kunne kommunisere risiko og risikoaksept knyttet til aktiviteter i komplekse omgivelser, særlig der risiko for

tvetydighet og faren sub-optimalisering er høy. Dette gjelder vertikalt så vel som horisontalt i og utenfor Forsvarets kjernevirksomhet.

# 10 Videre arbeid

For at rammeverket skal ha nytteverdi for strategisk styring av IKT-sikkerhet for Forsvarets bruk av IKT, bør rammeverket og bruken av det være «så enkelt som mulig, men samtidig så komplekst som nødvendig». For å sikre dette må det foreslåtte rammeverket testes for flere områder av IKT-virksomheten, ikke kun skisseres ved det enkle QRA-eksempelet som vi har benyttet.

I utviklingen av rammeverk har vi benyttet en luftoperativ evne som eksempel. For å teste og utvikle rammeverket videre, bør andre kontekster testes, og da gjerne kontekster som er vesensforskjellig fra luftoperativ virksomhet. To eksempler kunne være strategisk krisehåndtering ved sikkerhetspolitisk krise og væpnet konflikt og alliert mottak spesielt knyttet til logistikkbehov. I begge disse eksemplene vil Forsvarets og FDs tette samarbeid med sivile totalforsvarsaktører, inkludert private virksomheter, være meget sentral. Ved å dele inn Forsvarets virksomhet i ulike temaer, vil det etter hvert kunne opparbeides og dokumenteres en systematisk innsikt i behovet for IKT-kritiske funksjoner i ulike situasjoner av betydning for nasjonal sikkerhet, og dermed kan det være mulig også utvikle et mer helhetlig bilde av sikkerhetstilstanden for disse. Et eksempel på en slik inndeling kan være:

- Strategisk kriseledelse på politisk-strategisk nivå
- Militær-strategisk ledelse i kriser
- Ledelse på operasjonelt nivå
- Luft kommando og kontroll
- Sjø kommando og kontroll
- Taktisk og stridsteknisk ledelse av landstyrker
- Spesialstyrkeoperasjon
- Logistikk
- Alliert mottak og vertslandstøtte
- Sanitet
- IKT-infrastruktur-operasjon
- Administrative oppgaver (væpnet konflikt)
- Administrative oppgaver (fred)

# Forkortelser

| | |
|---|---|
| 5G | Femte generasjons mobilnett |
| DRP | Digital reguleringsplan |
| DSB | Direktoratet for samfunnssikkerhet og beredskap |
| C3 | Consultation, Command and Control |
| CAOC | Combined Air Operations Centre |
| Digdir | Digitaliseringsdirektoratet |
| DRP | Digital reguleringsplan |
| ekom | Elektronisk kommunikasjon |
| FD | Forsvarsdepartementet |
| FFI | Forsvarets forskningsinstitutt |
| FFOD | Forsvarets fellesoperative doktrine |
| FMA | Forsvarsmateriell |
| FSJ | Forsvarssjefen |
| FST | Forsvarsstaben |
| GNF | Grunnleggende nasjonal funksjon |
| IKT | Informasjons- og kommunikasjonsteknologi |
| ISO | International Organization for Standardization |
| JD | Justis- og beredskapsdepartementet |
| K2 | Kommando og kontroll |
| LTP | Langtidsplanen for forsvarssektoren |
| NAOC | National Air Operations Centre |
| NATO | North Atlantic Treaty Organisation |
| NIST | National Institute for Standards and Technology |
| NSM | Nasjonal sikkerhetsmyndighet |
| NS | Norsk Standard |
| OBBO | observere, bedømme, beslutte, ordre |
| OODA | Observe, Orient, Decide, Act |
| PACE | Primary, Alternate, Contingency, Emergency |
| PTO | personell, teknologi og organisasjon |
| QRA | Quick Reaction Alert |
| STPA-Sec | System-Theoretic Process Analysis for Security |

# Referanser


Aven, T. (2010). «On how to define, understand and describe risk». *Reliability Engineering and System Safety 95*, s. 623–631.

