STORTINGET

Innst. 259 S

(2022–2023)

Innstilling til Stortinget
fra kontroll- og konstitusjonskomiteen

Dokument 3:3 (2022–2023)

Innstilling fra kontroll- og konstitusjonskomiteen om Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner

Til Stortinget

1. Sammendrag

1.1 Innledning

Forsvarets operative evne avhenger av effektiv kommando og kontroll og evne til å samhandle på tvers av enheter i Forsvaret og med NATO og allierte. Kommando og kontroll er det militære begrepet for planlegging og ledelse av operasjoner. Forsvarets operasjoner deles inn i daglige operasjoner, operasjoner ved nasjonale kriser og operasjoner ved væpnet konflikt (krig).

Evnen til samhandling i operasjoner avhenger av informasjonssystemer. Informasjonssystemer til bruk i Forsvarets operasjoner kalles gjerne kommando- og kontrollinformasjonssystemer. For at disse systemene skal virke effektivt, må de være interoperable. Det vil si at systemene må kunne samvirke og fungere med hverandre for å levere informasjon og tjenester til, og ta imot informasjon og tjenester fra, andre systemer. Dette avhenger også av kommunikasjonsinfrastrukturen som gjør det mulig å overføre data mellom systemene. Forsvarets kommunikasjonsinfrastruktur (FKI) består av kjernenett, aksessnett, radionett og mobile og deployerbare kommunikasjonsløsninger.

Forsvarets informasjonssystemer og kommunikasjonsinfrastruktur (IKT) må beskyttes mot sikkerhetstruende virksomhet. Det vil si at de må beskyttes mot tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. Slike handlinger kan for eksempel være sabotasje- eller terroraksjoner eller spionasje fra en fremmed stat.

Forsvarsdepartementet har ansvar for utforming og iverksetting av norsk sikkerhets- og forsvarspolitikk og er ansvarlig for overordnet styring og kontroll av underlagte etaters virksomhet. Av departementets fire underlagte etater inngår Forsvaret og Forsvarsmateriell i denne undersøkelsen. Etterretningstjenesten og Forsvarets spesialstyrker er ikke omfattet av undersøkelsen.

Forsvarets hovedoppgave er å ivareta Norges sikkerhet mot eksterne trusler, anslag og angrep. Forsvarets hovedleveranse er operativ evne. Forsvaret er eier og bruker av informasjonssystemene som omtales i undersøkelsen. Forsvarsmateriell skal gjennom materiellanskaffelser og materiellforvaltning bidra til utvikling av Forsvarets operative evne. Dette inkluderer anskaffelser og forvaltning av informasjonssystemer til bruk i Forsvaret.

Undersøkelsen har blant annet tatt utgangspunkt i følgende vedtak og forutsetninger fra Stortinget:

- Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) av 20. mars 1998.
- Lov om nasjonal sikkerhet (sikkerhetsloven) av 1. januar 2019.
- Innst. 103 L (2017–2018) fra utenriks- og forsvarskomiteen om Lov om nasjonal sikkerhet (sikkerhetsloven), jf. Prop. 153 L (2016–2017).
- Innst. 62 S (2016–2017) fra utenriks- og forsvarskomiteen om Kampkraft og bærekraft, jf. Prop. 151 S (2015–2016).
- Innst. 7 S om Statsbudsjettet for årene 2017, 2018, 2019 og 2020, jf. årlige Prop. 1 S for Forsvarsdepartementet.

Målet med undersøkelsen har vært å vurdere om Forsvarets kommando- og kontrollinformasjonssystemer understøtter Forsvarets operative evne gjennom effektiv og sikker kommunikasjon og informasjonsutveksling i operasjoner, og om styringen av IKT-området i forsvarssektoren har lagt til rette for effektive og sikre systemer.

Undersøkelsen omfatter perioden 2017–2020, men det er i noen tilfeller vist til forhold som ligger både før og etter undersøkelsesperioden i tid.

Rapporten ble forelagt Forsvarsdepartementet ved brev av 22. november 2021. Departementet har i brev av 17. desember 2021 gitt kommentarer til rapporten. Kommentarene er i hovedsak innarbeidet i rapporten og i dette dokumentet. Rapporten, riksrevisorkollegiets oversendelsesbrev til departementet av 16. juni 2022 og statsrådens svar av 8. juli 2022 følger som vedlegg til Riksrevisjonens dokument.

1.2 Konklusjoner

- Mangler i samvirket mellom Forsvarets kommando- og kontrollinformasjonssystemer kan påvirke Forsvarets operative evne.
  - Kommando- og kontrollinformasjonssystemer med ulik teknologi påvirker mulighetene for samhandling.
  - Ulike sikkerhetsdomener påvirker informasjonsutvekslingen mellom systemer.
  - Mangler ved taktisk datalink reduserer mulighetene for utveksling av data.
- Sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer gir risiko for svekket operativ evne.
  - Mangler i oversikt og dokumentasjon på IKT-området påvirker muligheten for ivaretakelsen av sikkerheten i informasjonssystemene.
  - Forsvaret har skjermingsverdige informasjonssystemer som ikke tilfredsstiller sikkerhetslovens krav.
  - Forsvaret har mangler i evnen til å oppdage og stanse digitale angrep.
  - Svakheter i sikkerhetsstyringen forsterker utfordringene.
- Forsvarsdepartementet har over tid ikke greid å realisere effektive og sikre informasjonssystemer som understøtter Forsvarets operative evne.
  - Svak styring har medvirket til utfordringene på IKT-området og svekket verdien av investeringer.
  - Overlappende og uklare ansvarsforhold mellom etatene i forsvarssektoren har påvirket gjennomføringsevnen på IKT-området.
  - Mangel på kompetanse har medvirket til at forsvarssektoren ikke har klart å løse mange av utfordringene på IKT-området.
  - Det er vesentlig risiko knyttet til den pågående IKT-satsingen i Mime og MAST.

1.3 Utdyping av konklusjoner

Ved behandlingen av langtidsplan for Forsvaret for perioden 2017–2020 sluttet Stortinget seg til at Forsvaret må ha evne til å lede og gjennomføre operasjoner gjennom et godt kommando- og kontrollapparat, og at dette krever klare styringslinjer, sikre og effektive kommunikasjonsløsninger og tilpasset infrastruktur. Det skulle videre utvikles en IKT-infrastruktur som gir Forsvaret nødvendig evne til å lede og samvirke i fellesoperasjoner.

Undersøkelsen viser at det er mangler ved Forsvarets kommando- og kontrollinformasjonssystemer både når det gjelder samvirke og sikkerhet. Riksrevisjonen mener at dette er svært alvorlig.

1.3.1 Mangler i samvirket mellom Forsvarets kommando- og kontrollinformasjonssystemer kan påvirke Forsvarets operative evne

Stortinget har forutsatt at investeringer i IKT vil bidra til at Forsvaret får mer effektiv informasjonsutveksling, felles situasjonsforståelse og økt tempo og presisjon i kommandokjeden. Det vil gi økt operativ evne å ha IKT-systemer som samvirker nasjonalt og med NATO og allierte.

Forsvarets operative evne avhenger av muligheten til samhandling i operasjoner, på tvers av enheter i Forsvaret, i kommandolinjen nasjonalt og med NATO og allierte. Slik fellesoperativ samhandling avhenger av kommando- og kontrollinformasjonssystemer som samvirker effektivt. Det innebærer at systemene må være interoperable, slik at de kan levere informasjon til, og ta imot informasjon fra, andre systemer.

Undersøkelsen viser mangler i samvirket mellom Forsvarets kommando- og kontrollinformasjonssystemer. Forsvaret har ikke utfordringer med å løse oppdraget i daglige operasjoner, men manglene gir risiko for redusert effektivitet og kan få betydning ved økt konfliktnivå dersom tid er av avgjørende betydning. Riksrevisjonen kritiserer dette. Kritikken er utdypet i Riksrevisjonens sikkerhetsgraderte rapport.

1.3.1.1 Kommando- og kontrollinformasjonssystemer med ulik teknologi påvirker mulighetene for samhandling

Undersøkelsen viser at Forsvaret har et høyt antall kommando- og kontrollinformasjonssystemer med ulike tekniske løsninger, og at dette bidrar til å gjøre samvirke mellom systemene vanskelig. Mengden av

systemer medfører også at det går ekstra ressurser til forvaltning og drift av systemene.

Det har lenge vært et mål å redusere antall informasjonssystemer i forsvarsektoren gjennom såkalt variantbegrensing, men Forsvaret har ikke i tilstrekkelig grad lyktes med dette. Årsakene er oppgitt å være at systemer har unike funksjoner som gjør at de ikke kan fjernes uten erstatning, og at enkelte fagmiljø ønsker å beholde eksisterende systemer. Forsvaret og Forsvarsmateriell påpeker at det er behov for en sterkere strategisk vektlegging knyttet til utfasing av informasjonssystemer. Det er etter Riksrevisjonens vurdering sterkt kritikkverdig at Forsvaret i liten grad har greid å begrense antall systemer, når dette i lang tid har vært et mål.

Forsvaret har de senere årene anskaffet mye nytt materiell, og det er planlagt med omfattende materiellinvesteringer i både nåværende- og kommende langtidsplanperioder. Nye våpenplattformer, som fly, båter og kjøretøy, leveres ofte med innebygde informasjonssystemer. Enkelte av disse systemene er ikke interoperable med Forsvarets eksisterende informasjonssystemer. Dette kan føre til begrensinger i utnyttelsen av potensialet materiellet skulle gitt. Riksrevisjonen merker seg at sjef Luftforsvaret mener at for å få full operativ utnyttelse av de nye kampflyene må kommando- og kontrollinformasjonssystemene som benyttes i flyene, videreutvikles.

1.3.1.2 Ulike sikkerhetsdomener påvirker informasjonsutvekslingen mellom systemer

Forsvaret benytter kommando- og kontrollinformasjonssystemer på ulike sikkerhetsdomener. Dette påvirker informasjonsutvekslingen mellom systemene.

Stortinget har vektlagt utvikling av IKT som støtter interoperabilitet og samvirke med NATO. Dette er viktig fordi mangler i interoperabilitet kan påvirke Forsvarets evne til å gjennomføre fellesoperasjoner og kommunikasjon med NATO og allierte.

1.3.1.3 Mangler ved taktisk datalink reduserer mulighetene for utveksling av data

Taktisk datalink er en sentral komponent i Forsvarets kommunikasjonsinfrastruktur og brukes til å utveksle taktiske data, inkludert situasjonsbilde, sensor- og måldatainformasjon, mellom to eller flere enheter i nær sanntid. Mangler ved taktisk datalink reduserer mulighetene for utveksling av data.

Det er flere planlagte og pågående prosjekter knyttet til oppgradering av taktisk datalink. Undersøkelsen viser at det er forsinkelser og risiko for mangelfull koordinering mellom disse prosjektene, og at det er risiko for at kapasitet ikke vil kunne utnyttes fullt ut.

1.3.2 Sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer gir risiko for svekket operativ evne

De nasjonale etterretnings- og sikkerhetstjenestene viser til at stadig mer av etterretningsaktiviteten mot Norge foregår i det digitale rom, og at norske mål er utsatt for et jevnt trykk av nettverksoperasjoner fra aktører som representerer fremmede stater.

Det vises også til at digitale angrep i økende grad har blitt en del av militære operasjoner. I NATO er det slått fast at et digitalt angrep vil kunne ha like alvorlige konsekvenser som et konvensjonelt angrep. Digitale angrep omfattes derfor av NATO-traktatens artikkel 5. Også i FN-pakten er det slått fast at digitale angrep kan utløse en stats rett til selvforsvar.

Sikkerhetsloven har krav om at skjermingsverdig informasjon, informasjonssystemer og infrastruktur skal beskyttes. Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner. Det vil si at informasjon er skjermingsverdige dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt eller blir endret eller utilgjengelig. Også skjermingsverdig infrastruktur skal beskyttes dersom det kan skade grunnleggende nasjonale funksjoner om den får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.

