Riksrevisjonen

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

Ugradert versjon av dokument 3:6 (2024−2025)

Forside: Forsvaret / Anette Ask
ISBN 978-82-8229-612-0

Riksrevisjonen

Til Stortinget

Riksrevisjonen legger med dette fram Dokument 3:6 (2024−2025) *Oppfølging av Dokument 3:3 (2022−2023) Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner*.

Dette er en ugradert versjon av Dokument 3:6 (2024−2025) (BEGRENSET). 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. Dette gjelder også to av underpunktene i konklusjonene. Forsvarsdepartementet vurderer det som at dette dokumentet ikke inneholder gradert informasjon.

Dokumentet har følgende inndeling:

- Riksrevisjonens konklusjoner, utdyping av konklusjoner, statsrådens svar og Riksrevisjonens uttalelse til statsrådens svar
- Vedlegg 1: Riksrevisjonens brev til statsråden
- Vedlegg 2: Statsrådens svar

Riksrevisjonen, 13. februar 2025

For riksrevisorkollegiet

Karl Eirik Schjøtt-Pedersen
riksrevisor

Innhold

Riksrevisjonen kan gi kritikk etter disse tre alvorlighetsgradene:

1. **Sterkt kritikkverdig** er Riksrevisjonens sterkeste kritikk. Vi bruker dette kritikknivået når vi finner alvorlige svakheter, feil og mangler. Ofte vil disse kunne få svært store konsekvenser for enkeltmennesker eller samfunnet.
2. **Kritikkverdig** bruker vi når vi finner betydelige svakheter, feil og mangler som ofte vil kunne få moderate til store konsekvenser for enkeltmennesker eller samfunnet.
3. **Ikke tilfredsstillende** bruker vi når vi finner svakheter, feil og mangler, men som i mindre grad får direkte konsekvenser for enkeltmennesker eller samfunnet.

1 Innledning

Bakgrunnen for denne undersøkelsen er Dokument 3:3 (2022–2023) *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner.* Dokumentet med vedlagt rapport ble overlevert Stortinget i oktober 2022 og bygde i hovedsak på data fra perioden 2017–2020.

Målet med denne undersøkelsen har vært å vurdere om konklusjoner og anbefalinger i Dokument 3:3 (2022–2023) er fulgt opp av Forsvarsdepartementet og underliggende etater. Undersøkelsen omfatter perioden 2022–2024.

Riksrevisorkollegiets oversendelsesbrev til departementet 23. januar 2025 og statsrådens svar 3. februar 2025 følger som vedlegg.

2 Konklusjoner

Konklusjoner

- Samvirket mellom Forsvarets informasjonssystemer er blitt bedre.
  - Det er utviklet mekanismer for automatisert dataflyt mellom flere informasjonssystemer.
  - Kapasiteten for taktisk datalink (Link 16) er økt, men det er fortsatt utfordringer.
  - Arbeidet med variantbegrensning av informasjonssystemer er utfordrende og tidkrevende.
  - Forsvaret jobber med å finne løsninger for kommunikasjon og informasjonsutveksling som raskere gir full utnyttelse av nytt materiell.
- Sikkerhetstilstanden til Forsvarets informasjonssystemer er fortsatt alvorlig, selv om det er iverksatt tiltak.
  - Forsvaret har fått bedre oversikt over sine informasjonssystemer, men det er fortsatt behov for avklaringer.
  - Forsvaret har fortsatt skjermingsverdige informasjonssystemer som ikke tilfredsstiller kravene i sikkerhetsloven.
  - Forsvarets sikkerhetsstyring har en svak positiv utvikling, men det er fortsatt mangler.
  - Forsvarets evne til å oppdage og stanse digitale angrep er blitt bedre, men det er fortsatt kapasitetsutfordringer.
- Det er fortsatt betydelig risiko knyttet til IKT-satsingen i programmene Mime og MAST.
  - Det har tatt tid å få opp leveransekapasiteten i Mime, og strategisk partnerskap fungerer ikke etter intensjonen.
  - Anskaffelsen av en strategisk partner i MAST er kansellert, og det er usikkerhet knyttet til gjennomføringen av programmet.
- Forsvarsdepartementet har iverksatt en styringsreform, som også omfatter IKT-området.
  - Ansvar og myndighet mellom etatene er forsøkt avklart i ny styringsmodell.
  - Forsvaret har fått mer helhetlig ansvar og myndighet på IKT-området.
  - Personell og kompetanse er fortsatt en utfordring, men det er bedring på enkelte områder.

Riksrevisjonen følger saken videre

3 Overordnet vurdering

Riksrevisjonens undersøkelse fra 2022 pekte både på sårbarheter i sikkerheten og mangler i samvirket mellom Forsvarets informasjonssystemer og på konsekvensene dette kunne ha for Forsvarets operative evne.

Riksrevisjonen registrerer at Forsvarsdepartementet, Forsvaret og Forsvarsmateriell har iverksatt en rekke tiltak, og at tiltakene følges opp systematisk av departementet og etatene.

Riksrevisjonen merker seg at Forsvarsdepartementet samlet sett fortsatt vurderer situasjonen som alvorlig. Departementet understreker at flere av de kritikkverdige forholdene som Riksrevisjonen har pekt på, er avhengig av større moderniseringsprosjekter som det vil ta år å gjennomføre.

Riksrevisjonen merker seg videre at sektoren har oppnådd forbedringer på flere områder. Det gjelder spesielt evnen til samvirke mellom informasjonssystemer og evnen til å oppdage og stanse digitale angrep. Sikkerhetstilstanden til Forsvarets informasjonssystemer har imidlertid fortsatt mangler. Det er fortsatt også betydelig risiko ved de to programmene Mime og MAST, som på sikt er ment å løse mange av utfordringene på IKT-området i forsvarssektoren. En ny digital grunnmur er en forutsetning for tilfredsstillende funksjonalitet og sikkerhet i Forsvarets IKT-systemer, og har stor betydning for Forsvarets operative evne.

Gjennom et reformarbeid i forsvarssektoren er det etablert en ny styringsmodell på IKT-området i Forsvaret. Modellen er under implementering og adresserer flere av utfordringene som har vært påpekt når det gjelder styring på området, men det er foreløpig for tidlig å si noe om effekten av denne.

Området er komplekst, og det er kort tid siden forrige undersøkelse ble rapportert til Stortinget. Dette har betydning for hvordan vi vurderer både omfanget av iverksatte tiltak, og når det er mulig å se effekter av tiltakene. Riksrevisjonen merker seg at tiltakene som er iverksatt har ført til forbedringer på flere områder. Selv om situasjonen fortsatt er alvorlig, fremmer Riksrevisjonen derfor ikke kritikk til departementets oppfølging. Riksrevisjonen følger saken videre.

4 Opprinnelig undersøkelse om Forsvarets informasjonssystemer

4.1 Riksrevisjonens konklusjoner og anbefalinger

Riksrevisjonen overleverte 4. oktober 2022 Dokument 3:3 (2022−2023) *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner* med tilhørende hovedanalyserapport til Stortinget. Både dokumentet og rapporten var gradert KONFIDENSIELT. Riksrevisjonen utarbeidet også et ugradert Dokument 3. Målet med undersøkelsen var å vurdere om Forsvarets informasjonssystemer understøttet Forsvarets operative evne gjennom effektiv og sikker kommunikasjon og informasjonsutveksling i operasjoner, og om styringen av IKT i forsvarssektoren hadde lagt til rette for effektive og sikre systemer.

Informasjonssystemer
I Dokument 3:3 (2022−2023) brukte vi begrepet kommando- og kontroll-informasjonssystemer om informasjonssystemer til bruk i operasjoner. I dette dokumentet bruker vi begrepet informasjons-systemer, om de samme systemene.

Evnen til samhandling i operasjoner avhenger av informasjonssystemer som kan samvirke og fungere med hverandre for å levere informasjon og tjenester til, og ta imot informasjon og tjenester fra, andre systemer. Forsvarets informasjonssystemer må også beskyttes mot sikkerhetstruende virksomhet. Med sikkerhetstruende virksomhet menes 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.

Riksrevisjonens hovedfunn ble gjengitt slik i ugradert versjon:

- Mangler i samvirket mellom Forsvarets informasjonssystemer kan påvirke Forsvarets operative evne.
    - Informasjonssystemer med ulik teknologi påvirker mulighetene for samhandling.
    - Ulike sikkerhetsdomener påvirker informasjonsutvekslingen mellom systemer.
    - Mangler ved taktisk datalink reduserer mulighetene for å utveksle data.
- Sårbarheter i sikkerheten i Forsvarets informasjonssystemer gir risiko for svekket operativ evne.
    - Mangler i oversikt og dokumentasjon på IKT-området påvirker muligheten for å ivareta sikkerheten i systemene.
    - 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 programmene Mime og MAST.

Med bakgrunn i dette anbefalte Riksrevisjonen 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 anskaffelse 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

4.2 Stortingets behandling av saken

Kontroll- og konstitusjonskomiteen avholdt 16. januar 2023 en lukket kontrollhøring, der både nåværende og tidligere politisk og militær ledelse møtte.

Kontroll- og konstitusjonskomiteen avga sin ugraderte innstilling den 28. mars 2023, jf. Innst. 259 S (2022−2023). Stortinget behandlet saken den 18. april 2023.

Komiteen viser til at Riksrevisjonen har undersøkt perioden 2017−2020, og at den sikkerhetspolitiske situasjonen er vesentlig forverret for Norge og våre allierte siden 2020. Samtidig foregår det et teknologikappløp mellom verdens maktsentra. Komiteen mener at disse forholdene danner et svært alvorspreget bakteppe for rapportens funn, konklusjoner og anbefalinger som er verdt å understreke.

4.2.1 Mangler i samvirket mellom Forsvarets informasjonssystemer

Komiteen viser til at Riksrevisjonen finner mangler i samvirket mellom Forsvarets kommando- og kontrollinformasjonssystemer som kan påvirke Forsvarets operative evne. Komiteen mener at denne mangelen er desto mer alvorlig i lys av den gjeldende sikkerhetspolitiske situasjonen.

Komiteen deler Forsvarets vurdering av at utfasing av informasjonssystemer må prioriteres, og understreker 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 at det også 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 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.

4.2.2 Sårbarheter i sikkerheten i Forsvarets informasjonssystemer

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 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 i Cyberforsvaret som Stortinget har forutsatt i behandlingen av langtidsplanen for forsvarssektoren 2021−2024, jf. Innst 87 S (2020−2021). Komiteen registrerer at forsvarsministeren svarer at full operativ kapasitet i responsmiljøet Cyberforsvarets cybersikkerhetssenter (MilCERT) blir 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.

4.2.3 Forsvarsdepartementet har ikke greid å realisere effektive og sikre informasjonssystemer

Komiteen viser til at IKT ble pekt på som et satsingsområde i langtidsplanen for forsvarssektoren 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 understreker 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. 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 Riksrevisjonenes 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 ansvarsforhold og mangel på kompetanse som 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 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 forskningsinstitutts (FFI) uttalelser i høringen og merker seg hvordan FFIs beskrivelse av situasjonen samsvarer med Riksrevisjonens funn. Komiteen merker seg også at FFIs beskrivelse av utfordringer knyttet til avklaring av roller og ansvar, sammen med kompetanseutfordringer, ble støttet av tillitsvalgte, av Nasjonal sikkerhetsmyndighet og av nåværende og tidligere forsvarssjefer i høringen.