Aven, T. (2015). «Implications of black swans to the foundations and practice of risk assessment and management». *Reliability Engineering and Systems Safety 134*, s. 83–91.

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

Bergsjø, H., Windvik, R. & Øverlier, L. (2020). *Digital sikkerhet. En innføring*. Oslo: Universitetsforlaget.

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

Busmundrud, O., Maal, M., Kiran, J. H. & Endregard, M. (2015). *Tilnærminger til risiko-vurderinger for tilsiktede uønskede handlinger*. FFI-rapport 2015/00923. Kjeller: Forsvarets forskningsinstitutt.

Carter, B. T, Bakirtzis, G., Elks, C. R. & Fleming, C. H. (2018). "A systems approach for eliciting mission-centric security requirements." *IEEE*. IEEE Xplore Full-Text PDF [sist besøkt 13.07.22].

Cyberforsvaret (2023). *Cyberforsvarets koordineringsordre CCO 23-001*. Jørstadmoen, 9. januar 2023. (BEGRENSET)

Cyert, R. & March, J. G. (1992). *A behavioral theory of the firm*. Blackwell.

Das, T. K. & Teng, B. S. (1999). "Cognitive biases and strategic decision processes: An integrative perspective." *Journal of Management Studies 36*(6), s. 757–778.

Digitaliseringsdirektoratet. *Informasjonssikkerhet.* Informasjonssikkerhet - en forutsetning for å nå virksomhetens mål | Digdir [sist besøkt 11.07.22].

DSB (2011). *Veileder om Enhetlig ledelsessystem (ELS).* veileder-om-enhetlig-ledelsessystem-els.pdf (dsb.no) [sist besøkt 15.07.22].

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

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

Endregard, M. & Elstad, A.-K. (2021). «Beredskap i teori og praksis: Hvordan står det til?» I A. K. Larssen (Red.), *Beredskap og krisehåndtering – Utfordringer på sentralt, regionalt og lokalt nivå*. Oslo: Cappelen Damm Akademisk, s. 23–45.

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

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

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

Farsund, B. H., Thuv, Aa. & Hansen, B. J. (2022). *Hvordan håndtere IKT i Forsvarets langtidsplanlegging*. FFI-rapport 22/01569. Kjeller: Forsvarets forskningsinstitutt.

Farsund, B. H., Thuv, Aa. & Hansen, B. J. (2022). *Hvordan håndtere operativ IKT i Forsvarets langtidsplanlegging? – et innspill med testcaser*. FFI-rapport 22/01703. Kjeller: Forsvarets forskningsinstitutt. (BEGRENSET)

Forskrift 20. desember 2018 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften). Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften) - Lovdata.

Forsvaret (2019). *Forsvarets fellesoperative doktrine*.

Forsvaret (2021). *Forsvarets IKT-strategi*. Desember 2021.

Forsvaret (2023a). *Dette er QRA – Quick Reaction Alert*. Dette er QRA – Quick Reaction Alert - Forsvaret. [sist besøkt 09.01.23].

Forsvaret (2023b). *Digital reguleringsplan*. (BEGRENSET)

Forsvarsdepartementet (2019). *IKT-strategi for forsvarssektoren*. Godkjent av Forsvarsministeren 27. mars 2019. ikt-strategi-for-forsvarssektoren---hoveddokument.pdf (regjeringen.no).

Forsvarsdepartementet (2020). *Risikostyring IKT-sikkerhet i forsvarssektoren*. FDs ref. 2020/50797-1/FD II 4/EKHB. BEGRENSET.

Forsvarsdepartementet og Justis- og beredskapsdepartementet. (2018). *Støtte og samarbeid. En beskrivelse av totalforsvaret i dag.*

Forsvarsmateriell (januar 2021). Strategisk samarbeidspartner innen IKT-leveranser (fma.no)

Forsvarsmateriell (20. februar 2023). *MAST*. https://www.fma.no/anskaffelser/virksomhetsprogrammet-mast

Forsvarsstaben (2018). *Digitaliseringsstrategi for Forsvaret*. fileresult (forsvaret.no)

Forsvarsstaben (2019). *Forsvarets fellesoperative doktrine*. https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2631948/FFOD 2019 .pdf

Forsvarsstaben (2022). *IKT-styringsmodell for forsvarssektoren*. September 2022. Ugradert – kan deles eksternt med godkjenning fra informasjonseier. Skal ikke publiseres åpent.