Etter sikkerhetsloven er departementene ansvarlig for forebyggende sikkerhetsarbeid innenfor sine ansvarsområder og skal identifisere og holde oversikt over grunnleggende nasjonale funksjoner.

Forsvarsdepartementet har identifisert evnen til kommando og kontroll over norske og allierte styrker som en grunnleggende nasjonal funksjon. Dette innebærer blant annet krav til beskyttelse og sikring av informasjonssystemer som i seg selv har avgjørende betydning for Forsvarets evne til kommando og kontroll, samt objekter og infrastruktur hvor det kan skade funksjonen dersom objektet eller infrastrukturen blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. Stortinget har også understreket viktigheten av å ivareta informasjonssikkerheten i Forsvaret gjennom å sikre og beskytte Forsvarets informasjonssystemer.

Riksrevisjonen vurderer at sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer gir risiko for svekket operativ evne, og kritiserer dette. Kritikken er utdypet i Riksrevisjonens sikkerhetsgraderte rapport.

1.3.2.1 Mangler i oversikt og dokumentasjon på IKT-området påvirker ivaretakelsen av sikkerheten i informasjonssystemene

Sikkerhetsloven stiller krav om at arbeidet med forebyggende sikkerhet skal være risikobasert. Oversikt over informasjonssystemer og tilhørende kommunikasjonsinfrastruktur er en grunnleggende forutsetning for at Forsvaret skal kunne foreta gode risikovurderinger og planlegge og gjennomføre effektive sikkerhetstiltak.

Undersøkelsen viser at Forsvaret ikke har god nok oversikt over alle informasjonssystemene som er i bruk. Kartlegging av hvilke av Forsvarets informasjonssystemer som er å anse som skjermingsverdige etter bestemmelsene i den nye sikkerhetsloven, er pågående. At gjennomføringen av verdi-, risiko- og skadevurderinger ikke er sluttført, innebærer at det ikke er fastsatt et forsvarlig sikkerhetsnivå for alle informasjonssystemene.

Forsvarssektorens egne direktiver og regelverk viser til krav om telling og kontroll av sikkerhetsgradert og sensitivt IKT-materiell i sektoren. Forsvarsmateriell har myndighet til å føre kontroll med sektorens materiellforvaltning, men har så langt i liten grad gjort dette på IKT-området.

Mangler i oversikten og kunnskapen om IKT-porteføljen svekker muligheten for en effektiv og forsvarlig ivaretakelse av sikkerheten i systemene. Riksrevisjonen mener dette er sterkt kritikkverdig.

1.3.2.2 Forsvaret har skjermingsverdige informasjonssystemer som ikke tilfredsstiller sikkerhetslovens krav

Både tidligere og nåværende sikkerhetslov har krav om at skjermingsverdige informasjonssystemer skal godkjennes av en godkjenningsmyndighet. For mange av Forsvarets informasjonssystemer er Nasjonal sikkerhetsmyndighet (NSM) godkjenningsmyndighet.

Et informasjonssystem som ikke er sikkerhetsgodkjent, kan få midlertidig brukstillatelse. Dette forutsetter imidlertid det benyttes kompenserende tiltak, slik at bruk av systemet er forsvarlig. I særlige tilfeller kan NSM også gi dispensasjon fra krav til midlertidig brukstillatelse. En slik dispensasjon skal kun gis i tilfeller der konsekvensene ved å ikke ta i bruk systemet overstiger konsekvensene ved sikkerhetsbrudd vurdert opp mot sannsynligheten for slike brudd.

Gjennom undersøkelsen har det fremkommet at Forsvaret har i bruk systemer som ikke tilfredsstiller sikkerhetslovens krav til godkjenning. Informasjonssystemer som ikke er sikkerhetsgodkjent, er ressurskrevende for sektoren å forvalte. Det har også kommet frem tilfeller der hensynet til operative behov har veid tyngre enn risikoen ved bruk av systemer uten sikkerhetsgodkjenning.

Forsvarets informasjonssystemer er avhengig av en underliggende kommunikasjonsinfrastruktur, bestående av blant annet fibernett, radionett og radiolinje. I tillegg strekker den seg over store geografiske områder. Det er identifisert sårbarheter i Forsvarets kommunikasjonsinfrastruktur.

I undersøkelsesperioden har det vært iverksatt flere tiltak på området. Blant annet er Handlingsplan for sikkerhetsgodkjenning av IKT-systemer utarbeidet, og det er iverksatt flere prosjekter for å oppgradere og sikre Forsvarets informasjonssystemer og kommunikasjonsinfrastruktur. Dette skal særlig realiseres gjennom virksomhetsprogrammene Mime og MAST.

Sikkerhetslovens krav skal sikre at skjermingsverdig informasjon ikke blir kjent for uvedkommende, går tapt eller blir endret eller utilgjengelig. Forsvarets manglende etterlevelse av sikkerhetslovens krav vil kunne få store konsekvenser i både fred, krise og krig. Riksrevisjonen mener dette er alvorlig.

1.3.2.3 Forsvaret har mangler i evnen til å oppdage og stanse digitale angrep

Forsvaret vurderer at det er mangler i egen evne til å oppdage og stanse digitale angrep. Forsvaret peker på sårbarheter i Forsvarets informasjonssystemer og tilgangen på personell med riktig kompetanse som årsaker til dette. Det tar lang tid for Cyberforsvaret å få personell opp på et tilstrekkelig godt kompetansenivå for gjennomføring av defensive cyberoperasjoner.

Det er iverksatt flere tiltak for å øke Forsvarets evne til å oppdage og stanse digitale angrep. De mest sentrale tiltakene er etablering av et sensornettverk og etablering og styrking av IKT-responsmiljøet MilCERT. Forsvarsdepartementet har også gitt etatene i forsvarssektoren føringer om å øve på bortfall av kommunikasjonsløsninger og håndtering av alvorlige IKT-hendelser. Med henvisning til langtidsplanen for forsvarssektoren for perioden 2021–2024 viser Forsvarsdepartementet også til at det fra 2021 er lagt opp til en bemanningsøkning i Cyberforsvaret.

Forsvarets evne til å oppdage og stanse digitale angrep er avgjørende for å kunne ivareta operativ evne gjennom å beskytte egne skjermingsverdige informasjonssystemer, inkludert kommando- og kontrollinformasjonssystemer. I ny langtidsplan for Forsvaret vises det til at digitale angrep i økende grad har blitt en del av militære operasjoner, og at skillelinjen mellom konvensjonell og irregulær krigføring har blitt mindre klar. Dette innebærer også at de tradisjonelle skillene mellom fred, krise og krig utfordres.

Riksrevisjonen mener det er alvorlig at Forsvarets evne til å oppdage og håndtere digitale angrep er begrenset ved et forhøyet trusselnivå.

1.3.2.4 Svakheter i sikkerhetsstyringen forsterker utfordringene

Virksomheter som er omfattet av sikkerhetsloven, skal etablere et system for sikkerhetsstyring som skal være en del av virksomhetens styringssystem. Sikkerhetsstyring omfatter alle aktiviteter med betydning for forebyggende sikkerhetsarbeid og skal bidra til et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige informasjonssystemer.

Undersøkelsen viser at Forsvaret har utfordringer med å ivareta krav til sikkerhetsstyring. Svakheter i sikkerhetsstyringen er erkjent av både Forsvaret selv og Forsvarsdepartementet og skyldes mangler i kompetanse, organisering og ressurser. I Informasjonssikkerhetsstrategi for forsvarssektoren fra 2017 peker Forsvarsdepartementet på behovet for å integrere informasjonssikkerhetsarbeidet i den helhetlige virksomhetsstyringen. Riksrevisjonens undersøkelse viser at sikkerheten på IKT-området fremdeles ikke er tilstrekkelig ivaretatt i virksomhetsstyringen i Forsvaret. Sikkerhetsstyringen har i tillegg i for stor grad blitt ensbetydende med prosessen for sikkerhetsgodkjenning av informasjonssystemer, framfor å være en del av den ordinære styringen.

Ansvaret for forvaltningen av informasjonssystemene er fordelt på flere aktører i forsvarssektoren. Forsvaret og Forsvarsmateriell har i undersøkelsesperioden hatt stor oppmerksomhet om ansvars- og rolleavklaring knyttet til forvaltningen av IKT-materiell, og jobber med å styrke forvaltningen ytterligere. Aktørenes forståelse og praktisering av ansvarsfordelingen framstår like fullt som en medvirkende årsak.

Forsvarssektoren har i undersøkelsesperioden truffet flere tiltak for å legge til rette for bedre sikkerhetsstyring og jobber videre med disse tiltakene. Samtidig står sektoren overfor potensielt vesentlige endringer i styring og forvaltning på IKT-området som følge av planer om strategisk samarbeid. Det vil stille endrede, men fortsatt høye, krav til kompetanse og kapasitet i Forsvaret for å forstå og håndtere operative og sikkerhetsmessige konsekvenser av bruk av IKT.

Det er i lys av dette sterkt kritikkverdig at Forsvaret ikke har et mer solid system for sikkerhetsstyring på plass.

1.3.3 Forsvarsdepartementet har over tid ikke greid å realisere effektive og sikre informasjonssystemer som understøtter Forsvarets operative evne

IKT ble pekt på som et satsingsområde i langtidsplanen for forsvarssektoren for 2017–2020. Formålet med IKT-satsingen var å tilrettelegge for at Forsvaret skulle kunne løse sine viktigste oppgaver, og å bidra til god utnyttelse av sektorens ressurser. IKT skulle benyttes som et virkemiddel for bedret samhandling i Forsvarets operasjoner. Målet var å utvikle en IKT-infrastruktur som skulle gi Forsvaret nødvendig evne til å lede og samvirke i et fellesoperativt perspektiv.

Det skulle i perioden også sikres en tydelig og helhetlig ledelse av IKT-virksomheten i Forsvaret underlagt forsvarssjefen. Overlappende styringsfunksjoner skulle unngås, og grensesnittet opp mot Forsvarsmateriell skulle vurderes som en del av den pågående konsolideringen av etaten. Bakteppet var at IKT-virksomheten i Forsvaret og forsvarssektoren var for fragmentert og manglet helhetlig og enhetlig ledelse og styring, og at dette hadde ført til høye kostnader, lav gjennomføringsevne og mangelfull funksjonalitet. IKT-området i Forsvaret og forsvarssektoren som helhet leverte ikke tilfredsstillende resultater sammenlignet med andre tilsvarende virksomheter. Det ble derfor pekt på at Forsvaret hadde et betydelig potensial for forbedring på IKT-området, knyttet både til organisering og til porteføljen av IKT-systemer som skulle realiseres i perioden.

Etter Riksrevisjonens vurdering er det sterkt kritikkverdig at Forsvarsdepartementet, Forsvaret og Forsvarsmateriell i liten grad har klart å svare ut de forventningene som ble stilt i forrige langtidsplan, hverken når det gjelder IKT-porteføljen eller styring og organisering. Sektoren har bred erkjennelse av utfordringene på området, men evnen til å løse disse har vært begrenset. Styringen i sektoren i perioden 2017–2020 har vært preget av manglende oversikt, uklar forståelse av roller og ansvar og svakheter i styringen av investeringer på IKT-området. Det er satt i verk tiltak for å bedre situasjonen, blant annet utarbeidelse av en IKT-strategi for forsvarssektoren og etablering av programmene Mime og MAST for anskaffelser av nye IKT-løsninger. Disse tiltakene har foreløpig hatt begrenset effekt, og det er for tidlig å si noe sikkert om de fremtidige effektene av disse tiltakene.

1.3.3.1 Svak styring har medvirket til utfordringene på IKT-området og svekket verdien av investeringer

Forsvaret har ansvar for at virksomheten har effektiv og sikker IKT til bruk i Forsvarets operasjoner. Dette inkluderer planer for virksomhetens bruk av IKT og ivaretakelse av sikkerheten i systemene.