Komiteen viser til «IKT-strategi for forsvarssektoren» der departementet gir 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 kjent i sektoren. 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 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 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 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-investeringer fremdeles er høy.

4.2.4 Risiko knyttet til IKT-satsingen i Mime og MAST

Komiteen viser til at statsråden i sitt svar til Riksrevisjonen trekker fram 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 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 for at de 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 i forsvarsministerens brev til komiteen datert 24. februar 2023.

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.

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.

5 Oppfølging av undersøkelsen av Forsvarets informasjonssystemer

5.1 Riksrevisjonens oppfølging

Riksrevisjonen har fulgt opp undersøkelsen som ble rapportert i 2022. Oppfølgingen er avgrenset til å omfatte konklusjonene og anbefalingene i den opprinnelige undersøkelsen og områdene som Stortinget har lagt særlig vekt på eller stilt forventninger til.

Vi har hentet inn informasjon fra Forsvaret, Forsvarsmateriell og Forsvarsdepartementet om status og utvikling i perioden 2022–2024.

Vi har gjennomgått

- tildelingsbrev til Forsvaret og Forsvarsmateriell
- Forsvarets og Forsvarsmateriells tertial- og årsrapporter
- referater fra etatsstyringsmøter med Forsvaret og Forsvarsmateriell
- årlige tilstandsrapporter fra Forsvarets sikkerhetsavdeling
- eksterne rapporter om programmene Mime og MAST
- rapport fra Forsvarsdepartementets internrevisjon
- strategiske styringsdokumenter fra Forsvaret

I tillegg har vi gjennomført intervjuer med

- Forsvarsmateriell ved IKT-kapasiteter og programorganisasjonen Mime/MAST
- Forsvarsmateriells ledelse
- Cyberforsvaret
- Forsvarsstaben
- Forsvarsdepartementet

Riksrevisjonen har ikke gjennomført egne tester av systemenes funksjonalitet eller sikkerhet.

5.2 Forsvarsdepartementets og etatenes oppfølging

Forsvarsdepartementet, Forsvaret og Forsvarsmateriell har iverksatt en særskilt oppfølging av Riksrevisjonens undersøkelse om Forsvarets informasjonssystemer. Forsvaret og Forsvarsmateriell utarbeidet våren 2023 en tiltakspakke for å følge opp Riksrevisjonens konklusjoner og anbefalinger og orienterte departementet om denne i felles etatsstyringsmøte i juni 2023.[1]

Fra mars 2024 har både Forsvaret og departementet rapportert månedlig om status for tiltakene på oppdrag fra departementet. Riksrevisjonen har innhentet rapporteringen til og med september 2024.

[1] (B) Forsvarsdepartementet. (2023). *Referat fra etatsstyringsmøte med Forsvaret og FMA om IKT 16. juni 2023.*

Tiltakslisten er i kontinuerlig utvikling. Per november 2024 rapporterer Forsvaret på 34 tiltak og Forsvarsdepartementet på 29.[2]

Forsvarsdepartementet gjennomførte fra februar til juni 2024 en ekstern gjennomgang av program Mime for å kartlegge risiko og foreslå risikoreduserende tiltak for det videre arbeidet i programmet. Gjennomgangen følges opp av en tiltakspakke på samme måte som oppfølgingen av Riksrevisjonens rapport.[3]

Internrevisjonen i Forsvarsdepartementet har gjennomført en bekreftelsesrevisjon av interoperabilitet og sikkerhet i informasjonssystemer i Forsvaret, og påvirkningen dette har på Forsvarets operative evne. Revisjonen ble ferdig i oktober 2024.[4]

Forsvarsdepartementet har gjennom tildelingsbrev til Forsvaret og Forsvarsmateriell gitt styringssignaler og stilt krav på IKT-området. Dette er fulgt opp i rapportering og etatsstyringsmøter. I tildelingsbrevene til Forsvaret for 2022, 2023 og 2024 har departementet blant annet stilt krav om å kartlegge skjermingsverdige informasjonssystemer, og i 2024 stilte det også krav om variantbegrensning av disse. Departementet har stilt krav til Forsvaret om et forsvarlig sikkerhetsnivå og sikkerhetsgodkjenning av skjermingsverdige informasjonssystemer. Forsvaret er i tillegg bedt om å gjennomføre tiltak innenfor sikkerhetsstyring og IKT-sikkerhetsstyring. I tildelingsbrevet for 2024 står det også at Forsvaret skal sørge for nødvendig, hensiktsmessig og relevant fagkompetanse på IKT-området.

I tildelingsbrevene til Forsvarsmateriell for 2022, 2023 og 2024 er det stilt krav om at informasjonssystemene som etaten anskaffer, skal ha et forsvarlig sikkerhetsnivå og skal kunne godkjennes i henhold til kravene i sikkerhetsloven.

Forsvaret har utarbeidet en digital reguleringsplan (DRP) for å sette IKT-strategien for forsvarssektoren ut i livet og utøve strategisk IKT-styring. Planen trådte i kraft 15. februar 2023, og arbeidet skal pågå til og med 2028.[5]

Gjennom reformarbeidet Forsvarssektoren 24 (F24) er det utviklet en ny modell for styring på IKT-området i forsvarssektoren. Dette er nærmere omtalt i punkt. 6.4.

[2] (B) Intervju med Forsvarsdepartementet 8. november 2024.
[3] (B) Forsvarsdepartementet. (2024). *Risikoreduserende helsesjekk av program Mime;* (B) intervju med Forsvarsdepartementet 8. november 2024.
[4] (B) Intervju med Forsvarsdepartementet 8. november 2024.
[5] (B) Forsvaret. (2023). *Digital reguleringsplan (DRP) for forsvarssektoren.*

6 Utdyping av konklusjoner

6.1 Samvirket mellom Forsvarets informasjonssystemer er blitt bedre

6.1.1 Det er utviklet mekanismer for automatisert dataflyt mellom flere informasjonssystemer

Forsvarets operative evne avhenger av muligheten til å samhandle i operasjoner, på tvers av enheter i Forsvaret, i kommandolinjen nasjonalt og med NATO og allierte. Slik fellesoperativ samhandling avhenger av at informasjonssystemer virker effektivt sammen. Det vil si at de kan levere informasjon til, og ta imot informasjon fra, andre systemer.

En av hovedkonklusjonene i den opprinnelige undersøkelsen var at mangler i samvirket mellom informasjonssystemene kan påvirke Forsvarets operative evne. Manglene skyldtes et høyt antall informasjonssystemer med ulik og til dels utdatert teknologi og på ulike sikkerhetsdomener. Men også nye våpenplattformer, som fly, fartøyer og kjøretøy, var levert med informasjonssystemer som ikke virket sammen med Forsvarets eksisterende informasjonssystemer. Undersøkelsen pekte også på at mangler ved taktisk datalink (Link 16) reduserte mulighetene for å utveksle data mellom Forsvarets enheter.

Forsvarsmateriell, Cyberforsvaret og Forsvarsstaben oppgir alle i intervjuer at evnen til samvirke mellom informasjonssystemene er blitt betydelig bedre etter Riksrevisjonens undersøkelse.[6] Det er utviklet mekanismer for automatisert dataflyt mellom flere informasjonssystemer. Som eksempel viser Cyberforsvaret og Forsvarsstaben til forskjellen mellom øvelsene Trident Juncture i 2018 og Nordic Response i 2024, som viste at evnen til å utveksle informasjon mellom de relevante systemene er forbedret.[7]

Cyberforsvaret viser også til arbeidet som gjennomføres i regi av NATOs initiativ *Federated Mission Networking*, som er et rammeverk for å etablere samvirke innad i NATO. De enkelte medlemslandene befinner seg på ulike stadier i iverksettingen av NATOs rammeverk. NATO har hatt en undersøkelse om iverksettingen av *Federated Mission Networking* som viser at Norge ligger godt an.[8]

Evnen til å utveksle informasjon avhenger også av tilgjengelige kommunikasjonsbærere. Cyberforsvaret opplyser at antallet og utbredelsen av kommunikasjonsbærere, som satellittkommunikasjon, 5G og fiber, øker i Forsvaret.[9]

Kommunikasjonsbærere
Begrepet brukes om kommunikasjonsløsninger eller kommunikasjons-infrastruktur, som satellitt, 5G og fibernett.

[6] (B) Intervju med Forsvarsmateriell 23. august 2024; (B) intervju med Cyberforsvaret 3. september 2024; (B) intervju med ledelsen i Forsvarsmateriell 9.oktober 2024; (B) intervju med Forsvarsstaben 16. oktober 2024.
[7] (B) Intervju med Cyberforsvaret 3. september 2024.
[8] (B) Intervju med Cyberforsvaret 3. september 2024.
[9] (B) Intervju med Cyberforsvaret 3. september 2024.

Forsvarsdepartementets internrevisjon har i 2024 gjennomført en undersøkelse som bekrefter at Forsvarets informasjonssystemer har fått en forbedret interoperabilitet.[10]

Samtidig rapporterer Forsvaret i september 2024 at det opereres med for mange og ulike informasjonssystemer med begrenset interoperabilitet, og at det er systemer som ikke tilfredsstiller sikkerhetslovens krav. Forsvaret oppgir at statusen til IKT-systemene og bruksbegrensningene gitt av NSM som følge av sikkerhetstilstanden har konsekvenser for operative tjenester.[11]

Forsvarsdepartementet bekrefter i intervju at mekanismene for informasjonsutveksling er forbedret for flere informasjonssystemer og at dette har ført til økt interoperabilitet. Samtidig er det fortsatt utfordringer.[12]

Interoperabilitet
For at informasjonssystemer skal virke effektivt, må de være *interoperable*. Det innebærer at de må kunne samvirke og fungere med hverandre for å levere informasjon og tjenester til, og ta imot informasjon og tjenester, fra andre systemer.

6.1.2 Kapasiteten for taktisk datalink (Link 16) er økt, men det er fortsatt utfordringer

Taktisk datalink er en sentral komponent i Forsvarets infrastruktur for kommunikasjon som brukes til å utveksle taktiske data. Det inkluderer situasjonsbilde og sensor- og måldatainformasjon mellom to eller flere enheter i tilnærmet sanntid. Forsvaret bruker Link 16 til å utveksle data mellom fly, fartøyer og landstyrker. Datalink er blant annet viktig for kommunikasjon med kampflyene F-35 og de maritime patruljeflyene P-8 Poseidon.

Taktisk datalink brukes til å utveksle taktiske data, inkludert situasjonsbilde og sensor- og måldata-informasjon, mellom to eller flere enheter i tilnærmet sanntid. Forsvaret bruker Link 16 til å utveksle data mellom fly, fartøyer og landstyrker.