Hollnagel, E., Paries, J., Woods, D.D & Wreathall J. (2011). *Resilience engineering in practice: A guidebook*. Farnham, UK: Ashgate.

Jacobsen, D. I. & Thorsvik, J. (2005). *Hvordan organisasjoner fungerer - Innføring i organisasjon og ledelse*. Fagbokforlaget Vigmostad og Bjørke.

Jasanoff, S. (2003). "Technologies of humility: Citizen participation in governing science", *Minerva* 41, s. 223–244.

Jasanoff, S. (2007). "Technologies of humility". *Nature 450:*33.

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

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

Leveson, N.G. (2011). *Engineering a Safer World. Systems Thinking Applied to Safety*. MIT Press.

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

Lysne, O. (2020). *Risikostyring i digitale verdikjeder*. Rapport fra en arbeidsgruppe ledet av professor Olav Lysne. Direktoratet for samfunnssikkerhet og beredskap.

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

Nasjonal sikkerhetsmyndighet (ingen dato). *Veileder i sikkerhetsstyring*. Versjon 1. Om denne veilederen - Nasjonal sikkerhetsmyndighet (nsm.no).

Nasjonal sikkerhetsmyndighet (2020). *NSMs Grunnprinsipper for IKT-sikkerhet*. Versjon 2.0. nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf [sist besøkt 05.12.22].

Nasjonal sikkerhetsmyndighet (30.09.22). *Oversikt over innmeldte grunnleggende nasjonale funksjoner.* Oversikt over innmeldte grunnleggende nasjonale funksjoner - Nasjonal sikkerhetsmyndighet (nsm.no) [sist besøkt 08.12.22].

Nasjonal sikkerhetsmyndighet (2023). *Sikkerhetsfaglig råd. Et motstandsdyktig Norge*. Sikkerhetsfaglig råd - Et motstandsdyktig Norge - Nasjonal sikkerhetsmyndighet (nsm.no).

National Institute of Standards and Technology (2017). *Framework for Cyber-Physical Systems. Volume 1, Overview*. Cyber-Physical Systems Public Working Group, Smart Grid and Cyber-Physical Systems Program Office Engineering Laboratory. https://doi.org/10.6028/NIST.SP.1500-201.

NATO (2021). *C3 Taxonomy baseline 5.0.* Consultation, Command and Control Board (C3B).

NATO Standardization Office (2020). *AJP-3.20. Allied Joint Doctrine for Cyberspace Operations*. Ed. A Version 1, January 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf [sist besøkt 14.04.23].

NIST (ingen dato). *Cybersecurity*. Cybersecurity | NIST [sist besøkt 19.01.23].

Njå, O., Sommer, M., Rake, E. L. & Braut, G. S. (2020). *Samfunnssikkerhet. Analyse, styring og evaluering*. Oslo: Universitetsforlaget.

NOU 2016: 19. *Samhandling for sikkerhet.* NOU 2016: 19 - regjeringen.no.

Perrow, C. (1999). *Normal Accidents: living with high-risk technologies*, New Jersey: Princeton University Press

Prop. 1 S (2021–2022). *For budsjettåret 2022*. Oslo: Justis- og beredskapsdepartementet. Prop. 1 S (2021–2022) - regjeringen.no.

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

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

Prop. 151 S (2015–2016). *Kampkraft og bærekraft. Langtidsplan for forsvarssektoren*. Oslo: Forsvarsdepartementet.

Prop. 153 L (2016–2017). *Lov om nasjonal sikkerhet (sikkerhetsloven)*. Oslo: Forsvarsdepartementet.

Richards, C. (2020). «Boyd's OODA loop». *Necesse 5*, nr 1.