Forsvaret mangler en virksomhetsarkitektur som kan legge til rette for gode prioriteringer i oppfølging av eksisterende IKT-løsninger og valg av nye. Oversikt over informasjonsbehov og informasjonssystemer er en forutsetning for å kunne legge hensiktsmessige planer og rammer for videreutviklingen av IKT-porteføljen. Forsvaret har ikke god nok oversikt over alle informasjonssystemene som er i bruk. Manglende virksomhetsarki-

tektur er også pekt på som en årsak til utfordringene med interoperabilitet mellom kommando- og kontroll-informasjonssystemene, og en virksomhetsarkitektur er avgjørende for å nå målet om å redusere antallet systemer i Forsvaret.

Forsvarssektoren har selv pekt på anskaffelser av IKT-materiell som en hovedutfordring i styringen av IKT-området. Forsvarsdepartementet har det overordnede ansvaret for investeringer i sektoren og styrer porteføljen av prosjekter. Fram til 1. januar 2020 var departementet også prosjekteier for det enkelte prosjekt. Departementet bemerker at porteføljen av investeringsprosjekter på IKT-området er stor, og at sterke avhengigheter mellom prosjektene gjør arbeidet med investeringsprosjekter på området krevende.

Forsvarets forskningsinstitutt peker i en rapport fra 2018 på omfattende forsinkelser i IKT-prosjekter i forsvarssektoren. Blant mulige årsaker nevnes nedprioritering og manglende tilgang på nødvendige ressurser, for optimistisk planlegging og lite effektiv prosjektgjennomføring.

Forsvarsmateriell planlegger og gjennomfører alle investeringsprosjekter i forsvarssektoren på oppdrag fra prosjekteier. Forsvarsmateriell oppgir at lang gjennomføringstid kan ha flere årsaker. Blant annet er flere prosjekter skjøvet ut i tid på grunn av mangel på finansiering i prosjektporteføljen. Forsvarsmateriell opplever også at de ikke har ressurser nok til å ha ønsket framdrift i alle investeringsprosjekter for IKT-området og samtidig ivareta forvaltningsoppgaver knyttet til IKT-materiell på ønsket måte. Forsvarsdepartementet bemerker at gjennomføringstiden for IKT-prosjekter har ført til en opphopning av IKT-systemer som venter på utskifting.

Forsvarets forskningsinstitutt fant at det også var store avvik mellom planlagte og faktiske kostnader i IKT-prosjektene. Forsvarsdepartementet har i en intern evaluering vist til at når teknologien blir forsinket eller mer kostbar enn planlagt, så svekkes verdien av IKT-investeringene.

Undersøkelsen viser at det er mangelfulle data om investeringsprosjekter i forsvarssektoren. Det er etablert et system for registrering og oppfølging av investeringsprosjekter, men systemet gir begrensede muligheter for analyse. Blant annet justeres milepæler årlig og nøkkeldata oppdateres løpende, og systemet gir begrenset mulighet til å hente ut historiske data. Med tanke på de store utfordringene sektoren har når det gjelder investeringer, kan svak tilgang på gode styringsdata få konsekvenser både for oppfølging av det enkelte prosjekt og for læring og forbedring på tvers av prosjekter.

Forsvarsdepartementet er ansvarlig for overordnet styring og kontroll av underlagte etaters virksomhet. Departementet bemerker at det har vært utfordrende å styre Forsvaret helhetlig på IKT-området. Forsvarsstaben har etter departementets vurdering ikke hatt tilstrekkelig kapasitet til å fastsette operative krav til IKT, prioritere på tvers av driftsenhetene og mellom investering og drift samt være et felles kontaktpunkt mot departementet innenfor IKT. Sjef Forsvarsstaben erkjenner at Forsvarsstabens kompetanse og styring på IKT-området har vært for dårlig, men viser til at det nå er tatt grep for å endre på dette. Kompetansen på IKT i Forsvarsstaben er styrket de siste par årene, og fra 2021 er ansvaret for gjennomføringen av IKT-strategi for forsvarssektoren overført fra departementet til Forsvaret. Med dette har Forsvaret fått ansvar på IKT-området for forsvarssektoren som helhet. I tillegg er rollen som prosjekteier i investeringsprosjekter overført fra departementet til forsvarssjefen. Både departementet og Forsvaret mener at overføring av mer ansvar til Forsvaret legger bedre til rette for en helhetlig styring innen IKT-området.

Etter Riksrevisjonens vurdering har det vært vesentlige svakheter både ved Forsvarsdepartementets og Forsvarets styring på IKT-området, som har negative følger for oversikt over og samvirke mellom systemer. Det har også vært svak styring av IKT-investeringer, med den følge at disse ikke har gitt ønsket verdi. Det er for tidlig å si om overføring av ansvar til Forsvaret vil gi bedre styring av IKT-området i Forsvaret og forsvarssektoren.

1.3.3.2 Overlappende og uklare ansvarsforhold mellom etatene i forsvarssektoren har påvirket gjennomføringsevnen på IKT-området

Forsvaret og Forsvarsmateriell er tydelige på at det etter opprettelsen av Forsvarsmateriell var nødvendig å avklare grensesnittet mellom etatene på IKT-området. En avklaring av roller og ansvar var også forventet av Forsvarsdepartementet i langtidsplanen for 2017–2020. Forsvarsdepartementet viser til at det ved etableringen av Forsvarsmateriell i 2016 ble utarbeidet retningslinjer for rolle- og ansvarsfordelingen mellom Forsvarsmateriell og Forsvaret, men at etterlevelsen av retningslinjene har vært beheftet med utfordringer. Departementet erkjenner at dette har resultert i noe overlappende oppgaveutførelse og lav gjennomføringsevne. Cyberforsvaret viser til at forholdet mellom Forsvaret ved Cyberforsvaret og Forsvarsmateriell er en del av forklaringen på at Forsvaret har brukt betydelige summer på ny teknologi uten å ha fått full utnyttelse av disse investeringene.

Undersøkelsen viser at det er lagt ned et omfattende arbeid for å avklare grensesnittet mellom Forsvaret og Forsvarsmateriell. Dette har blant annet ført til overføring av oppgaver og personell mellom etatene. Både Forsvaret, Forsvarsmateriell og departementet mener at ansvarfordelingen nå er blitt klarere, og at samarbeidet er blitt bedre. Samtidig ser man ved overgangen til ny langtidsperiode at det gjenstår utfordringer knyttet til ansvarsdelingen mellom Forsvaret og Forsvarsmateriell.

Blant annet viser Forsvarsmateriell til at etaten fortsatt er i prosess med å finne sin rolle på enkelte områder, og at det fremdeles er noe overlapp mellom oppgavene som utføres av Forsvaret og Forsvarsmateriell.

1.3.3.3 Mangel på kompetanse har medvirket til at forsvarssektoren ikke har klart å løse mange av utfordringene på IKT-området

Ved behandlingen av langtidsplanen for 2017–2020 sluttet Stortinget seg til at personellet er en avgjørende innsatsfaktor for forsvarssektoren, og at sektoren må ha evne til å rekruttere, anvende, beholde og utvikle kompetansen den trenger.

Forsvarssektoren har selv identifisert flere kompetansegap i sektoren når det gjelder IKT. Det er kompetanseutfordringer knyttet bruk, drift og forvaltning av eksisterende IKT-systemer og innen utvikling av nye løsninger. Det har også manglet kompetanse i styringen av IKT-området, helt opp til øverste nivå i Forsvaret og forsvarssektoren.

Manglende kompetanse er en medvirkende årsak til flere av utfordringene som beskrives i denne undersøkelsen, og til at forsvarssektoren ikke har klart å løse mange av utfordringene på IKT-området. I dette bildet må det tas med at forsvarssektoren, på lik linje med forvaltningen og samfunnet for øvrig, er truffet av mangel på ulike typer IKT-kompetanse. Sjef Cyberforsvaret viser til at det er utfordrende å rekruttere personell som har både riktig IKT- og militærfaglig kompetanse. Riksrevisjonen bemerker likevel at Svendsen-utvalget i 2020 påpeker at Forsvaret ikke har klart å henge med i utviklingen eller evnet å omstille seg i takt med nye behov for kompetanse for å utnytte teknologien og møte en økende trussel i det digitale rom. Det er ifølge Riksrevisjonen bekymringsfullt med tanke på dagens trusselbilde og hvor viktig effektive og sikre IKT-systemer er for Forsvarets operative evne.

Strategisk samarbeid med industrien, blant annet gjennom programmene Mime og MAST, er i undersøkelsen pekt på som et av de viktigste tiltakene for å øke kompetansen på IKT-området i forsvarssektoren. Det er etter Riksrevisjonens vurdering avgjørende at Forsvaret og Forsvarsmateriell klarer å rekruttere, utvikle og beholde nødvendig kompetanse i egne virksomheter, også ved bruk av strategisk samarbeid.

1.3.3.4 Det er vesentlig risiko knyttet til den pågående IKT-satsingen i Mime og MAST

For å møte en del av utfordringene på IKT-området startet Forsvarsdepartementet i 2018 virksomhetsprogrammene Mime og MAST. I program Mime inngår en rekke investeringsprosjekter som skal gi en taktisk informasjonsinfrastruktur som dekker nåværende og framtidige behov for kommando og kontroll. Mime er avhengig av MAST, som skal modernisere Forsvarets IKT-plattformer og gi forsvarssektoren tilgang på skytjenester på alle graderingsnivå.

Program Mime skal avsluttes i 2030, mens program MAST skal vare til 2028. Etter den innledende etablerings- og oppstartsfasen er begge programmene forsinket. Flere sentrale spørsmål av betydning for gjennomføringen og leveransene fra programmene står dessuten ubesvart. Riksrevisjonen mener dette utgjør en risiko for ytterligere forsinkelser og mangelfull gevinstrealisering.

Mime og MAST hviler på en anskaffelsesstrategi der strategisk samarbeid med overdragelse av drifts-, forvaltnings- og vedlikeholdsoppgaver til leverandørindustrien står sentralt. Forsvarssektorens krav til sikkerhet og beredskap skal vektlegges spesielt ved etablering av strategisk partnerskap. Det er så langt ikke avklart hva som vil være de folkerettslige konsekvensene av en overdragelse av disse oppgavene til sivile leverandører. En folkerettslig avklaring er nødvendig for å kunne fastsette de sivile leverandørenes forpliktelser overfor Forsvaret ved krise og krig og dermed Forsvarets tilgang på nødvendig IKT-understøttelse. Beslutningen om å gå i dialog om strategisk partnerskap med sivile leverandører før de folkerettslige konsekvensene av det planlagte samarbeidet er avklart, medfører risiko for at forhandlinger og eventuelle avtaler ikke reflekterer det reelle handlingsrommet og behovet i sektoren.

Forsvarets forskningsinstitutt konkluderte i januar 2021 med at bruk av skytjenester kan bidra til økt robusthet i Forsvarets kommunikasjonsinfrastruktur og være positivt for sikkerheten. Det er imidlertid fortsatt mye uavklart knyttet til regelverk og hvordan sikkerhetsvurdering og -godkjenning av slike systemer skal gjøres. Det kan i ytterste konsekvens bety at Forsvaret ikke kan ta i bruk eller hente ut ønskede effekter av skytjenester.

Forsvarssektoren har jobbet lenge med å finne løsninger som balanserer sektorens behov for sikkerhet og effektivitet i informasjonssystemer. Usikkerhet knyttet til valg av løsninger gjør at beslutninger og utbedringer trekker ut i tid.

Programorganiseringen i Mime og MAST skal legge til rette for å kunne se IKT-investeringer i sammenheng og vurdere innbyrdes avhengigheter mellom dem i prioriteringen av ressurser. Det er ut fra dette bekymringsfullt at ekstern kvalitetssikring av Mime peker på utfordringer med å foreta kost–nytte–vurderinger og å prioritere ut fra foreliggende styringsinformasjon. At programorganisasjonen også peker på behov for avklaring av ambisjonsnivå og sammenhengen med investeringer som faller utenfor programmet, forsterker et inntrykk av vesentlige svakheter i styringsinformasjonen og risiko for gjennomføringen. Programorganisasjonen for

Mime og MAST peker så sent som i juni 2021, ett år etter formell oppstart av programgjennomføringen for Mime, på at den mangler verktøyene for å gjennomføre programmet som forutsatt. For MAST er programmets virkningsområde ikke avklart ved overgangen til gjennomføringsfasen.