Riksrevisjonens undersøkelse avdekket mangler ved taktisk datalink som gjorde det utfordrende å utveksle informasjon mellom enheter i Forsvaret. Undersøkelsen viste også at det var flere planlagte og pågående prosjekter knyttet til oppgradering av taktisk datalink, men at det var forsinkelser og risiko for mangelfull koordinering mellom disse prosjektene.[13]

Ved behandlingen av Dokument 3:3 2022–2023) uttrykte Stortinget en forventning om at regjeringen sørger for at oppgraderingene av Link 16 får den forutsatte gevinsten.[14]

Både Forsvaret og Forsvarsmateriell bekrefter i intervju at situasjonen for taktisk datalink (Link 16) er forbedret. Kapasiteten er økt, men det er fortsatt utfordringer.[15]

6.1.3 Arbeidet med variantbegrensning av informasjonssystemer er utfordrende og tidkrevende

Riksrevisjonens undersøkelse avdekket at Forsvaret hadde et høyt antall informasjonssystemer med ulike tekniske løsninger til tross for at det lenge har vært et mål å redusere antallet ulike systemer gjennom såkalt variantbegrensning. Undersøkelsen viste også at mengden av systemer

[10] (B) Forsvarsdepartementet. (2024). *B30 - Tilstanden i sektoren etter Riksrevisjonens rapport om K2IS.*
[11] (B) Forsvaret (2024) Forsvarets halvårlige rapport 2024.
[12] (B) Intervju med Forsvarsdepartementet 8. november 2024.
[13] Dokument 3:3 (2022–2023) *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner.*
[14] Innst. 259 S (2022–2023) til Dokument 3:3 (2022–2023).
[15] (B) Intervju med Forsvarsmateriell 23. august 2024; (B) intervju med Cyberforsvaret 3. september 2024; (B) intervju med ledelsen i Forsvarsmateriell 9. oktober 2024; (B) intervju med Forsvarsstaben 16. oktober 2024.

bidrar til å gjøre samvirket mellom systemene vanskelig, og at det går ekstra ressurser til forvaltning og drift av systemene.

Riksrevisjonen anbefalte i Dokument 3:3 (2022−2023) Forsvarsdepartementet å sørge for at Forsvaret og Forsvarsmateriell intensiverer arbeidet med variantbegrensning av Forsvarets informasjonssystemer.

Forsvaret og Forsvarsmateriell opplyser at arbeidet med variantbegrensning er forsterket, og at det er utarbeidet en plan for gjennomføringen. Parallelt med utfasing av gamle informasjonssystemer pågår det konsolidering av systemer. Konsolidering er enten at funksjonalitet og IKT fra et system integreres i et annet, eller at funksjonalitet og IKT fra to eller flere systemer slås sammen. Dette bidrar til å øke interoperabiliteten.[16]

Men både Forsvarsmateriell og Cyberforsvaret viser til utfordringer i arbeidet med variantbegrensning og konsolidering. Forsvarsmateriell peker på utfordringer med personell, teknisk gjeld i eksisterende systemer og teknologi som er tett integrert med innarbeidede prosesser i Forsvaret.[17]

Forsvaret og Forsvarsmateriell viser til at de har unngått ytterligere variantøkning ved å integrere ny funksjonalitet og IKT på en eksisterende plattform. Samtidig øker risikoen når mer funksjonalitet og IKT samles på én plattform.[18]

Forsvarsstaben bekrefter at konsolidering og variantbegrensning er ressurskrevende og tar tid. Arbeidet prioriteres fortløpende ut fra kritiske behov, det unike systemets operative verdi og etterlevelse av NATO-krav. Nye systemer erstatter ikke alltid fullt ut eksisterende systemer. Det kan resultere i perioder med nødvendig overlapp inntil det gamle systemet kan fases ut.[19]

Både Forsvarsstaben og Forsvarsdepartementet trekker fram at forsvarssektoren fortsatt har mange IKT-systemer med teknisk gjeld, selv om det er iverksatt flere tiltak for å begrense antallet informasjonssystemer. Begge peker også på at modernisering av den digitale grunnmuren, som er det største og viktigste tiltaket, vil ta tid.[20] Modernisering av Forsvaret digitale grunnmur omtales i punkt 6.3.2.

6.1.4 Forsvaret jobber med å finne løsninger for kommunikasjon og informasjonsutveksling som raskere gir full utnyttelse av nytt materiell

Forsvaret har de senere årene anskaffet mye nytt materiell, og ifølge langtidsplanen skal forsvarssektoren gjennomføre omfattende investeringer i nytt materiell også i årene som kommer.

[16] (B) Intervju med Forsvarsmateriell 23. august 2024; (B) intervju med Cyberforsvaret 3. september 2024; (B) intervju med Forsvarsstaben 16. oktober 2024.
[17] (B) Intervju med Cyberforsvaret 3. september 2024.
[18] (B) Intervju med Forsvarsmateriell 23. august 2024; (B) intervju med Forsvarsstaben 16. oktober 2024.
[19] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[20] (B) intervju med Forsvarsstaben 16. oktober 2024, (B) intervju med Forsvarsdepartementet 8. november 2024.

Undersøkelsen fra 2022 viste at nye våpenplattformer ofte leveres med innebygde informasjonssystemer som ikke alltid kommuniserer med Forsvarets eksisterende informasjonssystemer. Det kan føre til at materiell ikke kan utnyttes optimalt, slik tilfellet var med kampflyene som ble levert med enkelte informasjonssystemer som ikke var interoperable med verken nasjonale systemer eller NATO-systemer.

Riksrevisjonen anbefalte i Dokument 3:3 (2022–2023) at Forsvarsdepartementet, i dialog med Forsvaret og Forsvarsmateriell, sikrer løsninger for kommunikasjon og informasjonsutveksling som raskere gir full utnyttelse av kapasiteter ved anskaffelse av nytt materiell.

Ifølge tildelingsbrevet for 2024 skal Forsvaret ha fokus på effekten fra IKT-tjenestene ved anskaffelse av nytt materiell.[21]

Forsvaret viser i halvårsrapporteringen i september 2024 til at de har fått mer ansvar for investeringsporteføljen, med IKT som delportefølje. Formålet er blant annet å oppnå full utnyttelse av kapasiteter og raskere effektrealisering ved nye anskaffelser.[22]

6.1.5 Riksrevisjonens vurdering

Riksrevisjonen merker seg at både aktørene i sektoren og Forsvarsdepartementets internrevisjon peker på at evnen til samvirke mellom Forsvarets informasjonssystemer til bruk i operasjoner er blitt bedre. Det er utviklet løsninger for sikker informasjonsutveksling både nasjonalt og med allierte. Utbredelse av bakkeinfrastruktur og terminaler for Link 16 er også økt, og det skal bli flere enheter gjennom pågående investeringsprosjekter. Samtidig øker også antallet og utbredelsen av kommunikasjonsbærere i Forsvaret.

Forsvaret har imidlertid fortsatt et høyt antall informasjonssystemer, som er krevende å forvalte og som påvirker evnen til samvirke. Riksrevisjonen merker seg at det er forsterket oppmerksomhet om variantbegrensning gjennom konsolidering og utfasing av systemer. Hovedutfordringen er imidlertid teknisk gjeld i porteføljen, noe som gjør arbeidet med modernisering både utfordrende og tidkrevende.

6.2 Sikkerhetstilstanden til Forsvarets informasjonssystemer er fortsatt alvorlig, selv om det er iverksatt tiltak

Riksrevisjonens undersøkelse viste at mangler i oversikt og dokumentasjon på IKT-området påvirker muligheten for å ivareta sikkerheten i informasjonssystemene. Undersøkelsen avdekket også at Forsvaret brukte skjermingsverdige informasjonssystemer som ikke var sikkerhetsgodkjent,

[21] (B) Forsvarsdepartementet. (2024). *Tildelingsbrev for Forsvaret 2024*, Styringsparameter 8 Sikkerhet og tilgjengelighet på IKT-tjenester.
[22] Forsvaret (2024) *Forsvarets halvårsrapport for 2024*.

og at det var svakheter i sikkerhetsstyringen. Det kom også fram at Forsvaret hadde mangler i evnen til å oppdage og stanse digitale angrep.

Riksrevisjonen anbefalte Forsvarsdepartementet å følge opp at sikkerhetsstyringen styrkes og at informasjonssikkerheten ivaretas i nye og eksisterende informasjonssystemer i Forsvaret. Riksrevisjonen anbefalte også departementet å styrke Forsvarets evne til å oppdage og stanse digitale angrep.

6.2.1 Forsvaret har fått bedre oversikt over sine informasjonssystemer, men det er fortsatt behov for avklaringer

Riksrevisjonens undersøkelse avdekket at Forsvaret ikke hadde god nok oversikt over informasjonssystemene sine. God oversikt over informasjonssystemene er en grunnleggende forutsetning for å kunne gjøre gode risikovurderinger og planlegge og gjennomføre effektive sikkerhetstiltak, slik sikkerhetsloven og Forsvarets eget regelverk krever.

Riksrevisjonen anbefalte Forsvarsdepartementet å følge opp arbeidet med å få en fullstendig oversikt over informasjonssystemene i Forsvaret, og at oversikten blir brukt som grunnlag for Forsvarets styring og investeringer på IKT-området.

Forsvaret har etablert en oversikt over Forsvarets informasjonssystemer. Riksrevisjonen har mottatt denne oversikten fra Forsvaret. Forsvarsstaben opplyser at Forsvaret har hatt en kritisk gjennomgang av hva som skal defineres som et informasjonssystem, og at det pågår en kartlegging av skjermingsverdighet og kritikalitet for hele porteføljen.[23]

Forsvarsstaben viser til at oversikten over informasjonssystemer kontinuerlig justeres og kvalitetssikres og derfor er i stadig endring. Det skyldes både endringer i hva som defineres som et informasjonssystem, konsolideringer og variantbegrensninger, og anskaffelse av nye strukturelementer og kapasiteter. Det er utfordrende og tidkrevende å etablere og opprettholde datakvaliteten i oversikten fordi systemporteføljen er så pass stor, det er et stort antall systemeiere og kompetansen er varierende.[24] Både Forsvarsstaben og Cyberforsvaret mener at definisjonen av et informasjonssystem ikke er tydelig.[25]

Forsvarets rapportering i perioden fra mars til september 2024 viser at det fortsatt er etterslep i oppdateringen av oversikten over informasjonssystemer.[26]

Riksrevisjonen pekte i undersøkelsen fra 2022 på at Forsvaret manglet en virksomhetsarkitektur. Forsvaret og Forsvarsmateriell viser til at Forsvarsstaben i ny styringsmodell har opprettet et IKT-arkitekturstyre med underliggende arkitekturråd i Cyberforsvaret og i Forsvarsmateriell IKT-

[23] B) Intervju med Forsvarsstaben 16. oktober 2024, (B) Forsvaret. (2024). *Forsvarets skjermingsverdige informasjonssystemer*. 8. oktober 2024.
[24] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[25] (B) Intervju med Forsvarsstaben 16. oktober 2024; (B) intervju med Cyberforsvaret 3. september 2024.
[26] (B) Forsvaret. (2024). *Rapportering på oppfølging av Riksrevisjonens rapport om Forsvarets informasjonssystemer*. Perioden mars 2024–september 2024.

kapasiteter. Sektoren har også opprettet en felles database der Forsvaret og Forsvarsmateriell legger inn data om systemene og applikasjonene.[27]

Riksrevisjonen påpekte i undersøkelsen fra 2022 at Forsvarsmateriell i liten grad hadde brukt sin myndighet til å føre kontroll med forsvarssektorens materiellforvaltning på IKT-området. Kontroll- og konstitusjonskomiteen mente at dette var kritikkverdig og uttrykte forventning om at regjeringen etablerer de rammene som trengs for at denne kontrollen utføres.[28]

Forsvarsmateriell oppgir at etter Stortingets behandling av Riksrevisjonens rapport er det prioritert å bruke tiden til å rette opp kritiske forhold framfor å gjøre kontrollaktiviteter utover et minimum for å ivareta krav i tildelingsbrev. Gjennom reformarbeidet Forsvarssektoren 24 har Forsvaret nå fått ansvar for å styre, drifte, vedlikeholde og utvikle Forsvarets IKT. Forsvarsmateriell skal ikke lenger ha ansvar for å føre kontroll med Forsvarets materiellforvaltning på IKT-området.[29]

Riksrevisjonen anbefalte også å bruke oversikten over informasjonssystemer som grunnlag for Forsvarets styring og investeringer på området.