Simon, H. A. (1964). "On the concept of Organizational Goal." *Administrative Science Quarterly 9*(1), s. 1–22.

Society for Risk Analysis (2018). *Society for Risk Analysis Glossary*. The Risk Analysis Glossary from the Society for Risk Analysis - Society for Risk Analysis (sra.org) [sist besøkt 07.07.22].

Språkrådet. *Samfunnskritisk sikkerhet*. Samfunnskritisk sikkerhet (sprakradet.no) [sist besøkt 07.07.22].

Standard Norge (2009). *Risikostyring Terminologi.* SN-ISO Guide 73:2009.

Standard Norge (2012). *Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Terminologi*. NS 5830:2012.

Standard Norge (2014). *Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse*. NS 5832:2014.

Standard Norge (2018a). *Risikostyring. Retningslinjer*. NS-ISO 31000: 2018.

Standard Norge (2018b). *Informasjonsteknologi. Sikringsteknikker: Risikostyring for informasjonssikkerhet*. NS-ISO/IEC 27005:2018.

Standard Norge (2019). *Risikostyring – Metoder for risikovurdering (Risk management – Risk assessment techniques)*. NS-IEC 31010:2019.

Standard Norge (2020) *Informasjonsteknologi. Sikringsteknikker. Ledelsessystemer for informasjonssikkerhet. Oversikt og terminologi*. NS-EN ISO/IEC 27000:2020.

Standard Norge (2021). *Krav til risikovurderinger*. NS 5814:2021.

Store norske leksikon. *Cyberdomenet*. cyberdomenet – Store norske leksikon (snl.no) [sist besøkt 08.07.22].

Store norske leksikon. *Informasjons- og kommunikasjonsteknologi*. informasjons- og kommunikasjonsteknologi – Store norske leksikon (snl.no) [sist besøkt 11.03.22].

Store norske leksikon. *Infrastruktur*. infrastruktur – Store norske leksikon (snl.no) [sist besøkt 05.12.22].

Store norske leksikon. *Sikkerhet*. sikkerhet – Store norske leksikon (snl.no) [sist besøkt 07.07.22].

Store norske leksikon. *Sikkerhet- sikkerhetsstyring*. sikkerhet – risikostyring – Store norske leksikon (snl.no) [sist besøkt 07.07.22].

Store norske leksikon. *System*. system – Store norske leksikon (snl.no) [sist besøkt 08.07.22].

Time, J. K. (2022). *Advarer mot vitenskapens overmot, intervju med Sheila Jaasanoff*, Morgenbladet nr 14.

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

Weinberg, G. M. (1975). *An Introduction to General Systems Thinking*. New York, NY: John Wiley & Sons.

World Economic Forum. *Fourth Industrial Revolution.* Fourth Industrial Revolution | World Economic Forum (weforum.org) [sist besøkt 15.07.22].