Leveransene fra Mime og MAST er av forsvarssektoren trukket fram som avgjørende for at forsvarssektoren skal nå mål om digitalisering, effektivisering og tilhørende økt operativ evne. Behovet for mer effektiv og sikker IKT-understøttelse i Forsvarets operasjoner bekreftes i denne undersøkelsen. Utsettelser og mangelfull gevinstrealisering fra Mime og MAST er derfor ikke bare et kostnads- og ressursspørsmål. En eventuell manglende realisering av ambisjonene i programmene har konsekvenser for operativ evne i Forsvaret, både på kort og lang sikt.

Riksrevisjonens kollegium mener at funnene i undersøkelsen er av en slik alvorlighetsgrad at det legger til grunn at Riksrevisjonen 1–2 år etter Stortingets behandling vil følge opp undersøkelsen, herunder programmene Mime og MAST.

1.4 Anbefalinger

Riksrevisjonen anbefaler at Forsvarsdepartementet

- følger opp arbeidet med å få en fullstendig oversikt over informasjonssystemer i Forsvaret, og at denne blir brukt som grunnlag for Forsvarets styring og investeringer på IKT-området
- sørger for at Forsvaret og Forsvarsmateriell intensiverer arbeidet med variantbegrensning av Forsvarets informasjonssystemer
- i dialog med Forsvaret og Forsvarsmateriell sikrer løsninger for kommunikasjon og informasjonsutveksling som raskere gir full utnytelse av kapasiteter ved anskaffelser av nytt materiell
- følger opp at sikkerhetsstyringen styrkes, og at informasjonssikkerheten ivaretas i nye og eksisterende informasjonssystemer i Forsvaret.
- styrker Forsvarets evne til å oppdage og stanse digitale angrep
- sørger for at Forsvarsmateriell og Forsvaret ivaretar nødvendig framdrift og gevinstrealisering i programmene Mime og MAST
- følger opp arbeidet med å avklare ansvaret mellom etatene i forsvarssektoren
- vurderer ytterligere tiltak for å rekruttere, utvikle og beholde nødvendig fagkompetanse på IKT-området i forsvarssektoren.

1.5 Statsrådens svar

Forsvarsministeren bemerker at Riksrevisjonen gjennom sin undersøkelse stadfester problemstillinger og et utfordringsbilde Forsvarsdepartementet erkjenner. Statsråden viser til at den gjeldende IKT-strategien for forsvarssektoren er utformet for å møte disse utfordringene. Det er imidlertid behov for tiltak som kan øke gjennomføringen av strategien. Statsråden ser svært alvorlig på dette og tar Riksrevisjonens anbefalinger med seg i det videre arbeidet.

1.5.1 Evne til å realisere effektive og sikre informasjonssystemer

Statsråden viser til IKT-strategi for forsvarssektoren som ble gitt ut i 2019, og mener at strategiens tiltaksområder står seg som svært relevante i møtet med Riksrevisjonens kritikk, til tross for at implementerte tiltak så langt har hatt begrenset effekt. Statsråden viser til at tiltakene i strategien er omfattende og strekker seg over tid, og at de innebærer gjennomgående endringer i både departementet og etatene.

Statsråden viser videre til at Forsvarsdepartementet i samråd med Forsvaret og Forsvarsmateriell utarbeider en plan for å øke gjennomføringsevnen med utgangspunkt i IKT-strategien. Statsråden mener derfor at det på nåværende tidspunkt er for tidlig å avvikle eller reversere besluttede tiltak. Han opplyser at hans første prioritering er å følge opp at de grunnleggende premissene for realisering av strategien kommer på plass, og at et tydelig, dokumentert og etterlevd styringssystem for IKT-området er sentralt. Forsvaret har gjennom tildelingsbrevet for 2022 fått et oppdrag som blant annet omfatter forutsetninger for å realisere IKT-strategien og å gi anbefalinger om en styringsmodell for IKT. Forsvarsdepartementet følger opp arbeidet gjennom etatsstyringen og i fagmøter.

Statsråden peker på at Forsvarsdepartementet i 2019 styrket den strategiske styringen av investeringsporteføljen, og at endringen fra 1. januar 2020 ga forsvarssjefen et tydeligere ansvar for investering, drift og gevinstrealisering innenfor IKT-området.

Statsråden bemerker at forsvarssektoren står overfor en omfattende omstilling og modernisering, og at det i denne prosessen er nødvendig at forsvarssektoren har tilgang til oppdatert teknologi, løsninger og kompetanse på områder der industrien er ledende. For å oppnå dette vurderes det strategisk samarbeid med én eller flere samarbeidspartnere.

Statsråden viser til at det gjennom virksomhetsprogrammene Mime (kampnær IKT) og MAST (militær anvendelse av skytjenester) etableres en ny operasjonsmodell for IKT i forsvarssektoren. Det er gjennomført en ekstern kvalitetssikring på både program- og leveransebølgenivå for Mime. Forsvarsdepartementet vil følge opp risikoene som Riksrevisjonen har påpekt og tiltakene som ekstern kvalitetssikrer har anbefalt.

Statsråden opplyser også om at Forsvarsdepartementet forsterker oppfølgingen av IKT-området gjen-

nom etatsstyringen. Dette inkluderer regelmessige fag- og styringsmøter mellom Forsvarsdepartementet og etatene og krav til utfyllende rapportering på IKT-området.

1.5.2 Manglende realisering av effektive kommando- og kontrollinformasjonssystemer

Statsråden viser til virksomhetsprogrammet Mime som sentralt i utbedringen av flere av de konkrete kommunikasjonsutfordringene som Riksrevisjonen viser til i sin undersøkelse. Gjennom toårlige leveransebølger fram mot 2030 skal programmet levere kampnær IKT til Forsvaret. Delleveransene som er godkjent av Stortinget, inkluderer en felles, taktisk IKT-plattform, satellitterminaler, bakke-til-luft-radioer, datalinkterminaler og programvare for kommando og kontroll, nye taktiske radioer til landstyrkene og start av fornyelsen av kommando- og kontrollsystem for luftdomenet. Statsråden viser videre til at Forsvarets evne til samvirke på tvers av graderingsnivåer er forbedret gjennom en løsning for sikker informasjonsutveksling mellom sikkerhetsdomener, levert av Forsvarsmateriell i 2021–2022.

1.5.3 Sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer

Statsråden peker på at Forsvarsdepartementet har informert Stortinget om at Forsvaret og Forsvarsmateriell har utfordringer med å beskytte informasjonssystemer i samsvar med sikkerhetslovens krav om et forsvarlig sikkerhetsnivå, og opplyser om at departementet vil videreføre sin særskilte oppfølging av Forsvarets og Forsvarsmateriells arbeid med informasjonssikkerhet så lenge det er behov for dette. Statsråden peker videre på at sikkerhetstilstanden i IKT-porteføljen påvirkes av andre utfordringer på IKT-området, og at det derfor er svært viktig også fra et sikkerhetsperspektiv at moderniseringen av Forsvarets IKT lykkes.

Når det gjelder Riksrevisjonens anbefaling om å styrke Forsvarets evne til å oppdage og stanse digitale angrep, viser statsråden til at oppbyggingen av milCERT går i henhold til planen og at full operativ kapasitet nås i 2024. Forsvarsdepartementet vil også se nærmere på ytterligere tiltak for å styrke Forsvarets evne i det digitale rom, jf. Meld. St. 10 (2021–2022) Prioriterte endringer, status og tiltak i forsvarssektoren. Forsvarets kapasitet til å oppdage og håndtere uønskede digitale hendelser ble derfor ifølge statsråden styrket gjennom Prop. 78 S (2021–2022), Endringer i statsbudsjettet 2022.

1.5.4 Personell og kompetanse

Statsråden viser til at etatene i forsvarssektoren har de samme utfordringene med tilgang til kompetanse på IKT-området som samfunnet for øvrig, og at de konkurrerer om de samme kandidatene som andre offentlige virksomheter og privat næringsliv. For å øke tilgangen på relevant kompetanse, herunder et særskilt behov for kompetanse innen teknologi og digitalisering, skal Forsvaret i tråd med gjeldende langtidsplan videreutvikle og øke utnyttelsen av verneplikten, lærlingeordningen, reservistordningen og samarbeidsordninger med allierte, næringslivet, sivile utdanningsinstitusjoner og andre sektorer. Statsråden opplyser videre at Forsvarsdepartementet følger opp kompetanse som en integrert del av styringen av etatene.

1.5.5 Avslutning

Statsråden gir uttrykk for at Riksrevisjonens konklusjoner og anbefalinger er viktige bidrag til forbedring av IKT-området i forsvarssektoren. Statsråden deler Riksrevisjonens oppfatning av at situasjonen er alvorlig, og bemerker at oppfølgingen av tiltakene som er beskrevet i det foregående, vil ha høy prioritet i både Forsvarsdepartementet, Forsvaret og Forsvarsmateriell. Dette er samtidig et område som vil kreve gjennomgående endringer både i Forsvarsdepartementet og i etatene, og som krever at tiltak må få virke over tid.

1.6 Riksrevisjonens uttalelse til statsrådens svar

Riksrevisjonen har ingen ytterligere merknader.

2. Komiteens behandling

Riksrevisjonen overleverte Dokument 3:3 (2022–2023) til Stortinget 4. oktober 2022. Denne innstillingen tar utgangspunkt i en ugradert versjon av dokumentet som ble offentliggjort samme dag. Riksrevisjonen har i dialog med Forsvarsdepartementet utarbeidet et ugradert dokument som er så fullstendig som mulig. Graderte opplysninger er fjernet, og en del informasjon er omskrevet og gjort mindre detaljert, slik at den ikke anses som gradert. Dette gjelder også noen av konklusjonene og deler av kritikken. Forsvarsdepartementet vurderer at dokumentet ikke inneholder gradert informasjon. Rapporten fra undersøkelsen, som følger som vedlegg til det graderte dokumentet til Stortinget, er gradert konfidensielt etter reglene i sikkerhetsloven.

Komiteen besluttet i møte 18. oktober 2022 å avholde en lukket kontrollhøring 16. januar 2023 som ledd i behandlingen av saken. Komiteen besluttet at høringen skulle omhandle – men ikke begrense seg til – følgende problemstillinger:

1. Hvordan oppstod manglene som Riksrevisjonen påpeker?
2. Hvordan følger Forsvarsdepartementet opp Riksrevisjonens konklusjoner og anbefalinger?
   - Hvordan ser Forsvaret og Forsvarsmateriell på sin rolle i dette arbeidet?
   - Riksrevisjonen påpeker risiko med tiltak som skulle avhjelpe problemene på IKT-området. Hvordan kan denne risikoen minimeres?
3. Hva er status når det gjelder konklusjonene i Riksrevisjonens rapport?
   - Mangler i samvirket mellom Forsvarets kommando- og kontrollinformasjonssystemer kan påvirke Forsvarets operative evne.
   - Sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer gir risiko for svekket operativ evne.
   - Forsvarsdepartementet har over tid ikke greid å realisere effektive og sikre informasjonssystemer som understøtter Forsvarets operative evne.

Følgende ble invitert og deltok på høringen:

- Norges offisers- og spesialistforbund v/forbundsleder Torbjørn Bongo
- Befalets Fellesorganisasjon v/leder Jens B. Jahren
- Nasjonal sikkerhetsmyndighet v/direktør Sofie Nystrøm
- Forsvarets forskningsinstitutt v/adm. direktør Kenneth Ruud
- Forsvars- og sikkerhetsindustriens forening v/adm. direktør Torbjørn Svensgård
- Tidl. direktør Forsvarsmateriell Mette Sørfonden
- Forsvarsmateriell v/direktør Gro Jære med programdirektør Forsvarsmateriell Mime/MAST Cathrine Devold
- Tidl. forsvarssjef admiral (P) Haakon Bruun-Hanssen
- Forsvarssjef general Eirik Johan Kristoffersen med sjef Cyberforsvaret Halvor Johansen
- Tidl. forsvarsminister Ine Eriksen Søreide
- Tidl. forsvarsminister Frank Bakke-Jensen
- Forsvarsminister Bjørn Arild Gram

Det ble tatt stenografisk referat fra den lukkede høringen. Komiteen har i samråd med Forsvarsdepartementet fått utarbeidet en offentlig versjon av referatet fra høringen.