Forsvarsstaben opplyser at oversikten over informasjonssystemene brukes som grunnlag for å planlegge og prioritere sikkerhetstiltak og for å følge opp sikkerhetstilstand og godkjenninger, og at Forsvaret skal starte arbeidet med å inkludere oversikten i den løpende porteføljestyrings- og prioriteringsprosessen.[30]

6.2.2 Forsvaret har fortsatt skjermingsverdige informasjonssystemer som ikke tilfredsstiller kravene i sikkerhetsloven

Sikkerhetsloven stiller krav om at informasjon, informasjonssystemer og infrastruktur som er skjermingsverdig, skal beskyttes. Skjermingsverdige systemer skal godkjennes som grunnlag for tillit til at sikkerhetsnivået for systemet er forsvarlig. Nasjonal sikkerhetsmyndighet er godkjenningsmyndighet for skjermingsverdige informasjonssystemer. Sikkerhetsmyndigheten kan gi midlertidig brukstillatelse og i særlige tilfeller dispensasjon.

Forsvaret har fortsatt skjermingsverdige informasjonssystemer som ikke tilfredsstiller kravene i sikkerhetsloven. Forsvarets sikkerhetsavdeling ser manglende sikkerhetsgodkjenning av informasjonssystemer som en stor utfordring.[31]

Samtidig rapporterer Forsvaret ifølge departementet om en positiv utvikling, at det gjennomføres tiltak for å bedre sikkerhetstilstanden, og at flere systemer har oppnådd sikkerhetsgodkjenning.[32]

Skjermingsverdig informasjonssystem
Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon eller i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner

Ulike utfall ved søknad om sikkerhetsgodkjenning

Godkjent

Midlertidig brukstillatelse kan gis dersom det er iverksatt kompenserende tiltak og foreligger en plan for å rette mangler

Dispensasjon fra krav kan gis i særlige tilfeller selv om krav over ikke er oppfylt, dersom systemet ut fra operative behov må brukes

Avslag.

[27] (B) Intervju med Forsvarsmateriell 23. august 2023; (B) intervju med Cyberforsvaret 3. september 2024.
[28] Innst. 259 S (2022–2023) Dokument 3:3 (2022–2023).
[29] Skriftlig svar fra Forsvarsmateriell 4. desember 2024.
[30] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[31] (B) Forsvarets sikkerhetsavdeling. (2023). *Forsvarets tilstandsrapport sikkerhet 2023.*
[32] (B) Intervju med Forsvarsdepartementet 8. november 2024.

Ifølge Forsvarsstaben har Forsvaret intensivert kartleggingen og vurderingen av informasjonssystemene for å prioritere systemene som er mest kritiske for operativ effekt og grunnleggende nasjonale funksjoner.[33]

Forsvarets sikkerhetsavdeling viser til at det fortsatt er utfordrende å rekruttere og beholde personell med teknisk kompetanse. I tillegg er mye av sikkerhetsarbeidet innenfor IKT manuelt og tungvint.[34]

Forsvaret bemerker i halvårsrapporteringen i september 2024 at varig bedring av sikkerhetssituasjonen for Forsvarets informasjonssystemer avhenger av moderniseringstiltak.[35]

Ifølge Forsvarsstaben opplever Forsvaret et for ensidig fokus på selve sikkerhetsgodkjenningen, noe som reduserer fokuset på sikkerhetsstyringen. Forsvarsstaben viser videre til at arbeidet med sikkerhetsgodkjenning av Forsvarets komplekse IKT-portefølje er krevende.[36]

Både Forsvarsstaben og Forsvarsdepartementet viser til at det er ulike oppfatninger mellom Forsvaret og Nasjonal sikkerhetsmyndighet om hva som er et forsvarlig sikkerhetsnivå etter sikkerhetsloven, og hvordan dette skal måles og dokumenteres. Det pågår en prosess for å få en mer omforent forståelse.[37]

6.2.3 Forsvarets sikkerhetsstyring har en svak positiv utvikling, men det er fortsatt mangler

Forsvarets sikkerhetsavdeling vurderte i 2023 at det var mangler i Forsvarets sikkerhetsstyring, men at den har en svak positiv utvikling. Tilsyn, kontroller og rapporteringer viser at Forsvaret fremdeles har utfordringer med sikkerhetsstyringen.[38]

Sikkerhetsstyring omfatter alle aktiviteter som har betydning for det forebyggende sikkerhetsarbeidet, og skal bidra til forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige informasjonssystemer

Driftsenhetene rapporterer at det er krevende å rekruttere og beholde sikkerhetspersonell, og at utskiftingstakten er høy i mange stillinger.[39]

Forsvarsstaben viser til at det er gjennomført tiltak som har bedret Forsvarets IKT-sikkerhetsstyring. Samtidig er det identifisert flere utfordringer for sikkerhetsstyringen i forsvarssektoren. Det er blant annet manglende kapasitet og samarbeid om sikkerhetsstyring, utfordringer med fortsatt uavklarte roller, ansvar og myndighet og manglende standardisering av rammeverk og krav. Det forventes at deler av disse utforingene løses gjennom F24 (som er nærmere omtalt i punkt 6.4). Deler av utfordringene krever ifølge Forsvarsstaben at Forsvarsdepartementet involverer seg. Det gjelder særlig standardisering av rammeverk og krav på sikkerhetsområdet.[40]

[33] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[34] (B) Forsvarets sikkerhetsavdeling. (2023). *Forsvarets tilstandsrapport sikkerhet 2023.*
[35] (B) Forsvaret. (2024). *Forsvarets halvårlige rapport 2024*.
[36] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[37] (B) Intervju med Forsvarsstaben 16. oktober 2024; (B) intervju med Forsvarsdepartementet 8. november 2024.
[38] (B) Forsvarets sikkerhetsavdeling. (2023). *Forsvarets tilstandsrapport sikkerhet 2023.*
[39] (B) Forsvarets sikkerhetsavdeling. (2023). *Forsvarets tilstandsrapport sikkerhet 2023.Vedlegg.*
[40] (B) Intervju med Forsvarsstaben 16. oktober 2024.

Forsvarsstaben viser også til at det som følge av ny modell for IKT-styring i forsvarssektoren, er etablert et IKT-sikkerhetsstyre på strategisk nivå i Forsvarsstaben.[41]

Forsvarsdepartementet bekrefter at det fortsatt er utfordringer med sikkerhetsstyringen i Forsvaret, men mener at den overordnede utviklingen er positiv, spesielt innenfor IKT-sikkerhetsstyring. Departementet viser til et større arbeid for å kartlegge og bedre sikkerhetsstyringen i hele sektoren. Alle etatene er vurdert på modenhet, og departementsrådens sikkerhetsforum har utarbeidet et veikart for utvikling av sikkerhetsstyringen framover. I tillegg revideres *Instruks for sikkerhetstjeneste i forsvarssektoren*, som er det styrende dokumentet for forebyggende sikkerhet i sektoren.[42]

Forsvarsdepartementet viser til at driftsenhetene i sektoren har ansvar for egen sikkerhetsstyring. Driftsenhetene har ulik kompetanse, praksis og modenhet i sikkerhetsstyringen, og har dessuten ulike operative behov og ulike ressurser. Området har høy kompleksitet, og det er nødvendig med en god kobling mellom sikkerhetsstyring og øvrig IKT-styring.[43]

Forsvaret har tidligere uttalt gjennom rapporteringen at de viktigste tiltakene for å bedre både sikkerhetsstyringen og informasjonssikkerheten på lengre sikt er programmene MAST og Mime.[44] Punktene 6.3.1 og 6.3.2 omtaler dette nærmere.

6.2.4 Forsvarets evne til å oppdage og stanse digitale angrep er blitt bedre, men det er fortsatt kapasitetsutfordringer

Undersøkelsen i 2022 avdekket at Forsvaret hadde mangler i evnen til å oppdage og håndtere digitale angrep, og Riksrevisjonen anbefalte i Dokument 3:3 (2022–2023) Forsvarsdepartementet å styrke Forsvarets evne på dette området.

Nasjonal sikkerhetsmyndighet viser i risikobildet for 2023 til at digitale trusler og dataangrep øker, og i økende grad rammer forsvarssektoren.[45]

Ifølge Cyberforsvaret er evnen til å oppdage og stanse digitale angrep forbedret. Et tiltak for å forbedre evnen til å oppdage og stanse digitale angrep er oppbyggingen av MilCERT.[46]

Både Forsvarsstaben, Forsvarsdepartementet og departementets internrevisjon bekrefter Cyberforsvarets beskrivelse av at evnen til å oppdage og stanse digitale angrep er forbedret.[47]

MilCERT (Computer Emergency Response Team) overvåker informasjonssystemene til alle driftsenhetene i Forsvaret, FFI, Forsvarsbygg og Forsvarsmateriell.

[41] (UO) Intervju med Forsvarsmateriell 23. august 2024; (B) intervju med Forsvarsstaben 16. oktober 2024.
[42] (B) Intervju med Forsvarsdepartementet 8. november 2024.
[43] (B) Intervju med Forsvarsdepartementet 8. november 2024.
[44] (B) Forsvarets tertialrapport nr. 1 2022.
[45] Nasjonal Sikkerhetsmyndighet. (2023). *Nasjonalt digitalt risikobilde 2023*.
[46] (B) Intervju med Cyberforsvaret 3. september 2024.
[47] (B) Intervju med Forsvarsstaben 16. oktober 2024; (B) Forsvarsdepartementet. (2024). *B30 - Tilstanden i sektoren etter Riksrevisjonens rapport om K2IS;* (B) intervju med Forsvarsdepartementet 8. november 2024.

Det framgår av halvårsrapporteringen fra Forsvaret i september 2024 at framdriften for MilCERT følger planen, og at MilCERT vil være ferdigstilt innen utgangen av året.[48]

Cyberforsvaret viser imidlertid til at selv om evnen til deteksjon er blitt bedre, er kapasiteten fortsatt utfordrende.[49] Forsvarsstaben bekrefter at det fortsatt er kapasitetsutfordringer når det gjelder personell, teknologi og organisasjon, men at langtidsplanen legger opp til en kapasitetsøkning. Konkretisering av hvordan kapasitetsøkningen skal oppnås er en del av Forsvarets arbeid med gjennomføringsplan og virksomhetsplan.[50]

Forsvarsdepartementet ser det som avgjørende at MilCERT videreutvikles for å sikre evnen til å reagere raskt og målrettet på digitale angrep både mot forsvarssektoren og mot totalforsvaret framover.[51]

Ellers peker både Cyberforsvaret og Forsvarsstaben på at modernisering av IKT-porteføljen vil styrke evnen til å oppdage og stanse digitale angrep.[52]

6.2.5 Riksrevisjonens vurdering

Det er positivt at Forsvaret har fått bedre oversikt over sine informasjonssystemer, selv om det fortsatt er behov for avklaringer. Det er også positivt at arbeidet med å utarbeide en virksomhetsarkitektur er påbegynt.