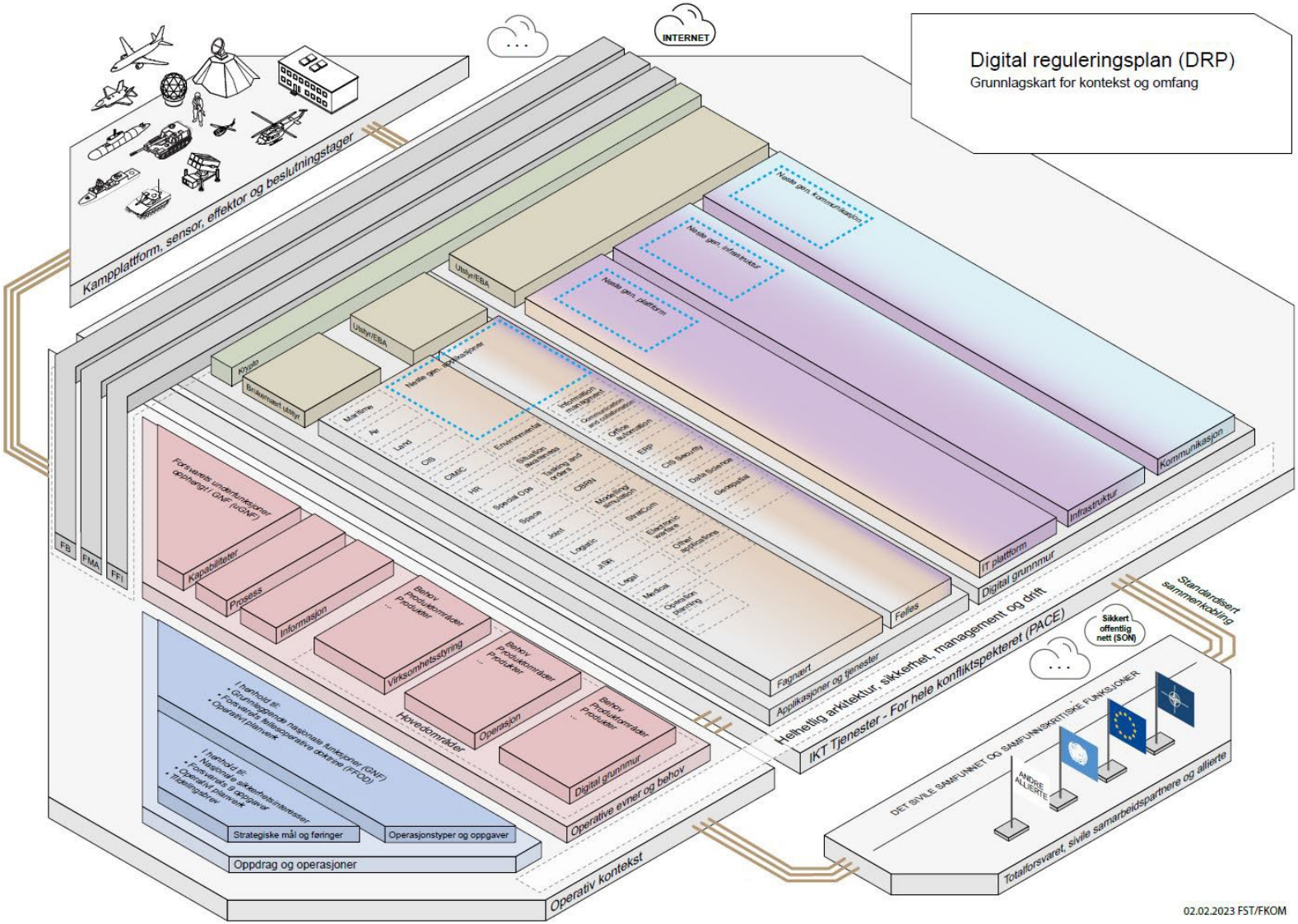
Young, W. & Leveson, N. (2013). *Systems thinking for safety and security*. In Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13). ACM, New York, NY, USA, s. 1–8.

# Vedlegg

# A Digital reguleringsplan – grunnlagskart for kontekst og omfang

Formålet med digital reguleringsplan (DRP) for forsvarssektorens IKT-virksomhet er å angi retning og regulere forsvarssektorens IKT. DRP setter rammer for utvikling, forvaltning og drift av IKT. DRPs grunnlagskart for kontekst og omfang fremstiller helheten i IKT-virksomheten og øvrig virksomhet i en lagvis platemodell. Kartet består av fire koblede hovedplater, henholdsvis «operativ kontekst og behov», «kampplattform, sensor, effektor og beslutningstager», «totalforsvaret og allierte» og «IKT-tjenester – for hele konfliktspekteret (PACE )». Denne siste platen viser applikasjons- og teknologiarkitekturen, og består av en digital grunnmur, applikasjoner og tjenester samt tilhørende utstyr.