Som ledd i behandlingen av saken sendte komiteen 21. februar 2023 brev med spørsmål til forsvarsministeren. Bakgrunnen var en pressemelding fra Forsvaret datert 13. februar 2023 med tittelen «Endrer planene for gjennomføring av MAST-programmet». Forsvarsministeren besvarte brevet 24. februar 2023.

Komiteen sendte 14. mars 2023 brev med oppfølgingsspørsmål til forsvarsministeren knyttet til beslutningen om å avlyse konkurransen knyttet til MAST-programmet. Forsvarsministeren besvarte brevet 21. mars 2023.

Korrespondansen følger som vedlegg til innstillingen.

3. Komiteens merknader

Komiteen, medlemmene fra Arbeiderpartiet, Kari Henriksen, Lubna Boby Jaffery og Bente Irene Aaland, fra Høyre, lederen Peter Frølich og Svein Harberg, fra Senterpartiet, Nils T. Bjørke, fra Fremskrittspartiet, Carl I. Hagen, fra Sosialistisk Venstreparti, Audun Lysbakken, fra Rødt, Seher Aydar, og fra Venstre, Grunde Almeland, viser til Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner.

Komiteen viser til at selve undersøkelsen er gradert etter sikkerhetsloven, men at Riksrevisjonen har utarbeidet en ugradert versjon av Dokument 3:3 (2022–2023). Komiteen viser videre til sin merknad i behandlingen av Harberg-utvalgets rapport, jf. Innst. 143 S (2021–2022):

> «Komiteen stiller seg bak utvalet si vurdering om at sjølv om informasjonseigar avgjer graderinga, har informasjonseigar like fullt ein skyldnad overfor offentlegheita som må takast omsyn til. Komiteen legg til grunn, i tråd med konklusjonen frå utvalet, at i den grad ein rapport inneheld graderte opplysningar som inneber at rapporten ikkje kan offentleggjerast i sin heilskap, forventar me at Riksrevisjonen utarbeider ein versjon av rapporten kor graderte opplysningar er unnatekne, og som elles er så fullstendig som mogeleg.»

Komiteen er fornøyd med at Riksrevisjonen i dialog med Forsvarsdepartementet har fulgt opp Stortingets forventning. Den ugraderte oppsummeringen muliggjør offentlig innsyn og åpen debatt, uten at graderte opplysninger kommer på avveie.

Komiteen viser videre til riksrevisors uttalelse i forbindelse med framleggingen av den ugraderte oppsummeringen:

> «Rapporten om Forsvarets informasjonssystemer er en av de mest alvorlige Riksrevisjonen noen gang har lagt frem.»

Komiteen deler riksrevisors vurdering av sakens alvor og viser til at denne også deles av forsvarsministeren i hans svar til Riksrevisjonen.

Komiteen har avholdt en lukket høring om rapportens funn.

Komiteen viser til Riksrevisjonens konklusjoner:

- Mangler i samvirket mellom Forsvarets kommando- og kontrollinformasjonssystemer kan påvirke Forsvarets operative evne.
  - Kommando- og kontrollinformasjonssystemer med ulik teknologi påvirker mulighetene for samhandling.
  - Ulike sikkerhetsdomener påvirker informasjonsutvekslingen mellom systemer.
  - Mangler ved taktisk datalink reduserer mulighetene for utveksling av data.
- Sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer gir risiko for svekket operativ evne.
  - Mangler i oversikt og dokumentasjon på IKT-området påvirker muligheten for ivaretakelsen av sikkerheten i informasjonssystemene.
  - Forsvaret har skjermingsverdige informasjonssystemer som ikke tilfredsstiller sikkerhetslovens krav.
  - Forsvaret har mangler i evnen til å oppdage og stanse digitale angrep.
  - Svakheter i sikkerhetsstyringen forsterker utfordringene.
- Forsvarsdepartementet har over tid ikke greid å realisere effektive og sikre informasjonssystemer som understøtter Forsvarets operative evne.
  - Svak styring har medvirket til utfordringene på IKT-området og svekket verdien av investeringer.
  - Overlappende og uklare ansvarsforhold mellom etatene i forsvarssektoren har påvirket gjennomføringsevnen på IKT-området.
  - Mangel på kompetanse har medvirket til at forsvarssektoren ikke har klart å løse mange av utfordringene på IKT-området.
  - Det er vesentlig risiko knyttet til den pågående IKT-satsingen i Mime og MAST.

Komiteen viser til at Riksrevisjonen har uttalt at denne rapporten, som undersøker perioden 2017–2020, er en av de mest alvorlige de har lagt fram. Den sikkerhetspolitiske situasjonen er vesentlig forverret for Norge og våre allierte siden 2020, med forhøyet konfliktnivå og økende ustabilitet. Samtidig foregår det et teknologikappløp mellom verdens maktsentra. Komiteen mener at disse forhold danner et svært alvorspreget bakteppe for rapportens funn, konklusjoner og anbefalinger som er verdt å understreke.

Mangler i samvirket mellom Forsvarets kommando- og kontrollinformasjonssystemer kan påvirke Forsvarets operative evne

Komiteen viser til at Riksrevisjonen finner at mangler i samvirket mellom Forsvarets kommando- og kontrollsystemer kan påvirke Forsvarets operative evne. Komiteen understreker at Forsvarets oppdrag er å trygge rikets sikkerhet, og at det ikke er tilfredsstillende at Forsvarets kommandosystemer samvirker godt nok til å løse daglige behov i fredstid. Komiteen mener at denne mangelen er desto mer alvorlig i lys av den gjeldende sikkerhetspolitiske situasjonen.

Komiteen registrerer at Forsvaret ikke har lyktes med å redusere antall informasjonssystemer i drift, til tross for at dette i lang tid har vært et mål. Komiteen deler Forsvarets vurdering av at utfasing av informasjonssystemer må prioriteres, og vil understreke at ansvaret for at dette blir gjort, i siste instans ligger hos Forsvarsdepartementet.

Komiteen viser til at samhandlingsproblemene i forsvarssektoren ikke bare knytter seg til eldre systemer som ennå ikke er faset ut, men også at det anskaffes nye våpenplattformer til Forsvaret som ikke er interoperable med systemene som allerede er i bruk. Komiteen forutsetter at anskaffelsesrutinene i forsvarssektoren ikke legger til rette for ytterligere samhandlingsproblemer.

Komiteen viser til at Riksrevisjonen finner mangler ved taktisk datalink som reduserer mulighetene for utveksling av data mellom Forsvarets enheter. Komiteen registrerer at det er flere planlagte og pågående prosjekter knyttet til å oppgradere taktisk datalink, men også at Riksrevisjonens undersøkelse påviser forsinkelser og risiko for mangelfull koordinering også mellom disse prosjektene, samt risiko for at kapasiteten ikke vil kunne utnyttes fullt ut. Komiteen forventer at regjeringen sørger for at oppgraderingene får den forutsatte gevinst.

Sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer gir risiko for svekket operativ evne

Komiteen viser til at Riksrevisjonen finner flere sårbarheter i Forsvarets informasjonssystemer og konkluderer med at disse gir risiko for at Forsvarets operative evne svekkes. Komiteen viser til Nasjonal sikkerhetsmyndighets (NSM) trusselvurdering «Risiko» for 2022, som allerede før Russlands invasjon av Ukraina fant en tredobling i antall alvorlige hendelser og cyberoperasjoner i perioden 2019 til 2021 og anførte:

«Risiko for alvorlige cyberoperasjoner er høy og øker for virksomheter som arbeider med utenriks-, forsvars- og sikkerhetspolitikk.»

Komiteen viser til sikkerhetslovens krav om at skjermingsverdig informasjon, informasjonssystemer og infrastruktur skal beskyttes, og at det er Forsvarsdepartementets ansvar å sørge for forebyggende sikkerhetsarbeid innenfor sitt ansvarsområde, herunder Forsvarets informasjonssystemer.

Komiteen viser til at Forsvaret på undersøkelsestidspunktet ikke hadde tilfredsstillende oversikt over informasjonssystemene som er i bruk, og ei heller hadde kartlagt skjermingsverdige systemer, og at det som en konsekvens ikke kunne fastsettes et forsvarlig sikkerhetsnivå for alle informasjonssystemene.

Komiteen finner det kritikkverdig at Forsvarsmateriell i liten grad har brukt sin myndighet til å føre kontroll med forsvarssektorens materiellforvaltning på IKT-området. Komiteen forventer at regjeringen etablerer rammene som trengs for at denne kontrollen utføres.

Komiteen deler Riksrevisjonens vurdering av at det er alvorlig at Forsvaret har tatt i bruk skjermingsverdige informasjonssystemer som ikke tilfredsstiller sikkerhetslovens krav, og slutter seg til at Forsvarets manglende etterlevelse av sikkerhetslovens krav vil kunne få store konsekvenser i fred, krise og krig.

Komiteen viser til at Forsvaret ifølge sine egne vurderinger ikke har god nok evne til å oppdage og stanse digitale angrep, og deler Riksrevisjonens vurdering av at det er alvorlig at denne evnen er begrenset ved et forhøyet trusselnivå. Komiteen forventer at regjeringen sikrer bemanningsøkningen til Cyberforsvaret som Stortinget har forutsatt i behandlingen av Langtidsplan for forsvarssektoren 2021–2024, jf. Innst. 87 S (2020–2021). Komiteen registrerer at forsvarsministeren svarer at full operativ kapasitet i responsmiljøet Cyberforsvarets cybersikkerhetssenter (milCERT) vil bli nådd i 2024.

Komiteen slutter seg til Riksrevisjonens vurdering av at det er sterkt kritikkverdig at Forsvaret mangler et solid system for sikkerhetsstyring. Komiteen viser til at ansvaret for å forvalte informasjonssystemene er fordelt på flere aktører, herunder Forsvaret og Forsvarsmateriell, og at Riksrevisjonens vurdering er at disse aktørenes forståelse og praktisering av ansvars- og rollefordelingen seg imellom har bidratt til svakhetene i sikkerhetsstyringen.

Forsvarsdepartementet har over tid ikke greid å realisere effektive og sikre informasjonssystemer som understøtter Forsvarets operative evne

Komiteen viser til at IKT ble pekt på som et satsingsområde i langtidsplanen for forsvarssektoren for 2017–2020, hvor IKT blant annet skulle benyttes for å bedre samhandlingen i Forsvarets operasjoner. Komiteen deler Riksrevisjonens vurdering av at det er sterkt kritikkverdig at Forsvarsdepartementet, Forsvarsmateriell og Forsvaret ikke har møtt forventningene Stortinget stilte til IKT-portefølje, styring og organisering i forrige langtidsplan.

Komiteen vil understreke viktigheten av at Forsvaret får etablert en virksomhetsarkitektur som muliggjør helhetlig styring og prioritering på IKT-området.

Komiteen viser til Riksrevisjonens funn om at overlappende og uklare ansvarsforhold mellom Forsvaret og Forsvarsmateriell har påvirket gjennomføringsevnen på IKT-området og bidratt til at IKT-investeringer ikke har blitt utnyttet til fulle. Forsvarsdepartementet erkjenner overfor Riksrevisjonen at etatene ikke har klart å etterleve de opprinnelige retningslinjene for rolle- og ansvarsfordeling, og at det har resultert i noe overlappende oppgaveutførelse og lav gjennomføringsevne.