Riksrevisjonen registrerer at sikkerhetstilstanden til Forsvarets informasjonssystemer fortsatt er alvorlig. Forsvaret har fortsatt skjermingsverdige informasjonssystemer som ikke er sikkerhetsgodkjent, til tross for at det er iverksatt tiltak for å bedre sikkerheten. En stor del av utfordringene er knyttet til systemer med teknisk gjeld. Riksrevisjonen registrerer at det på flere områder er ulik oppfatning om hva som er et forsvarlig sikkerhetsnivå etter sikkerhetsloven. Etter Riksrevisjonens vurdering er det viktig at aktørene blir enige om hva som er et forsvarlig sikkerhetsnivå, og hvordan dette skal måles og dokumenteres. Riksrevisjonen registrerer at det pågår en prosess for å avklare dette.

Riksrevisjonen registrerer også at det er iverksatt tiltak for å bedre sikkerhetsstyringen, men at sikkerhetsstyringen i Forsvaret fortsatt vurderes som mindre god.

Riksrevisjonen ser det som positivt at evnen til å oppdage og stanse digitale angrep er bedret gjennom oppbyggingen av IKT-responsmiljøet MilCERT i Cyberforsvaret, og at MilCERT skal være fullt operativt innen 1. januar 2025.

Et viktig tiltak for å bedre sikkerheten i informasjonssystemene og styrke evnen til å oppdage og stanse digitale angrep er å modernisere IKT-porteføljen og den digitale grunnmuren til Forsvaret.

---

[49] (B) Intervju med Cyberforsvaret 3. september 2024.
[50] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[51] (B) Intervju med Forsvarsdepartementet 8. november 2024.
[52] (B) Intervju med Cyberforsvaret 3. september 2024; (B) intervju med Forsvarsstaben 16. oktober 2024.

6.3 Det er fortsatt betydelig risiko knyttet til IKT-satsingen i programmene Mime og MAST

Forsvarsdepartementet startet i 2018 programmene Mime og MAST for å møte utfordringene på IKT-området i Forsvaret. Forsvaret er programeier og leder programstyret, som er plassert på strategisk nivå i Forsvarsstaben. Gjennomføringen av programmene er lagt til Forsvarsmateriell.

I 2022 konkluderte Riksrevisjonen med at det var stor risiko knyttet til den pågående IKT-satsingen i Mime og MAST, blant annet som følge av at sentrale spørsmål med betydning for gjennomføring og leveranser sto ubesvart. Både Mime og MAST hvilte på en strategi om å overdra ansvaret for drifts-, forvaltnings- og vedlikeholdsoppgaver til en strategisk partner fra leverandørindustrien, samtidig som de folkerettslige prinsippene ved en overdragelse av disse oppgavene til en sivil partner var uavklart.

Riksrevisjonen anbefalte Forsvarsdepartementet å sørge for at Forsvarsmateriell og Forsvaret ivaretar nødvendig framdrift og gevinstrealisering i programmene Mime og MAST.

6.3.1 Det har tatt tid å få opp leveransekapasiteten i Mime, og strategisk partnerskap fungerer ikke etter intensjonen

I Forsvarsdepartementets oppdrag om gjennomføring av program Mime fra 2020 står det at «anskaffelsene som foretas i Mime-programmet vil være av avgjørende betydning for Forsvaret virksomhet i fred, krise og krig, og leveransene vil være kritiske for Forsvarets operative evne». Ved oppstarten i 2020 besto programmet av 17 prosjekter.[53] Prosjektene skulle bidra til kampnær IKT til bruk på taktisk nivå i Forsvaret.[54]

Program Mime har gradvis gått fra tradisjonell prosjektstyring til såkalt smidig metodikk og styring på effekter for Forsvaret (effektrealisering). Etter hvert er det blitt færre prosjekter i Mime som følge av at prosjekter fullføres i IKT-kapasiteter. Dette er gjerne prosjekter der investeringen er relativt konkret definert. Prosjekter med behov for videreutvikling blir gjennomført i program Mime.[55] De fleste prosjektene i IKT-porteføljen gjennomføres utenfor Mime. En stor andel av disse prosjektene er forsinket [56]

Program Mime gjennomføres i leveransebølger. Det defineres effekter for hver leveransebølge som Forsvaret skal realisere.[57] I halvårs-rapporteringen i september 2024 viser Forsvaret til at det er utfordringer med å oppnå effekter fra leveransebølgene.[58]

Høsten 2024 er Mime i slutten av leveransebølge 2. Ifølge Forsvarsmateriell var ikke programorganisasjonen i Mime på plass før et godt stykke inn i leveransebølge 1 (2021–2022), og gjennomføringsoppdraget for

Mime er et program for investeringsprosjekter innen såkalt kampnær IKT. Prosjektene skal modernisere informasjons- og kommunikasjons-systemene for taktisk ledelse i Forsvaret

Kampnær IKT er et begrep som brukes om taktiske ledelsessystemer for land-, sjø- og luftdomenet.

[53] (UO) Forsvarsdepartementet (2020) *Program Mime - helhetlig taktisk informasjonsinfrastruktur - Oppdrag om gjennomføring*, 26. juni 2020.
[54] (B) Intervju med Forsvarsmateriell 23. august 2024; (B) intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.
[55] (B) Intervju med Forsvarsmateriell 23. august 2024; (B) intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.
[56] (B) Forsvarsmateriell (2024). *IKT-prosjekter i og utenfor programmene* 20. august 2024.
[57] (B) Intervju med ledelsen Forsvarsmateriell 9. oktober 2024.
[58] (B) Forsvaret (2024) *Forsvarets halvårlige rapport 2024*.

leveransebølge 1 kom ikke før årsskiftet 2021/2022. Dermed ble deler av det som skulle gjennomføres i leveransebølge 1, dratt med over i neste leveransebølge. I leveransebølge 2 har programmet hentet inn forsinkelsene. Ifølge Forsvarsmateriell leverer Mime nå i tråd med planen. Leveransebølge 3 er planlagt behandlet av Stortinget i 2025 og omfatter flere store materiellanskaffelser med lange ledetider. Det ble derfor besluttet å utvide bølgen til tre år.[59]

Program Mime har tidligere rapportert om kapasitetsutfordringer, men kapasiteten er ifølge Forsvarsmateriell styrket de siste årene og er nå på 94 prosent av beregnet behov. I oktober 2024 er fordelingen mellom ansatte og innleide 70 : 30, noe Forsvarsmateriell vurderer som hensiktsmessig. Ifølge Forsvarsmateriell tilsier erfaring at en slik fordeling over tid gir både ekstern kompetansetilførsel og skalerbarhet, samtidig som nødvendig kontinuitet opprettholdes.[60]

Forsvarsmateriell viser til at overgangen til smidig metodikk i Mime har krevd utvikling av ny kompetanse, ervervet over tid gjennom kurs, kompetanseplaner og erfaring. Programmet har utviklet seg fra en teoretisk tilnærming med stor vektlegging av selve metodikken til kompetanse basert på erfaring og vekt på leveranser og effekter.[61]

Forsvarsstaben mener at det har vært for høye forventninger til Mime og hva programmet kan levere på kort tid. Programmet har brukt lang tid til å opparbeide leveransekapasitet, og det er risiko ved programmets bruk av markedet og at strategisk partnerskap ikke fungerer etter intensjonen.[62]

Forsvarsdepartementet syntes det var krevende å få oversikt over framdrift og leveranser i Mime. Det var en av årsakene til at departementet bestilte en gjennomgang av programmet for å kartlegge risiko og foreslå risikoreduserende tiltak for det videre arbeidet.[63] Gjennomgangen ble gjennomført av Boston Consulting Group (BCG) i februar–juni 2024.[64]

BCG undersøkte seks hovedområder og konkluderte i rapporten *Risikoreduserende helsesjekk av program Mime* med at det er vesentlig risiko ved tre av disse. Områdene omtales kort nedenfor.

Gevinstrealisering og økonomi: Ifølge BCG gir de økonomiske nøkkeltallene i Mime begrenset styringsinformasjon, spesielt om kostnadseffektivitet. Rapporteringen til programstyret handler hovedsakelig om forpliktelse av midler, mens det i begrenset grad rapporteres på effekten av forpliktelsene. Det pekes også på at effektene som det skal styres etter, i liten grad er målbare.[65] Forsvarsmateriell viser til effektrealiseringsplanene og påpeker at reell effektrealisering også forutsetter andre leveranser og realiseringer, for eksempel brukertiltak.[66]

[59] (B) Intervju med Forsvarsmateriell 23. august 2024, (B) intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.
[60] (B) Intervju med Forsvarsmateriell 23. august 2024, (B) intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.
[61] (B) Intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.
[62] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[63] (B) Intervju med Forsvarsdepartementet 8 november 2024.
[64] (B) Forsvarsdepartementet. (2024). *Risikoreduserende helsesjekk av program Mime.*
[65] (B) Forsvarsdepartementet. (2024). *Risikoreduserende helsesjekk av program Mime.*
[66] (B) Intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.

Styring og organisering: BCG mener at organiseringen av Mime kan føre til avvikende mål og konflikter i styringen, fordi programmet er eierstyrt og behovsstyrt fra Forsvaret, men organisatorisk plassert i Forsvarsmateriell. Rapporten konkluderer også med at Forsvarets eierstyring kan svekkes fordi finansieringen ikke går via Forsvaret som er programeier.[67] Forsvarsmateriell viser til at Forsvaret styrer programmet gjennom eierskap til IKT-porteføljen, behovseierrollen for operasjoner og programeierrollen for Mime. Pengestrømmen påvirkes ikke av disse.[68]

Partnerskap og leveranser: Forsvarsmateriell og Kongsberg Defence & Aerospace (KDA) inngikk den 12. mai 2022 en partnerskapsavtale.[69] Ifølge rapporten fra BCG har det strategiske partnerskapet med KDA lav modenhet og er ikke etablert i henhold til intensjonene. Den opprinnelige intensjonen var at den strategiske partneren skulle være en ende-til-ende-tjeneste- og systemintegrator, men i stedet er den på vei til å bli en konsulentleverandør.[70] Forsvarsmateriell uttaler at det har tatt tid å vurdere spørsmålet om jus og habilitet i forholdet mellom Forsvarsmateriell og en aktør som både er strategisk partner og leverandør. Forsvarsmateriell vurderer at avtalene som nå er inngått med Kongsberg Defence & Aerospace, er på et riktig nivå.[71]

Forsvarsdepartementet har gitt Forsvaret, i samarbeid med Forsvarsmateriell, i oppdrag å utarbeide en plan for å gjennomføre tiltakene som rapporten fra BCG anbefalte for å redusere risiko.[72]

Forsvarsstaben presiserer at de tar funnene og anbefalingene fra gjennomgangen av Mime på største alvor. Forsvaret har utarbeidet en plan for tiltakene, og den ble sendt til Forsvarsdepartementet for godkjenning 25. oktober 2024. Forsvarsstaben framhever at det er viktig å holde oppmerksomheten på leveransene i Mime samtidig som det arbeides med å redusere risiko og lukke tiltakene.[73]

Forsvarsdepartementet vurderer det som alvorlig at BCG i sin gjennomgang fant tre områder med særlig høy risiko. Tiltakspakken følges opp annenhver måned, etter samme format som oppfølgingen av anbefalingene fra Riksrevisjonen. Departementet ser framdrift i arbeidet, og planen er å lukke tiltakene innen juni 2025.[74]

6.3.2 Anskaffelsen av strategisk partner i MAST er kansellert, og det er usikkerhet knyttet til gjennomføringen av programmet

MAST ble etablert som et program for å levere nye IKT- plattformer for alle formål i Forsvaret. Gjennomføringsmodellen for MAST er endret, men målene består. Programmet skal levere en ny digital grunnmur til

[67] (B) Forsvarsdepartementet. (2024). *Risikoreduserende helsesjekk av program Mime.*
[68] (B) Intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.
[69] Kongsberg valgt som strategisk partner. Lastet ned 4.november 2024 fra https://www.fma.no/aktuelt-og-media/2020/kongsberg-valgt-som-strategisk-partner
[70] (B) Forsvarsdepartementet. (2024). *Risikoreduserende helsesjekk av program Mime.*
[71] (B) Intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.
[72] (B) Forsvarsdepartementet (2024). *Supplerende tildelingsbrev nr. 15 til Forsvaret i 2024. Oppdrag om veikart og tidsplan for gjennomføring av risikoreduserende tiltakspakke for Mime. 15. oktober 2024.*
[73] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[74] (B) Intervju med Forsvarsdepartementet 8 november 2024.

forsvarssektoren og modernisere forvaltningssystemene.[75] Den digitale grunnmuren omtales også som digital plattform og sikker plattform.