*Figur A.1 Neste side: Grunnlagskartet for kontekst og omfang fra Digital reguleringsplan (DRP) (gjengitt med tillatelse fra Forsvaret (2023).*


Digital reguleringsplan (DRP)
Grunnlagskart for kontekst og omfang
INTERNET
Kampplattform, sensor, effektor og beslutningstager
Kryptо
Brukernært utstyr
Utstyr/EBA
Utstyr/EBA
Nestе gen. applikasjoner
Nestе gen. plattform
Nestе gen. infrastruktur
Nestе gen. kommunikasjon
Maritime
Air
Land
CIS
CIMIC
HR
Environmental
Special Ops
Space
Joint
Logistic
JISR
Legal
Medical
Operative planning
Situation awareness
Tasking and Orders
CBRN
Modelling simulation
StratCom
Electronic warfare
Cyber applications
Information management
Communication and collaboration
Office automation
ERP
CIS Security
Data Science
Geospatial
Fagnært
Felles
Applikasjoner og tjenester
IT plattform
Infrastruktur
Kommunikasjon
Digital grunnmur
FB
FMA
FFI
Forsvarets underfunksjoner opphørt i GNF (UOOF)
Kapabiliteter
Prosess
Informasjon
Behov Produktområder Produkter
Virksomhetsstyring
Behov Produktområder Produkter
Operasjon
Behov Produktområder Produkter
Digital grunnmur
Hovedområder
Operative evner og behov
I hht til:
• Grunnleggende nasjonale funksjoner (GNF)
• Forsvarets tilleggsoperative oppgaver (FFOO)
• Operativt planverk
I hht til:
• Nasjonale sikkerhetsinteresser
• Forsvarets oppgaver
• Operativt planverk
• Tilleggsoppgaver
Strategiske mål og føringer
Operasjonstyper og oppgaver
Oppdrag og operasjoner
Operativ kontekst
Helhetlig arkitektur, sikkerhet, management og drift
IKT Tjenester - For hele konfliktspekteret (PACE)
Sikkert offentlig nett (SON)
Standardisert sammenkobling
DET SIVILE SAMFUNNET OG SAMFUNNSKRITTISKE FUNKSJONER
ANDRE ALLIERTE
Totalforsvaret, sivile samarbeidspartnere og allierte
02.02.2023 FST/FKOM

## Om FFI

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

## FFIs formål

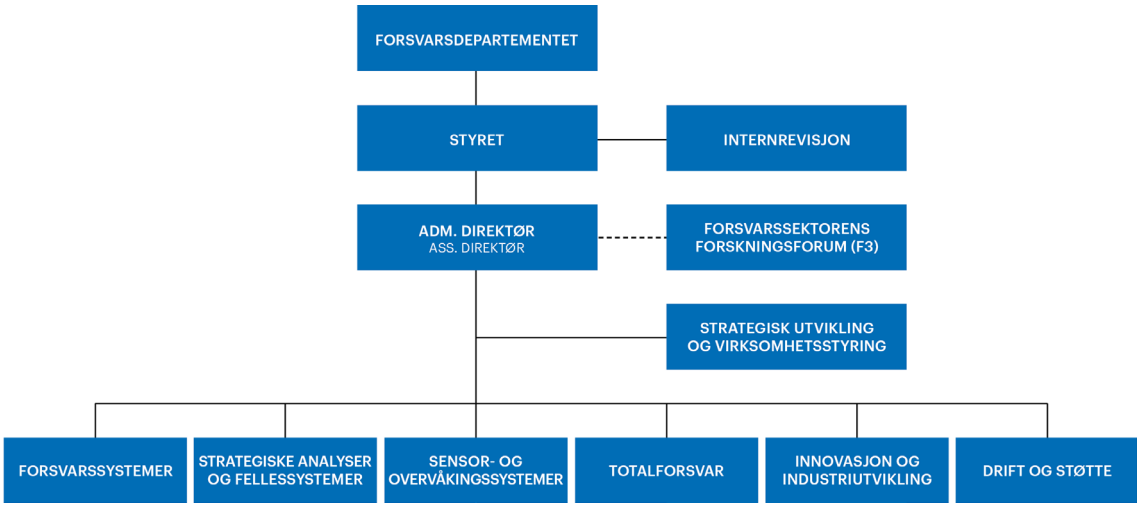
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som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