Komiteen registrerer at Riksrevisjonen identifiserer forsvarssektorens mangel på kompetanse helt opp til øverste nivå som en medvirkende årsak til at sektoren ikke har klart å løse mange av utfordringene på IKT-området. Komiteen deler Riksrevisjonens vurdering av at det er avgjørende at Forsvaret og Forsvarsmateriell klarer å rekruttere, utvikle og beholde nødvendig kompetanse i egne virksomheter, også ved bruk av strategisk samarbeid.

Komiteen viser til at Riksrevisjonen har pekt på svak styring, overlappende og uklare ansvarsforhold og mangel på kompetanse som viktige årsaker til at Forsvarsdepartementet over tid ikke har realisert effektive og sikre informasjonssystemer som understøtter Forsvarets operative evne.

Komiteen viser til at IKT ble pekt på som et satsingsområde i langtidsplanen for forsvarssektoren for 2017–2020, jf. Prop. 151 S (2015–2016) Kampkraft og bærekraft – Langtidsplan for forsvarssektoren. IKT-satsingen skulle tilrettelegge for at Forsvaret skulle kunne løse sine viktigste oppgaver, og bidra til god utnyttelse av sektorens ressurser. IKT skulle også benyttes som et virkemiddel for å bedre samhandlingen i Forsvarets operasjoner og for å effektivisere styrkeproduksjon og forvaltning i forsvarssektoren. Målet var å utvikle en IKT-infrastruktur som skulle gi Forsvaret nødvendig evne til å lede og samvirke i et fellesoperativt perspektiv.

Komiteen viser til Forsvarets forskningsinstitutt, som uttalte følgende i høringen:

«FFI har siden 2004 forsket på modernisering og effektivisering av Forsvarets virksomhet, herunder operativ virksomhet. Vår forskning viser at evnen til å modernisere har vært for svak, og at ledelsen av Forsvaret har manglet kompetanse og kapasitet til å drive slike prosesser framover. Forsvaret og forsvarssektoren for øvrig er preget av mange tunge fagmiljøer med sine egne faglige identiteter. Kompetansen er utpreget militær av karakter, og agendaer og kulturen er rettet mot å bevare heller enn å endre. Summen av dette bidrar til at modernisering og effektivisering, gjerne tenkt støttet av nye IKT-systemer, mister retning og kraft i møte med personell lenger ned i organisasjonen. FFI har også vist at forsvarssektoren bruker lang tid på å utfase materiell, herunder IKT-systemer, noe som reduserer evnen til å modernisere virksomheten.

[...]For det første ser vi at dette vi kan kalle fellesprosjekter, altså IKT, logistikk og lignende, har i liten grad hatt en tydelig eier i forsvarssektoren, og de har blitt prioritert ned over tid sammenlignet ned prosjekter knyttet til grenene, som kampvogner, kampfly, overflatefartøy f.eks.»

«Så mener vi også å se en utydelig styring av IKT-virksomheten knyttet til investeringer. Det er flere ulike oppfatninger av roller og ansvar og myndighet i sektoren, som også gjør det utydelig for oss hvem som av og til er mottaker av våre råd knyttet til både utvikling av IKT-virksomheten og materiellanskaffelser.»

Komiteen merker seg hvordan FFIs beskrivelse av situasjonen samsvarer med Riksrevisjonens funn. FFIs beskrivelse av utfordringer knyttet til avklaring av roller og ansvar, sammen med kompetanseutfordringer, ble støttet både av tillitsvalgte, av NSM og av nåværende og tidligere forsvarssjefer i høringen.

Forbundsleder Torbjørn Bongo fra Norges offisers- og spesialistforbund uttalte følgende i høringen:

«Vi mener dette er de bakenforliggende årsakene som det må ryddes opp i: Den første er RAM, roller, ansvar og myndighet og da roller, ansvar og myndighet mellom Forsvaret og FMA på sektornivå. Etter vår vurdering ligger det betydelige utfordringer og problemer her.»

Leder Jens Bernhard Jahren fra Befalets Fellesorganisasjon uttalte følgende i høringen:

«Enhetlig styring er en veldig avgjørende faktor. Vi var veldig skeptisk til den oppsplittingen som ble gjort med etableringen av Forsvarsmateriell, hvor man altså splittet opp deler av IKT-miljøene, men også andre elementer. Vi mener at vi i dag ser de svakhetene som ble påpekt allerede da denne oppsplittingen kom. Det er viktig at dette området ledes fra ett sted, og at det er veldig godt avklart. Vi ser at de svakhetene kommer veldig klart til uttrykk.»

Direktør Sofie Nystrøm i Nasjonal sikkerhetsmyndighet (NSM) sa følgende i høringen:

«Det er tre områder som helt åpenbart er viktig for forsvarssektoren å styrke framover, og vi har vært inne på det: Sikkerheten må tydeliggjøres i styringsmodellen, roller, ansvar og myndighet må gås opp på sikkerhetstemaer slik at det er tydeligere mellom etatene, eller man må få en annen styringsmodell for hvordan sikkerhet og risiko skal helhetlig integreres, for sikkerhet må være integrert i prosessene i større grad.

Det andre punktet er teknisk gjeld, som jeg har vært inne på, gamle systemer – sterkere styring på dette området og variantbegrensning som vil gjøre at det er mye enklere for Forsvaret og partnere og leverandører å ha oversikt og kontroll.

Det siste er arkitektur. Virksomhetsarkitektur – en solid. helhetlig arkitektur – må være målbildet framover for å kunne styre dette på en god måte. Å styrke det med både kompetanse, styring og ressurser blir et avgjørende punkt for forsvarssektoren.»

Tidligere forsvarssjef admiral (P) Haakon Bruun-Hanssen sa følgende i høringen:

«De utfordringene innenfor operativ IKT som Riksrevisjonen peker på, er etter min vurdering et resultat av at Forsvaret ikke evnet å følge med i utviklingen innenfor IKT. Investeringsprosessene i Forsvaret gikk ikke raskt nok til å følge utviklingen innenfor datateknologi, og gapet i kompetansebehov bare økte som følge av manglende evne til å konkurrere om den arbeidskraften i et tøft marked. Opprettelsen av FMA i 2016 skapte uklare roller og ansvarsforhold i forsvarssektoren og bidro til at man ikke kom i gang raskt nok med å finne løsninger på de IKT-utfordringene som var avdekket.»

På spørsmål fra saksordfører Seher Aydar om hvorvidt forsvarssjefen i dag opplever å ha forutsetningene og myndigheten til å sikre Forsvaret effektive og sikre kommando- og kontrollinformasjonssystemer, svarte forsvarssjef general Eirik Kristoffersen:

«Det er et veldig godt spørsmål. Jeg har opplagt ansvaret, men myndigheten er ikke der ennå. Det snakkes om rolle, ansvar og myndighet. Jeg er ikke så opptatt av rolle. Jeg er opptatt av ansvar og myndighet. Jeg har fått ansvaret for dette i sektoren, men fortsatt rapporterer f.eks. Forsvarsmateriell i en annen kommandokjede enn det jeg gjør. Vi rapporterer begge som likeverdige etater, som også tidligere forsvarssjef påpekte, men der jobbes det med å finne løsninger som gjør at vi skal avklare dette.»

Komiteen viser til at tidligere forsvarsminister Ine Eriksen Søreide hadde den samme oppfatningen:

«Området har også vært gjenstand for uklare både rolle- og ansvarsforhold. Til dels har det vært gjennomført en god del omkamper oppigjennom, og det har vært liten evne til å fase ut gamle systemer når det har vært nødvendig, samtidig som man da har mange ulike systemer i bruk på samme tid. Ikke minst har investeringsprosessene vært for lange. Jeg syns egentlig tidligere forsvarssjef Bruun-Hanssen illustrerte det på en ganske god måte, hvordan overgangen i de operative miljøene har vært, fra teleks – litt billedlig forklart – og over til bilde og data.»

Eriksen Søreide uttalte følgende om hvilke tiltak som ble iverksatt:

«Man kan si at langtidsplanen 2017–2020 egentlig var det aller viktigste samledokumentet. Som Riksrevisjonen også påpeker i sin rapport, var IKT utpekt som et satsingsområde i LTP'en. Det handlet om penger, selvfølgelig, og om oppmerksomhet, men også om en erkjennelse av at det området ikke hadde vært godt nok håndtert gjennom lang tid. […]

Jeg tenker at det også kan være nyttig å bruke litt tid på etableringen av FMA, for det har vært et tilbakevendende tema her. Da tror jeg det er nyttig å ha med seg historien. FLO ble opprettet i 2002. FLO løste egentlig aldri de problemene FLO var ment å løse, til tross for gjentatte både omorganiseringer og endringer. […]

Noe av hovedutfordringen var at ansvars- og styringslinjene var for lange. […] Det var en veldig stor utfordring. som man så for seg å løse gjennom opprettelsen av FMA. Det betyr ikke at vi nødvendigvis hadde alt klart da FMA ble opprettet, i den forstand at alle grensesnitt var gått opp. Men det lå også i forutsetningene at det skulle gjøres.»

Komiteen viser til at daværende forsvarsminister Frank Bakke-Jensen den 27. mars 2019 godkjente hoveddokumentet «IKT-strategi for forsvarssektoren». I strategien gir departementet en analyse av nåsituasjonen og utfordringene og etablerer et målbilde med tilhørende tiltaksområder. Komiteen viser til at strategien er utformet for å møte utfordringsbildet som er erkjent i sektoren.

Komiteen viser til at det på IKT-området er mindre tydelige skiller mellom investering og drift enn det som er alminnelig innenfor tradisjonelle anskaffelser i forsvarssektoren. Forsvarsdepartementet skriver i IKT-strategien for forsvarssektoren under punkt 8.4 følgende:

«Det vil være viktig å forstå hvordan dagens prosesser, organisering og kultur knyttet til investeringer påvirker, og i noen tilfeller hindrer, innføring av ny teknologi. Dagens inndeling i drifts- og investeringsbudsjett, og hvordan IKT-prosjekter plasseres i de ulike kategoriene, er ikke hensiktsmessig. Inndelingen er ikke tilpasset den teknologiske endringstakten. Det er også lang ledetid ved gjennomføring av IKT-prosjekter. Dette forårsakes blant annet av lite smidig bruk av sektorens investeringsprosess, PRINSIX. Utprøvning av ny teknologi i forkant av investeringer blir viktigere fremover.»

Komiteen viser til at forsvarsministeren i sitt svar til Riksrevisjonen mener at strategien står seg som svært relevant i møte med Riksrevisjonens kritikk. Komiteen legger til grunn at Forsvarsdepartementet og forsvarssektoren sørger for at prosesser, organisering og kultur rundt investeringer og drift bidrar til at Forsvaret følger den teknologiske utviklingen på en måte som underbygger operativ evne.

Komiteen viser også til at IKT-strategiens strategiske mål om å være fremtidsrettet og nytenkende løfter frem kompetanse, kultur og styring. Riksrevisjonen har pekt på at mangel på kompetanse har medvirket til at forsvarssektoren ikke har klart å løse mange av utfordringene, og har anbefalt departementet å vurdere å rekruttere, utvikle og beholde nødvendig fagkompetanse på IKT-området. Komiteen understreker behovet for at Forsvaret, inkludert Forsvarets ledelse, er organisert på en måte som bygger kompetanse og kultur for å nå målsettingene fastsatt av Stortinget.

Komiteen viser til at forsvarsminister Bjørn Arild Gram i høringen pekte på at sektoren sliter med for utydelig ansvarsdeling og manglende gjennomføringsevne:

«Først til styringsutfordringene i sektoren. Jeg mener at dette går til kjernen også av det som Riksrevisjonen belyser i sin rapport. Etter en tid i Forsvarsdepartementet må jeg konstatere at sektoren sliter med for utydelig ansvarsdeling og manglende gjennomføringsevne. Dette har også konsekvenser for IKT-området. Innenfor rammen av regjeringens tillitsreform ønsker jeg å etablere en styringsmodell for forsvarssektoren som tydeligere plasserer ansvar og rydder opp i ansvarsdeling og grensesnitt mellom de ulike aktørene i sektoren.