Forsvaret utarbeidet i perioden 2020–2022 en konseptvalgutredning for modernisering av Forsvarets sikre plattformer med tilhørende kjernetjenester og virksomhetsstyringssystem (ERP).[76] Utredningen anbefaler et konsept med sikre plattformer, datasentre og et nytt digitalt ERP, som skal erstatte dagens løsning (SAP). Den eksterne kvalitetssikreren beskriver konseptet som et stort omstillingsprosjekt med en meget høy kostnad og høy risiko, og støttet under tvil konklusjonen i utredningen.[77]

MAST (Militær anvendelse av skytjenester) er et program for investeringsprosjekter som skal modernisere IKT-plattformer for alle formål i Forsvaret.

Opprinnelig bygde program MAST på en ide om en strategisk partner med ansvar for innovasjon og tjenesteintegrasjon, samt utvikling, drift og vedlikehold av plattformene. Fra januar i 2021 ble det jobbet med å anskaffe en strategisk partner. Etter nye vurderinger, blant annet som følge av den sikkerhetspolitiske situasjonen, kom Forsvaret i februar 2023 fram til at den planlagte driftsoverføringen av systemer og tjenester ikke kunne gjennomføres, og avlyste konkurransen.[78] Forsvarssjefen mener at avlysningen av konkurransen var en riktig beslutning, fordi risikoen ved en driftsoverføring var for stor.[79]

Digital grunnmur innebærer generelt at en organisasjon har en felles digital infrastruktur, bestående av maskin- og programvare som tilbyr et sett av IKT-tjenester.

Etter at konkurransen om strategisk partner ble avlyst, har Forsvaret og Forsvarsmateriell planlagt en ny gjennomføringsmodell. En av de viktigste endringene som følge av ny styringsmodell er at Forsvaret ved Cyberforsvaret skal ha ansvar for tjenesteintegrasjon. I stedet for en strategisk partner vil Forsvaret ha flere leverandører, og selv ha ansvaret for styringen.[80]

Tjenesteintegrasjon handler om å få ulike IKT-tjenester og systemer til å fungere sammen på en sømløs måte. Dette innebærer å koble sammen forskjellige applikasjoner, databaser og teknologier slik at de kan utveksle data og samarbeide effektivt.

Ifølge Forsvarsstaben skal Forsvaret i samarbeid med Forsvarsmateriell inngå samarbeid med industrien. Forsvaret jobber nå med en plan for dette. I tillegg må Forsvaret gjenvinne tilliten fra industrien etter at samarbeidet stoppet opp forrige gang.[81]

Forsvaret og Forsvarsmateriell viser til at det vil ta lang tid før en ny digital grunnmur er på plass. Forprosjektene forventes å løpe til 2025/2026, og gjennomføringsfasen forventes å starte 2026/2027. Samtidig som framtidens løsninger planlegges, må kritiske oppgraderinger gjennomføres og levetiden forlenges på eksisterende plattformer og systemer. Dette arbeidet ledes av Forsvaret med støtte fra Forsvarsmateriell.[82]

I begynnelsen av november 2024 fikk Forsvaret i oppdrag å starte forprosjekter på modernisering av Forsvarets sikre plattformer og nytt ERP-system. Forsvaret fikk også i oppdrag å starte forprosjekt for bygging av

[75] *Virksomhetsprogrammet MAST*. Lastet ned 14. november 2024 fra https://www.fma.no/anskaffelser/virksomhetsprogrammet-mast
[76] Enterprise Resource Planning.
[77] (UO) Metier. (2023). *Kvalitetssikring av KVU modernisering av Forsvarets sikre plattformer med tilhørende kjernetjenester og ERP*. 21. april 2023.
[78] (B) Intervju med ledelsen i Forsvarsmateriell 9. oktober 2024; (B) intervju med Forsvarsstaben 16. oktober 2024.
[79] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[80] (B) Intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.
[81] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[82] (B) Intervju med ledelsen i Forsvarsmateriell 9. oktober 2024; (B) intervju med Forsvarsstaben 16. oktober 2024.

datasentre.[83] Ifølge Forsvarsdepartementet dekker forprosjektene i betydelig grad omfanget som var planlagt i program MAST.

Forsinkelsene i moderniseringen av IKT-plattformene kan påvirke leveransene i Mime fordi en del av leveransene i program Mime skulle bygge på leveranser i program MAST. For å minimere konsekvensene av dette er noen leveranser som tematisk hørte hjemme i MAST, initiert under Mime, ifølge Forsvarsmateriell.[84]

Forsvarsdepartementet vurderer at prosjektene for modernisering av IKT-plattformene er store og komplekse, og at det er risiko ved gjennomføringen. Prosjekt datasenter er et stort EBA-prosjekt (eiendom, bygg og anlegg), mens prosjekt sikre plattformer og ERP er store IKT-prosjekter. Begge typene prosjekter fører med seg høy risiko for ikke å levere på tid og kostnad, særlig gitt forsvarssektorens historikk for gjennomføring av slike prosjekter. I tillegg skal prosjektene gjennomføres i en tid der det skjer mange endringer i forbindelse med styringsreformen F24.[85]

Ved behandlingen av langtidsplan for forsvarssektoren 2020−2024[86] fattet Stortinget et anmodningsvedtak der regjeringen ble bedt om å utrede bruken av ikke-militært ansatte og forhold knyttet til krigens folkerett. I investeringsproposisjonen for 2024 ble utredningen med utgangspunkt i anmodningsvedtaket presentert.[87]

6.3.3 Riksrevisjonens vurdering

Riksrevisjonen merker seg at det fortsatt er betydelig risiko knyttet til gjennomføringen av programmene Mime og MAST.

Riksrevisjonen registrerer at det har tatt tid for program Mime å få opp leveransekapasiteten, og at det har vært krevende for departementet å få oversikt over framdrift og leveranser i programmet. Riksrevisjonen registrerer videre at en ny ekstern evaluering også har pekt på høy risiko på sentrale områder for programmet.

De fleste av IKT-prosjektene i forsvarssektoren gjennomføres utenfor programmene. En oversikt over framdriften i disse prosjektene viser at en stor andel av prosjektene er forsinket.

Riksrevisjonen merker seg at modernisering av IKT-plattformene er forsinket etter at konkurransen om strategisk partner ble avlyst, og at Forsvarsdepartementet peker på at det er høy risiko ved gjennomføringen av prosjektene. En ny digital grunnmur er en forutsetning for at Forsvarets IKT-systemer skal ha tilfredsstillende funksjonalitet og sikkerhet, og har stor betydning for Forsvarets operative evne. Derfor er det avgjørende at Forsvaret lykkes med denne satsingen. Inntil en ny digital grunnmur er på plass, må samtidig midler benyttes til å forlenge levetiden på de eksisterende plattformene.

---

[83] (B) Intervju med Forsvarsdepartementet 8. november 2024.
[84] (B) Intervju med Forsvarsmateriell 23. august 2024.
[85] (B) Intervju med Forsvarsdepartementet 8. november 2024.
[86] Prop. 14 S (2020−2021) *Evne til forsvar – vilje til beredskap Langtidsplan for forsvarssektoren.*
[87] Prop. 59 S (2023−*2024) Investeringar i Forsvaret og andre saker.*

6.4 Forsvarsdepartementet har iverksatt en styringsreform, som også omfatter IKT-området

6.4.1 Ansvar og myndighet mellom etatene er forsøkt avklart i ny styringsmodell

Undersøkelsen i 2022 avdekket overlappende og uklare rolle- og ansvarsforhold på IKT-området mellom etatene i forsvarssektoren til tross for at sektoren hadde lagt ned et omfattende arbeid for å avklare dette.

Riksrevisjonen anbefalte i Dokument 3:3 (2022–2023) at Forsvarsdepartementet følger opp arbeidet med å avklare ansvaret mellom etatene i forsvarssektoren.

Ved behandlingen av Dokument 3:3 (2022–2023) understreket Stortinget behovet for å etablere en styringsmodell for forsvarssektoren med tydeligere ansvar og myndighet og at Forsvaret og forsvarssjefen gis et mer helhetlig ansvar.

På bakgrunn av utfordringer i sektoren satte Forsvarsdepartementet i begynnelsen av 2023 i gang et reformarbeid kalt Forsvarssektoren 24 (F24), for blant annet å avklare ansvarsforholdet mellom etatene.[88] Det ble satt i gang utredninger på flere områder, blant annet på IKT-området.[89]

Forsvarsdepartementet ga i august 2023 Forsvaret og Forsvarsmateriell i oppdrag å anbefale en ny styringsmodell for IKT-området og hvordan denne skulle implementeres. Departementet ga samtidig noen føringer for oppdraget, blant annet at ansvaret for utvikling, drift og vedlikehold skulle samles i Forsvaret, og at det i første omgang skulle avgrenses til Forsvarets sikre plattformer. [90] Forsvaret leverte i januar 2024 anbefalingen om en omforent ny IKT-styringsmodell til departementet, hvor utvikling, drift og vedlikehold av Forsvarets sikre plattformer skulle samles i Forsvaret.[91]

Ny IKT-styringsmodell gir Forsvaret ansvar for arkitektur- og datastyring, sikkerhetsstyring, mål- og resultatstyring, risikostyring og kapasitets- og kompetansestyring, mens Forsvarsmateriell har ansvar for anskaffelser (prosjekt- og driftsanskaffelser) og avtaleforvaltning.[92]

Både Forsvaret og Forsvarsmateriell mener at den nye styringsmodellen har gjort ansvarsfordelingen mellom de to etatene tydeligere.[93]

[88] De andre målene med F24 er: tydeligere mål i sektoren, mer helhetlig beslutningsgrunnlag basert på fakta, mindre fragmentering, og økt styring og kontroll.
[89] De andre områdene var anskaffelser, vedlikehold, investeringer, personell og kompetanse, FoU og operasjoner.
[90] Forsvarsdepartementet. (2023). *IKT-beslutning om videre prosess*. Brev til forsvarsstaben og forsvarsmateriell datert 22. august 2023.
[91] (UO) Forsvaret. (2024). *Fremtidens IKT-virksomhet i Forsvaret. Vedlegg A F24 IKT-Rapport*.
[92] (B) Intervju med Forsvarsstaben 16. oktober 2024; (B) intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.
[93] (B) Intervju med Forsvarsstaben 16. oktober 2024; (B) intervju med ledelsen i Forsvarsmateriell 9. oktober 2024.