Jeg registrerer at det i 2021 ble gitt et større ansvar til forsvarssjefen for den strategiske styringen av IKT-området. Hensikten var å forbedre integreringen av IKT-utviklingen i Forsvarets egen virksomhetsstyring. Gjennom nye retningslinjer for investeringer i forsvarssektoren fikk forsvarssjefen også en rolle som programeier for investeringstiltakene innenfor IKT. Jeg mener at det var en utvikling i riktig retning å gi forsvarssjefen rollen som premissgiver på IKT-området, men ikke tilstrekkelig. Det er behov for å gå enda mer grunnleggende til verks – derfor initiativet til å etablere en ny styringsmodell og rydde i grensesnitt. På IKT-området har ansvaret siden 2016 vært delt mellom Forsvaret ved Cyberforsvaret og Forsvarsmateriell. Det er mye som taler for at Forsvaret igjen skal få et mer helhetlig ansvar.»

Komiteen understreker behovet for å etablere en styringsmodell for forsvarssektoren med tydeligere ansvar og myndighet og at Forsvaret og forsvarssjefen gis et mer helhetlig ansvar.

Komiteen viser til at det innenfor IKT er særlig tette bånd mellom investering, drift og vedlikehold, noe som det også pekes på i IKT-strategien for forsvarssektoren av 27. mars 2019. Komiteen viser til at forsvarssjef general Eirik Kristoffersen uttalte følgende i høringen:

«Forsvarsmateriell har en tydelig rolle innenfor anskaffelse og avhending av materiell. Det som er utfordringen, er mellomfasen der vi skal drifte, forvalte og utvikle materiellet og IKT-en. Der mener jeg det er potensial for at Forsvaret får en tydeligere rolle.»

Sjef Cyberforsvaret Halvor Johansen sa følgende til komiteen i høringen:

«Det har blitt berørt av både tidligere og nåværende forsvarssjef, så jeg skal ikke gjenta det, men det jeg kanskje vil trekke fram, er den kompleksiteten innenfor IKT-områder som gjør at prosessene må være veldig tett koordinert og godt samordnet for at det skal fungere.

Utviklingen innenfor IKT går veldig fort, og vi er svært avhengig av at utvikling, drift og vedlikehold samordnes og koordineres på en veldig god måte.»

Komiteen merker seg at Forsvarsdepartementet i Meld. St. 10 (2021–2022) Prioriterte endringer, status og tiltak i forsvarssektoren har understreket at risikoen for forsinkelser i IKT-investeringene fremdeles er høy:

«IKT-området i sektoren er preget av utvikling og omfattende satsinger. Regjeringen vurderer at risikoen for forsinkelser i IKT-investeringene fremdeles er høy. Eventuelle forsinkelser vil kunne ha vesentlig negativ effekt på operativ evne, herunder kommando- og kontrollsystemer.»

Det er vesentlig risiko knyttet til den pågående IKT-satsingen i Mime og MAST

Komiteen viser til at statsråden i sitt svar til Riksrevisjonen fremhever virksomhetsprogrammene Mime, som skal modernisere Forsvarets kampnære IKT, og MAST, som skal modernisere Forsvarets IKT-plattformer og gi dem tilgang på skytjenester, som løsningen på flere av manglene som Riksrevisjonen påpeker. Begge programmene hviler på strategiske samarbeid, hvor oppgaver innen drift, forvaltning og vedlikehold overdras til sivile leverandører.

Komiteen viser til at sentrale spørsmål rundt programmene ikke er avklart, og at dette utgjør en risiko for ytterligere forsinkelser og manglende gevinstrealisering i programmene. Komiteen viser videre til følgende uttalelse i Riksrevisjonens oppsummering:

«Beslutningen om å gå i dialog om strategisk partnerskap med sivile leverandører før de folkerettslige konsekvensene av det planlagte samarbeidet er avklart medfører risiko for at forhandlinger og eventuelle avtaler ikke reflekterer det reelle handlingsrommet og behovet i sektoren.»

Komiteen deler Riksrevisjonens vurdering av at en folkerettslig avklaring er nødvendig for å kunne fastsette de sivile leverandørenes forpliktelser overfor Forsvaret ved krise og krig og dermed Forsvarets tilgang på nødvendig IKT-støtte. Komiteen imøteser en slik avklaring fra regjeringen.

Komiteen viser til at programorganisasjonen for Mime og MAST så sent som ett år etter den formelle oppstarten av Mime ga uttrykk til Riksrevisjonen for at den mangler verktøyene som trengs for å gjennomføre programmet som forutsatt.

Komiteen viser videre til at Forsvaret har besluttet å avlyse konkurransen om strategisk partnerskap sett i lys av nye vurderinger, som opplyst om i forsvarsministerens brev til komiteen av 24. februar 2023.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Sosialistisk Venstreparti, Rødt og Venstre viser til at forsvarsministeren fastslår at målsettingene knyttet til MAST ligger fast. Forsvarsministeren skriver:

«Dialogen med leverandørene og nye vurderinger har ført til flere justeringer av både innhold og omfang. Nye risikovurderinger også i lys av den sikkerhetspolitiske situasjonen gjør at Forsvarets vurdering nå er at det ikke skal gjennomføres en driftsoverføring av dagens systemer og tjenester. Forsvaret har opplyst at samlet er endringene så store at de går ut over de rammene som er satt for konkurransen og at anskaffelsen derfor nå er avlyst.»

Et annet flertall, medlemmene fra Arbeiderpartiet, Senterpartiet, Sosialistisk Venstreparti og Rødt, har tillit til at Forsvaret her har gjort en klok vurdering, og understreker viktigheten av forsvarsministerens siste setning:

«Ambisjonene knyttet til MAST ligger fast og jeg forventer at Forsvaret leverer på målene i programmet.»

Komiteen noterer seg at Riksrevisjonen mener at funnene i undersøkelsen er av en slik alvorlighetsgrad at Riksrevisjonen vil følge opp undersøkelsen, herunder Mime og MAST, ett til to år etter Stortingets behandling.

Riksrevisjonen anbefaler at Forsvarsdepartementet

- følger opp arbeidet med å få en fullstendig oversikt over informasjonssystemer i Forsvaret, og at denne blir brukt som grunnlag for Forsvarets styring og investeringer på IKT-området
- sørger for at Forsvaret og Forsvarsmateriell intensiverer arbeidet med variantbegrensning av Forsvarets informasjonssystemer
- i dialog med Forsvaret og Forsvarsmateriell sikrer løsninger for kommunikasjon og informasjonsutveksling som raskere gir full utnyttelse av kapasiteter ved anskaffelser av nytt materiell
- følger opp at sikkerhetsstyringen styrkes og at informasjonssikkerheten ivaretas i nye og eksisterende informasjonssystemer i Forsvaret
- styrker Forsvarets evne til å oppdage og stanse digitale angrep
- sørger for at Forsvarsmateriell og Forsvaret ivaretar nødvendig framdrift og gevinstrealisering i programmene Mime og MAST
- følger opp arbeidet med å avklare ansvaret mellom etatene i forsvarssektoren
- vurderer ytterligere tiltak for å rekruttere, utvikle og beholde nødvendig fagkompetanse på IKT-området i forsvarssektoren

Komiteen slutter seg til Riksrevisjonens anbefalinger, men registrerer at spørsmålet om framdrift og gevinstrealisering i Mime og MAST berører politiske spørsmål om hvordan disse programmene er organisert, som partigruppene har delte meninger om.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, viser til at Svendsen-

utvalget la frem sin rapport «Økt evne til å kombinere menneske og teknologi – Veier mot et høyteknologisk forsvar» 24. juni 2020. Utvalget peker på utfordringer ved dagens system og kommer med en nåtidsbeskrivelse. I tillegg kommer de med en rekke anbefalinger om hvordan Forsvaret, Forsvarsmateriell og resten av forsvarsorganisasjonen bør utvikles. Flertallet viser til at en del av utvalgets observasjoner og anbefalinger er relevante for den videre oppfølgingen av Riksrevisjonens rapport og for Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner.

På lik linje med Riksrevisjonen anbefaler utvalget å øke tilgangen på relevant kompetanse og styrke insentiver for å beholde kompetansen. Stortinget har, som påpekt av Riksrevisjonen, sluttet seg til at personellet er en avgjørende innsatsfaktor for forsvarssektoren, og at sektoren må ha evne til å rekruttere, anvende, beholde og utvikle den kompetansen den trenger. Riksrevisjonen merket seg at Svendsen-utvalget påpekte at Forsvaret ikke hadde klart å henge med i utviklingen eller evnet å omstille seg i takt med behovet for ny kompetanse for å utnytte teknologien og møte den økende trusselen i det digitale rom. Riksrevisjonen omtalte dette som bekymringsfullt.

Komiteens medlemmer fra Sosialistisk Venstreparti og Rødt viser til at både forbundsleder Torbjørn Bongo fra Norges offisers- og spesialistforbund og leder Jens Bernhard Jahren fra Befalets Fellesorganisasjon i omtalen av programmet MAST i høringen understreket at driftsansvaret ikke bør overlates til strategiske samarbeidspartnere.

I høringen uttalte Bongo følgende:

«Det jeg er mest kritisk til, er at vi eventuelt skal outsource driftsansvaret fra Forsvaret og over til en privat aktør. Det mener jeg vi ikke skal gjøre. De må gjerne støtte oss i å utvikle, ta i bruk og videreutvikle teknologien, men selve driftsansvaret bør forbli hos Forsvaret […] Det som er viktigst med MAST nå, er at vi sørger for at driftsansvaret forblir i forsvarssektoren.»

Jahren uttalte følgende i høringen:

«Vi mener det er viktig at det forblir et strategisk partnerskap, og at man ikke f. eks. overtar driftsoppgaver. For idet man begynner å overta for mange driftsoppgaver, får man veldig lett bindinger hvor det etter hvert er nesten umulig å komme seg ut, og da blir det noe annet enn det som var tenkt.»

Disse medlemmer forventer at forsvarsministeren sørger for at de tillitsvalgtes oppfordring blir tatt til følge i programmene MAST og Mime.

Komiteens medlemmer fra Høyre, Fremskrittspartiet og Venstre har den bestemte mening at Forsvaret ikke vil evne å realisere effektive og sikre informasjonssystemer som understøtter Forsvarets operative evne uten å benytte seg av strategisk partnerskap med privat næringsliv. Det er hverken realistisk eller ønskelig at Forsvaret skal bygge kompetanse på et høyt nok nivå – kvalitativt eller kvantitativt – internt i egen organisasjon. Det er derimot både en ønskelig og realistisk forventning at Forsvaret skal evne å forvalte samarbeid med privat næringsliv på en forutsigbar, effektiv og tillitvekkende måte.

Komiteens medlem fra Venstre mener at både Riksrevisjonens rapport og informasjonen om Forsvaret og Forsvarsmateriells avlysing av MAST-programmet vitner om at forsvarssektoren ikke lever opp til disse forventningene.

Dette medlem registrerer at det i Riksrevisjonens rapport benyttes en noe uklar ordlyd i omtalen av Forsvarets evne til å oppdage og håndtere digitale angrep. Det skrives at «Riksrevisjonen mener det er alvorlig at Forsvarets evne til å oppdage og håndtere digitale angrep er begrenset ved et forhøyet trusselnivå». Basert på Riksrevisjonens øvrige redegjørelse legger dette medlem til grunn at Riksrevisjonen i hovedsak refererer til Forsvarets evne til å oppdage og håndtere digitale angrep mot egne datasystemer og egen infrastruktur. Dette medlem mener like fullt at påstanden kan leses som at Forsvaret har begrenset evne til å håndtere digitale angrep mot norske mål som sådan, enten de befinner seg på sivile eller militære datasystemer og infrastruktur. Dette er imidlertid et arbeid som både privat næringsliv, sivile offentlige aktører og deler av Forsvaret som ikke er vurdert i Riksrevisjonens rapport, har sentrale roller i. Dette medlem vil understreke at dette medlem i alle tilfeller deler Riksrevisjonens kritikk på dette punkt.