6.4.2 Forsvaret har fått mer helhetlig ansvar og myndighet på IKT-området

Forsvaret har gradvis fått mer ansvar på IKT-området. Forsvarssjefen har fra 2021 hatt ansvaret, myndigheten og funksjonen for å utøve og videreutvikle den strategiske IKT-styringen i sektoren.

Fra 1. oktober 2024 ble også ansvaret for porteføljestyringen av investeringer overført fra Forsvarsdepartementet til Forsvaret.[94] Det innebærer at Forsvaret har fått et større og mer helhetlig ansvar. Samtidig er det i stor grad de samme ressursene som tidligere jobbet i departementet, som nå midlertidig løser oppgavene i Forsvaret og sikrer kontinuitet inntil Forsvaret legger fram sin vurdering av det varige behovet for kompetanse og kapasitet på området.[95]

Utvikling, drift og vedlikehold av Forsvarets sikre plattformer ble overført fra Forsvarsmateriell til Cyberforsvaret 1. januar 2025. I den forbindelse ble 82 årsverk overført fra Forsvarsmateriell IKT-kapasiteter til Cyberforsvaret. Fra 1. januar 2026 skal ytterligere anslagsvis 60−80 årsverk overføres.[96]

Forsvarsstaben styrkes for å ivareta de nye oppgavene. Det er ansatt en direktør for teknologi og IKT, som på vegne av forsvarssjefen skal ha utøvende ansvar for å styre og utvikle Forsvarets IKT, og det ansettes ledere og personell innenfor ulike fagområder[97]under IKT-direktøren.[98]

Forsvarssjefen har tidligere gitt uttrykk for at han var gitt ansvar uten myndighet, men utrykker at han får nødvendig myndighet med de endringene som blir operasjonalisert gjennom F24.[99]

Forsvarsdepartementet har identifisert en rekke risikoområder som må tas hensyn til i det videre arbeidet med styringsmodellen. Blant annet er det risiko ved kompleksiteten i ledelsesstrukturen, og departementet mener at IKT-direktøren må ha et tydelig mandat. Departementet mener videre at det er risiko ved produktorientering og brukerinvolvering. Dette begrunnes både med erfaringer fra andre offentlige virksomheter og med at IKT-funksjonen i Forsvaret ikke er ett organisatorisk element, men alle elementene som samlet leverer IKT for å understøtte Forsvarets behov. Departementet mener at forsvarsgrenenes premissgivende rolle må styrkes for at produktorienteringen skal fungere. Departementet har bedt Forsvaret om å oppdatere sine risikovurderinger. I en tid med høye ambisjoner og vesentlig økte investeringer framover kan konsekvensene av forsinkelser bli store.[100]

Departementet har videre bedt Forsvaret om å utarbeide en plan for framdrift og rekkefølge for oppgaver som skal overføres til Forsvaret på IKT-området, og en plan for å styrke alle styringsområdene som er nødvendige for å lykkes på IKT-området. Som del av dette må strategien for bruk av marked

---

[94] Forsvarsdepartementet. (2024). *Supplerende tildelingsbrev nr. 14 til Forsvaret for 2024 - Overføring av ansvar for porteføljestyringen fra Forsvarsdepartementet til Forsvaret*. 4. september 2024.
[95] (B) Intervju med Forsvarsdepartementet 8. november 2024.
[96] (UO) Forsvarsdepartementet. *Sammendrag F24 IKT;* (B) intervju med ledelsen i Forsvarsmateriell 9. oktober 2024; En milepæl for IKT-satsningen i forsvarssektoren Lastet ned 10. januar 2025.
[97] IKT-arkitektur, data og KI, og IKT-sikkerhet.
[98] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[99] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[100] (B) Intervju med Forsvarsdepartementet 8. november 2024.

og partnere revurderes, blant annet på grunn av utfordringene i Mime og MAST.[101]

6.4.3 Personell og kompetanse er fortsatt en utfordring, men det er bedring på enkelte områder

Den opprinnelige undersøkelsen om Forsvarets informasjonssystemer avdekket at mangel på kompetanse har vært en medvirkende årsak til at forsvarssektoren ikke har klart å løse mange av utfordringene på IKT-området. Blant annet viste undersøkelsen til utfordringer med kompetanse på bruk, drift og forvaltning av eksisterende IKT-systemer, utvikling av nye systemer og styring av IKT-området. Det ble også pekt på at det var vanskelig å rekruttere personell som både har riktig IKT-kompetanse og har militærfaglig bakgrunn.

Riksrevisjonen anbefalte Forsvarsdepartementet å vurdere ytterligere tiltak for å rekruttere, utvikle og beholde nødvendig fagkompetanse på IKT-området i forsvarssektoren.

Ifølge Forsvarsstaben har gjennomførte tiltak for å rekruttere, utvikle og beholde personell på IKT-området i forsvarssektoren hatt effekt. Blant annet er utdanningskapasiteten på cyberområdet økt, og de uteksaminerte blir i stor grad værende i Forsvaret. Forsvarsstaben viser også til gjennomført kompetansehevingsprogram for ledere og etablerte møtearenaer for IKT-ledelse.[102]

Men det går også fram av Forsvarets rapportering fra september 2024 at situasjonen for kompetanse på IKT-området fortsatt er utfordrende.[103]

I september 2024 hadde Cyberforsvaret en årlig rotasjon på om lag 10 prosent. Ettersom det er krevende å beholde militært og sivilt personell med riktig kompetanse, er Cyberforsvaret avhengig av å kjøpe spisskompetanse og midlertidig arbeidskraft. Cyberforsvaret konkurrerer med private og offentlige aktører som tilbyr bedre betingelser, og situasjonen med uavklart pensjonsordning for ansatte i Forsvaret virker negativt inn. Det er imidlertid iverksatt tiltak for å rekruttere og beholde personell.[104]

Forsvarsmateriell oppgir å ha tilstrekkelig personell og kompetanse til å ivareta framdriften på IKT-investeringene innenfor dagens portefølje, men er avhengig av å samarbeide med Forsvaret eller leverandører for å løse oppdragene.[105] Ifølge direktøren har Forsvarsmateriell hatt vekst i antall ansatte. Samtidig understreker hun at veksten må fortsette for at Forsvarsmateriell skal være i stand til å håndtere oppgavene som vil følge av forsvarsløftet. Det er et kontinuerlig arbeid å opprettholde nok personell og kompetanse.[106]

---

[101] (B) Forsvarsdepartementet. (2024). *Supplerende tildelingsbrev nr. 17 til forsvaret i 2024.* 15. november 2024.
[102] (B) Intervju med Forsvarsstaben 16. oktober 2024.
[103] (B) Forsvaret. (2024). *Rapportering på oppfølging av Riksrevisjonens rapport om Forsvarets informasjonssystemer*. September 2024.
[104] (B) Intervju med Cyberforsvaret 3. september 2024.
[105] (B) Intervju med Forsvarsmateriell 23. august 2024.
[106] (B) Intervju med ledelsen i Forsvarsmateriell 9. november 2024.

6.4.4 Riksrevisjonens vurdering

Riksrevisjonen har merket seg at Forsvarsdepartementet gjennom reformen Forsvarssektoren 24 har etablert en ny styringsmodell på IKT-området i Forsvaret. Modellen er under implementering høsten 2024 og våren 2025. Modellen adresserer flere av utfordringene med styringen på området, men det er foreløpig for tidlig å si noe om effekten av den nye modellen.

Riksrevisjonen registrerer at det pekes på at det fortsatt er en utfordring å ha nok personell og kompetanse i sektoren, selv om det er bedring på enkelte områder. Det gjennomføres tiltak for å rekruttere, utvikle og beholde personell på alle nivåer på IKT-området i forsvarssektoren. Samtidig er sektoren avhengig av å kjøpe ekstern kompetanse. Riksrevisjonen legger til grunn at tilgangen på tilstrekkelig kapasitet og kompetanse og god utnyttelse av disse ressursene vil være avgjørende for sektorens evne til å gjøre nødvendige forbedringer på IKT-området.

7 Statsrådens svar

Dokument 3:6 (2024−2025) *Oppfølging av Dokument 3:3 (2022−2023) Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner* ble oversendt statsråden i Forsvarsdepartementet. Statsrådens svar følger i vedlegg 2.

8 Riksrevisjonens uttalelse til statsrådens svar

Riksrevisjonen har ingen ytterligere merknader.

Saken sendes Stortinget.

Vedtatt i Riksrevisjonens møte 11. februar 2025.

Karl Eirik Schjøtt-Pedersen Anne Tingelstad Wøien

Arve Lønnum

Jens A. Gunvaldsen

Vedlegg

Vedlegg 1:

Riksrevisjonens brev til statsråden i Forsvarsdepartementet

Riksrevisjonen

Vår saksbehandler
Bente Willumsen

Vår dato	Vår referanse
23.01.2025	2024/00038-11
Deres dato	Deres referanse

FORSVARSDEPARTEMENTET
Postboks 8126 Dep,
0032 OSLO

Oppfølging av Dokument 3:3 (2022–2023) Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer til bruk i operasjoner

Vedlagt oversendes utkast til dokument 3:6 (2024–2025) Oppfølging av Dokument 3:3 (2022–2023) *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer til bruk i operasjoner* (BEGRENSET).

Vedlagt oversendes også en ugradert versjon av dokumentet. Stortinget vil motta både det graderte og det ugraderte dokumentet til behandling.

Dokumentet har vært forelagt Forsvarsdepartementet for faktasjekk og vurdering av gradering.

Vi ber statsråden redegjøre for hvordan departementet vil følge opp Riksrevisjonens konklusjoner, og eventuelt om departementet er uenig med Riksrevisjonen.

Statsrådens svar vil i sin helhet bli lagt ved dokumentet. Vi ber om at svaret oversendes som PDF lagret fra Word, ikke skannet bilde, slik at innholdet kan gjøres tilgjengelig for alle i samsvar med krav til universell utforming.

Svarfrist 6. februar 2025.

For riksrevisorkollegiet

Karl Eirik Schjøtt-Pedersen
riksrevisor

Brevet er digitalt godkjent og har derfor ingen håndskreven signatur

Vedlegg:

Utkast til dokument 3:6 (2024–2025) Oppfølging av Dokument 3:3 (2022–2023) *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer til bruk i operasjoner (BEGRENSET)*

Utkast til dokument 3:6 (2024–2025) Oppfølging av Dokument 3:3 (2022–2023) *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer til bruk i operasjoner (Ugradert versjon)*

Uten vedlegg er dette brevet ugradert.

Postadresse	Kontoradresse	Telefon	E-post	Nettsted	Bankkonto	Org.nr.
Postboks 6835 St Olavs plass 0130 Oslo	Storgata 16	22 24 10 00	postmottak@riksrevisjonen.no	www.riksrevisjonen.no	7694 05 06774	974760843

Vedlegg 2:

Statsrådens svar

DET KONGELIGE
FORSVARSDEPARTEMENT

Statsråden

RIKSREVISJONEN

Postboks 6835 St. Olavs plass
0130 OSLO

Deres ref	Vår ref	Dato
	25/00317	3. februar 2025

Oppfølgingen av Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer - statsrådens uttalelse

1. Innledning

Jeg viser til brev fra Riksrevisjonen datert 23. januar 2025, vedrørende utkast til *Oppfølging av Dokument 3:3 (2022-2023) Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner.*

Bakgrunnen for oppfølgingsrevisjonen er Dokument 3:3 (2022–2023) *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner.* Dokumentet med vedlagt rapport ble overlevert til Stortinget i oktober 2022, og bygde i hovedsak på data fra perioden 2017–2020.