4. Komiteens tilråding

Komiteen har for øvrig ingen merknader, viser til dokumentet og råder Stortinget til å gjøre følgende

vedtak:

Dokument 3:3 (2022–2023) – Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner – vedlegges protokollen.

Oslo, i kontroll- og konstitusjonskomiteen, den 28. mars 2023

Peter Frølich
leder

Seher Aydar
ordfører

STORTINGET

VEDLEGG 1

Statsråd Bjørn Arild Gram
Forsvarsdepartementet
Pb. 8126 Dep.
0032 Oslo

Vår ref.:	Deres ref.:	Dato:
2022/3750		21.02.2023

Vedr. Dokument 3:3 (2022-2023)

Kontroll- og konstitusjonskomiteen viser til behandlingen av Dokument 3:3 (2022-2023) - Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner.

Komiteen viser til pressemelding fra Forsvaret 13. februar 2023 med tittelen *Endrer planene for gjennomføring av MAST-programmet*. Av pressemeldingen fremgår det:

> «Etter nye vurderinger har Forsvaret besluttet at MAST-programmet (Militær anvendelse av skytjenester) ikke kan gjennomføre en driftsoverføring av dagens systemer og tjenester til en strategisk partner slik situasjonen er i dag.»

Komiteen ber om en redegjørelse for hva som er bakgrunnen for beslutningen og hvordan endringen påvirker statsrådens arbeid med å løse utfordringene Riksrevisjonen har identifisert i Dokument 3:3 (2022–2023). Komiteen stiller følgende spørsmål:

1. Hvorfor har Forsvaret besluttet å endre gjennomføringen av program MAST?
2. Endrer avlysningen ambisjonsnivået knyttet til MAST?
3. Hvem har tatt beslutning om å avlyse konkurransen, samt ikke gjennomføre utsetting av dagens drift?
4. Mener statsråden at avlysning av konkurransen er riktig sett i lys av Riksrevisjonens rapport?

Av hensyn til den videre fremdrift i saken, ber komiteen om svar innen fredag 24. februar 2023.

Kontroll- og konstitusjonskomiteen
Stortinget
Postboks 1700 Sentrum
NO-0026 OSLO

Tlf. 23 31 30 50

www.stortinget.no

Med vennlig hilsen
Kontroll- og konstitusjonskomiteen

Peter Frølich
Komitéleder

VEDLEGG 2

DET KONGELIGE
FORSVARSDEPARTEMENT

Statsråden

Kontroll- og konstitusjonskomiteen
Stortinget
0026 OSLO

Deres ref.:	Vår ref.:	Dato:
22/3750	2022/1082-14/FD III 2/LIST	24.02.2023

Brev fra kontroll- og konstitusjonskomiteen vedr. MAST

Viser til spørsmål fra komiteen 21.februar vedrørende spørsmål knyttet til beslutningen om avlyse konkurransen knyttet til program MAST.

Under følger svar på de fire spørsmålene fra komiteen:

1. Hvorfor har Forsvaret besluttet å endre gjennomføringen av program MAST?

Program MAST skal etablere ny plattform og løsninger, og i utviklingen av dette er det behov for samarbeid med næringslivet. Gjennom en konkurransepreget dialog med tre tilbydere har Forsvaret siden januar 2021 jobbet for å finne en strategisk partner som både skulle ta over og forbedre driften av flere av dagens systemer og tjenester, og samtidig ta ansvar for å utvikle fremtidens løsninger. Dialogen med leverandørene og nye vurderinger har ført til flere justeringer av både innhold og omfang. Nye risikovurderinger også i lys av den sikkerhetspolitiske situasjonen gjør at Forsvarets vurdering nå er at det ikke skal gjennomføres en driftsoverføring av dagens systemer og tjenester. Forsvaret har opplyst at samlet er endringene så store at de går ut over de rammene som var satt for konkurransen og at anskaffelsen derfor nå er avlyst.

2. Endrer avlysningen ambisjonsnivået knyttet til MAST?

Programmet MAST skal levere ny digital grunnmur, ny virksomhetsstyringsløsning, ny IKT-operasjonsmodell og utvikling og organisering av IKT i forsvarssektoren. Målet er å styrke Forsvarets evne til å løse sine oppgaver. Målsetningene knyttet til MAST ligger fast. Programmet skal fortsatt modernisere og styrke grunnmuren i Forsvarets IKT, og sørge for at videre digitalisering understøttes gjennom en modernisering av Forsvarets IKT-plattformer.

Postadresse: Postboks 8126 Dep., 0032 Oslo
Kontoradresse: Glacisgata 1, Oslo
Telefon: 23 09 80 00
Org.nr.: 972 417 823

3. Hvem har tatt beslutning om å avlyse konkurransen, samt ikke gjennomføre utsetting av dagens drift?

Ansvaret for program MAST er delegert til Forsvaret gjennom et mandat fra departementet. Forsvaret har fattet beslutningen om å avlyse konkurransen om strategisk partnerskap sett i lys av nye vurderinger. Dette er i tråd med delegert myndighet til å inngå avtaler om strategisk partnerskap.

4. Mener statsråden at avlysning av konkurransen er riktig sett i lys av Riksrevisjonens rapport?

Som jeg har redegjort for i min uttalelse til Dokument 3:3 (2022-2023), står forsvarssektoren overfor en omfattende omstilling og modernisering. Det er i denne prosessen nødvendig at forsvarssektoren har tilgang til oppdatert teknologi, løsninger og kompetanse på områder der industrien er ledende. For å oppnå dette vurderes det også strategisk samarbeid med en eller flere samarbeidspartnere, for eksempel NATO, allierte, næringslivet og andre statlige virksomheter.

Forsvaret har foretatt en fornyet vurdering av risikoen ved å overføre drift av dagens systemer og tjenester til en strategisk partner i program MAST, og Forsvaret har konkludert med at dette ikke bør gjøres. Jeg legger til grunn Forsvarets og Forsvarsmateriells merkantile vurdering om at endringene det er behov for å gjøre i MAST-programmet ikke kan håndteres innenfor rammene av den utlyste konkurransen. Med de vurderingene Forsvaret har gjort, mener jeg det nå er riktig å endre strategien for gjennomføring av MAST-programmet.

Sårbarheter i Forsvarets systemer kan i en forverret sikkerhetssituasjon gi større konsekvenser. Det er derfor riktig å se på nytt hvordan risikoreduserende tiltak kan gjennomføres på en mest effektiv måte. Det inkluderer også å styrke kompetansen internt i Forsvaret og styringen av IKT- prosessene i sektoren

Ambisjonene knyttet til MAST ligger fast og jeg forventer at Forsvaret leverer på målene i programmet.

Med hilsen

Bjørn Arild Gram

Dokumentet er elektronisk godkjent og signert, og har derfor ikke håndskrevne signaturer.

STORTINGET

VEDLEGG 3

Statsråd Bjørn Arild Gram
Forsvarsdepartementet
Postboks 8126 Dep
0032 Oslo

Vår ref.:	Deres ref.:	Dato:
2022/3750		14.03.2023

Vedr. Dokument 3:3 (2022-2023)

Kontroll- og konstitusjonskomiteen viser til statsrådens svarbrev av 24. februar 2023 vedrørende MAST-programmet og har følgende oppfølgingsspørsmål:

1. Hvilke endringer oppsto i anbudsprosessen som medførte at endringene gikk utover rammene som var satt for anskaffelsen, og var det nødvendig å avlyse anskaffelsen for å kunne ta hensyn til disse endringene?

2. Kan statsråden bekrefte at beslutningen ikke er begrunnet i synet på samarbeid mellom forsvarssektoren og sivil sektor og næringslivet?

3. Hvordan planlegger statsråden å arbeide – og sikre nødvendig framdrift – for at målene som lå til grunn for program MAST nås etter at det er endringer i planene for gjennomføringen av MAST-programmet?

Komiteen ber om svar innen 21. mars 2023.

Med vennlig hilsen
Kontroll- og konstitusjonskomiteen

Lubna Boby Jaffery
Første nestleder

Kontroll- og konstitusjonskomiteen
Stortinget
Postboks 1700 Sentrum
NO-0026 OSLO

Tlf. 23 31 30 50

www.stortinget.no

VEDLEGG 4

DET KONGELIGE
FORSVARSDEPARTEMENT

Statsråden

Stortingets president

Deres ref.:	Vår ref.:	Dato:
	2023/606-2/FD III 2/LIST	21.03.2023

Vedrørende Dokument 3:3 (2022-2023) vedr. MAST

Viser til spørsmål fra komiteen 14.mars vedrørende oppfølgingsspørsmål knyttet til beslutningen om avlyse konkurransen knyttet til program MAST.

Under følger svar på de tre spørsmålene fra komiteen:

1. Hvilke endringer oppsto i anbudsprosessen som medførte at endringene gikk utover rammene som var satt for anskaffelsen, og var det nødvendig å avlyse anskaffelsen for å kunne ta hensyn til disse endringene?

   Jeg legger til grunn Forsvarets og Forsvarsmateriells merkantile vurdering om at endringene det er behov for å gjøre i MAST-programmet ikke kan håndteres innenfor rammene av den utlyste konkurransen. Forsvaret har opplyst at beslutningen om å ikke tjenesteutsette drift av dagens systemer som en del av startomfanget for konkurransen innebærer en så stor endring at den opprinnelige konkurransen måtte kanselleres.

2. Kan statsråden bekrefte at beslutningen ikke er begrunnet i synet på samarbeid mellom forsvarssektoren og sivil sektor?

   Det er Forsvaret som har tatt denne beslutningen. I etatsstyringsmøte mellom Forsvaret og departementet i desember orienterte Forsvaret om at det var usikkerhet knyttet til inngåelse av strategisk partnerskap for MAST. På bakgrunn av dette ba departementet Forsvaret, NSM og FMA om en redegjørelse for status i arbeidet og eventuell revidert strategi. Etatene ble også bedt om å synliggjøre ev. behov for endrede føringer fra departementet. Departementet ble gjennom svar på dette orientert om Forsvarets endringer knyttet til den aktuelle konkurransen og endringer i Forsvarets plan for å løse oppdraget. Beslutningen ble tatt på bakgrunn av den endrede sikkerhetssituasjonen kombinert med sikkerhetstilstanden i Forvarets

Postadresse: Postboks 8126 Dep., 0032 Oslo
Kontoradresse: Glacisgata 1, Oslo
Telefon: 23 09 80 00
Org.nr.: 972 417 823

systemer slik det blant annet fremkommer i rapporten fra Riksrevisjonen. Det har ikke blitt gitt endringer i oppdraget fra departementet.

3. Hvordan planlegger statsråden å arbeide – og sikre framdrift – for at målene som lå til grunn for program MAST nås etter at det er endringer i planene for gjennomføringen av MAST-programmet?

   Forsvarssjefen har de siste årene fått økt ansvar for IKT, både den strategiske styringen av IKT-området i sektoren, men også som programeier for investeringstiltakene innenfor IKT inkludert MAST. Jeg mener at det er en utvikling i riktig retning å gi Forsvarssjefen rollen som premissgiver på IKT-området. Sett i lys av funnene i Riksrevisjonens rapport ser jeg behov for å følge opp framdrift. Som jeg sa til komiteen har Forsvarsdepartementet i 2022 iverksatt forsterket styring på IKT-området, i form av særskilte styringsmøter og intensivert oppfølging av den strategiske IKT-utviklingen i Forsvaret. Forsvarets videre håndtering av MAST ambisjonene inngår i denne dialogen nå.

   Forsvaret har så langt opplyst at Forsvaret og FMA nå arbeider med å utarbeide en strategi og avklare styring av framtidige sivil(e) partner(e) før Forsvaret igjen henvender seg til markedet. Parallelt arbeides det med å ferdigstille utredninger for investeringsbeslutning for ny digital grunnmur og ny virksomhetsstyringsløsning.

Med hilsen

Bjørn Arild Gram

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets administrasjon