Målet med Riksrevisjonens oppfølgingsrevisjon har vært å vurdere om konklusjoner og anbefalinger i Dokument 3:3 (2022-2023) er fulgt opp av Forsvarsdepartementet og underliggende etater. Undersøkelsen omfatter perioden 2022-2024.

Riksrevisjonens rapport i 2022 konkluderte med at det var mangler med Forsvarets kommando- og kontrollinformasjonssystemer for både samvirke og sikkerhet. Riksrevisjonen konkluderte videre med at det heftet vesentlig risiko knyttet til programmene Mime og MAST. Samlet ble kritikken av Forsvarets K2IS vurdert som *svært alvorlig.*

Tilbake i 2022 uttalte jeg at oppfølging av anbefalingene og kritikken fra Riksrevisjonen ville ha høy prioritet i Forsvarsdepartementet og underliggende etater. Flere tiltak ble iverksatt på tvers av sektoren for å dekke manglene som ble belyst. Mens enkelte tiltak virker på kortere sikt, vil andre trenge lenger tid for å ha effekt. For å følge arbeidet har det blitt iverksatt

Postadresse	Kontoradresse	Telefon	Avdeling	Saksbehandler
Postboks 8126 DEP 0032 OSLO	Glacisgata 1	23098000	IKT-utvikling	Morten Bergersen Gjellerud
postmottak@fd.dep.no	regjeringen.no/fd	Org.nr 972417823		

månedlig rapportering internt i Forsvarsdepartementet og fra underliggende etater for å redegjøre for status på tiltakene som tar tak i Riksrevisjonens kritikk. Rapporteringen og oppfølgningen pågår fortsatt og følges nøye. Som del av oppfølgingsarbeidet ble det gjennomført en bekreftelsesrevisjon av Forsvarsdepartementets internrevisjon i 2024. Bekreftelsesrevisjonen pekte på tydelig fremgang i arbeidet med å følge opp kritikken til Riksrevisjonen, samtidig som det ble fremhevet at situasjonen fortsatt er alvorlig.

Jeg merker meg at Riksrevisjonens oppfølgingsrevisjon konkluderer med at det har vært forbedringer på flere områder og ikke ser behov for å fremme kritikk til departementets oppfølging av tiltakene. Det trekkes frem at samvirket mellom Forsvarets informasjonssystemer er bedret og at Forsvarets evne til å oppdage og stanse digitale angrep er styrket. Samtidig fremhever Riksrevisjonen at det fortsatt er utfordringer. Riksrevisjonen påpeker blant annet mangler i Forsvarets sikkerhetsstyring, samt vedvarende risiko knyttet til programmene Mime og MAST.

Jeg er enig i utfordringsbildet som Riksrevisjonen legger frem. Til tross for en bedring i status, anser jeg fortsatt situasjonen som alvorlig, og understreker behovet for å fortsette det gode arbeidet med tiltakene i sektoren. Jeg merker meg samtidig at Riksrevisjonen ikke fremmer ytterligere tiltak eller anbefalinger, og vi fortsetter dermed arbeidet der vi kontinuerlig vurderer tiltakene som pågår.

2. Samvirket mellom Forsvarets informasjonssystemer er blitt bedre

Riksrevisjonen har konkludert med at samvirket mellom Forsvarets informasjonssystemer til bruk i operasjoner er bedret siden undersøkelsen i 2022. Det er etablert nye sikkerhetsmekanismer for dataflyt mellom informasjonssystemer. De nye løsningene er automatisert i større grad, og løsningene har blitt bedre for datastrømmer mellom flere systemer.

Riksrevisjonens rapport i 2022 kritiserte mangler ved taktisk datalink som kunne redusere mulighetene for utveksling av data. Siden 2022 har taktisk datalink blitt modernisert. Riksrevisjon trekker i oppfølgingsrevisjonen frem at kapasiteten for taktisk datalink er økt, men at det fortsatt er mangler. Manglene ved taktisk datalink er delvis knyttet opp mot utfordringer med Norges topografi. Forsvaret og Forsvarets forskningsinstitutt (FFI) skal jobbe videre med å teste alternative løsninger for disse utfordringene.

Riksrevisjonen peker i oppfølgingsrevisjonen på at det fortsatt er et høyt antall informasjonssystemer i sektoren, og at mengden systemer bidrar til å gjøre samvirket mellom systemer vanskelig. Jeg vil her trekke frem at det er utført flere konsolideringer av informasjonssystemer og det pågår arbeid med å fase ut utdaterte systemer, men at arbeidet er tidkrevende og har en stor avhengighet til de igangsatte forprosjektene for modernisering av Forsvarets datasenter, sikre plattformer og ERP.

Det er avgjørende at Forsvarsdepartementet med underliggende etater opprettholder innsatsen for å sikre videre fremdrift på dette området.

3. Sikkerhetstilstanden til Forsvarets informasjonssystemer er fortsatt alvorlig, selv om det er iverksatt tiltak

Riksrevisjonen trekker frem en positiv utvikling innen sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer. Det vises til bedre oversikt over informasjonssystemer, økt evne til å oppdage og stanse digitale angrep og tiltak for å bedre sikkerhetsstyringen. Det fremkommer samtidig at det fortsatt er utfordringer på området, blant annet tilknyttet sikkerhetsgodkjenning av informasjonssystemer, med et betydelig antall som mangler endelig sikkerhetsgodkjenning. Utfordringene er i stor grad knyttet til teknisk gjeld, som har avhengighet til forprosjektene som nå er satt i gang for modernisering av Forsvarets datasenter, sikre plattformer og ERP.

Siden Riksrevisjonens kritikk i 2022 har MilCERT (Computer Emergency Response Team) blitt etablert i Cyberforsvaret. MilCERT har nå nådd full operasjonell kapasitet, og overvåker informasjonssystemene hos alle driftsenhetene i Forsvaret, samt FFI, Forsvarsbygg og Forsvarsmateriell. Etableringen av MilCERT har resultert i styrket evne til å oppdage og stanse digitale angrep. Det er et pågående arbeid i Forsvarsdepartementet knyttet til å forbedre sikkerhetsstyringen på IKT-området i sektoren, samt øke verdien og effektivisere ressursbruken i prosessen for sikkerhetsgodkjenning av informasjonssystemer. Dette arbeidet koordineres med Forsvarets pågående arbeid med sikkerhetsstyring og begrepsavklarering. Forprosjektene for datasenter, sikre plattformer og ERP vil videre styrke sikkerheten i Forsvarets informasjonssystemer på sikt.

Jeg anser videreutvikling av sikkerheten for Forsvarets informasjonssystemer som svært viktig, og dette vil prioriteres fremover i fortsettelsen av arbeidet med oppfølging av Riksrevisjonens kritikk. Med et internasjonalt trusselbilde der cyberangrep stadig blir mer sofistikert og målrettede, er det kritisk at Forsvaret har evne til å håndtere sektorens sikkerhetsutfordringer.

4. Det er fortsatt betydelig risiko knyttet til IKT-satsingen i programmene Mime og MAST

Riksrevisjonen merker seg at det fortsatt er betydelig risiko knyttet til program Mime. Forsvarsdepartementet gjennomførte en risikoreduserende gjennomgang av programmet våren 2024 for å kartlegge risiko og foreslå risikoreduserende tiltak. Gjennomgangen konkluderte med at det hefter vesentlig risiko ved særlig tre sentrale områder for programmet: «Gevinstrealisering og økonomi», «Styring og organisering» og «Partnerskap og leveranser». En omfattende tiltakspakke ble anbefalt for å ta ned risikoen.

Funnene fra den risikoreduserende gjennomgangen av Mime blir tatt alvorlig og Forsvaret har på oppdrag fra Forsvarsdepartementet igangsatt arbeid med den risikoreduserende tiltakspakken, samtidig som det er fokus på å opprettholde leveransetakten i Mime. Tiltakspakken følges opp av Forsvarsdepartementet annenhver måned. Det er fremdrift i arbeidet, og planen er å lukke de risikoreduserende tiltakene i løpet av juni 2025.

Riksrevisjonen påpekte i 2022 høy risiko ved program MAST. MAST fikk ved opprettelse i oppdrag å modernisere Forsvarets sikre IKT-plattformer. Etter en helhetlig risikovurdering ble programmets planlagte anskaffelse kansellert i 2023. Program MAST har siden kanselleringen av anskaffelsen planlagt en reorientering av innretning og tilnærming. De igangsatte forprosjektene for modernisering av Forsvarets datasenter, sikre plattformer og ERP dekker i betydelig grad omfanget som lå til grunn for program MAST. Det er fortsatt høy risiko for ikke å levere prosjektene på tid og kost, og Forsvarsdepartementet følger opp forprosjektene månedlig for å sikre fremdrift og redusere gjennomføringsrisiko.

Forprosjektene er helt sentrale i å lykkes med å ta tak i de bakenforliggende årsakene for mye av kritikken fra Riksrevisjonen som påpekt i flere av tiltakene over. Prosjektene har dermed stor betydning for Forsvarets operative evne. Dette er store, komplekse prosjekter som vil følges tett fremover og som har svært høy prioritet.

5. Forsvarsdepartementet har iverksatt en styringsreform som også omfatter IKT-området

Riksrevisjonens undersøkelse i 2022 avdekket overlappende og uklare rolle- og ansvarsforhold på IKT-området mellom etatene i forsvarssektoren. På bakgrunn av utfordringer i sektoren satte Forsvarsdepartementet i begynnelsen av 2023 i gang et reformarbeid kalt Forsvarssektoren 24 (F24), og som en del av dette ble Forsvaret og Forsvarsmateriell gitt i oppdrag å anbefale en ny styringsmodell på IKT-området. Ny IKT-styringsmodell blir nå implementert, og både Forsvaret og Forsvarsmateriell mener at ansvarsfordelingen mellom de to etatene er blitt tydeligere. Samtidig har Forsvaret fått mer helhetlig ansvar og myndighet på IKT-området.

Riksrevisjonen merker seg at modellen som nå er under implementering, følger opp flere av utfordringene som gjelder styring på IKT-området, men at det foreløpig er for tidlig å si noe om effekten av den nye modellen. Jeg vil trekke frem at Forsvarsdepartementet følger både utvikling og implementering av modellen tett gjennom etatsstyringen.

Riksrevisjonen legger frem i sin oppfølgingsrevisjon at tilgang på tilstrekkelig kapasitet og kompetanse og god utnyttelse av disse ressursene vil være avgjørende for sektorens evne til å gjennomføre nødvendige forbedringer på IKT-området. Videre fremskritt innen rekruttering og avklaring av ansvarsområdet mellom etatene er en prioritet i det kommende året. Det pågår arbeid i Forsvaret knyttet til å utvikle en plan for IKT-kompetanse, og det forventes at planen vil ha en positiv innvirkning på området.

Arbeidet med styringsendringene, både tilknyttet avklaring av ansvar og rekruttering, er som påpekt av Riksrevisjonen i for tidlig fase for å konkludere på effekt, men jeg har tro på at vi nå gjør de riktige tiltakene for å se bedring på dette området.

6. Avslutning

Jeg deler Riksrevisjonens oppfatning av situasjonen. Flere tiltak har blitt iverksatt for å tette gapet fra Riksrevisjonens kritikk i 2022, samtidig som situasjonen fortsatt er alvorlig. Tiltakene vil fortsette å ha høy prioritet i kommende år, frem til effektene fra tiltakene er hentet ut, og situasjonen er forbedret.

Med hilsen

Bjørn Arild Gram

Bjørn Arild Gram