Riksrevisjonen

Riksrevisjonens undersøkelse av Forsvarets informasjons-systemer for kommunikasjon og informasjonsutveksling i operasjoner

Ugradert versjon av Dokument 3:3 (2022–2023)

Riksrevisjonen

Til Stortinget

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

Dette er en ugradert versjon av Dokument 3:3 (2022–2023). Riksrevisjonen har i dialog med Forsvarsdepartementet utarbeidet et ugradert dokument som er så fullstendig som mulig. Graderte opplysninger er fjernet, og en del informasjon er omskrevet og gjort mindre detaljert, slik at den ikke anses som gradert. Dette gjelder også noen av konklusjonene og deler av kritikken. Forsvarsdepartementet vurderer at dokumentet ikke inneholder gradert informasjon.

Rapporten fra undersøkelsen, som følger som vedlegg til det graderte dokumentet til Stortinget, er gradert (KONFIDENSIELT). Det er ikke utarbeidet en ugradert versjon av rapporten.

Dokumentet har følgende inndeling:

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

Riksrevisjonen, 4. oktober 2022

For riksrevisorkollegiet

Karl Eirik Schjøtt-Pedersen
Riksrevisor

Forsidebilde: Forsvaret / Anette Ask
ISBN-978-82-8229-546-8

Innhold

Riksrevisjonen benytter følgende begreper for kritikk, med denne rangeringen etter høyest alvorlighetsgrad:

1. **Svært alvorlig** brukes ved forhold der konsekvensene for samfunnet eller berørte borgere er svært alvorlige, for eksempel risiko for liv eller helse.
2. **Alvorlig** benyttes ved forhold som kan ha betydelige konsekvenser for samfunnet eller berørte borgere, eller der summen av feil og mangler er så stor at dette må anses som alvorlig i seg selv.
3. **Sterkt kritikkverdig** angir forhold som har mindre alvorlige konsekvenser, men gjelder saker med prinsipiell eller stor betydning.
4. **Kritikkverdig** brukes for å karakterisere mangelfull forvaltning der konsekvensene ikke nødvendigvis er alvorlige. Dette kan gjelde feil og mangler som har økonomiske konsekvenser, overtredelse av regelverk eller saker som er tatt opp tidligere og som fortsatt ikke er rettet opp.

1 Innledning

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

Evnen til å samhandle i operasjoner avhenger av informasjonssystemer[1]. Informasjonssystemene som brukes i Forsvarets operasjoner, kalles gjerne kommando- og kontrollinformasjonssystemer. For at disse systemene skal virke effektivt må de være *interoperable.* Det vi si at systemene må kunne samvirke og fungere med hverandre for å levere informasjon og tjenester til, og ta imot informasjon og tjenester fra, andre systemer. Dette avhenger også av kommunikasjonsinfrastrukturen som gjør det mulig å overføre data mellom systemene. Forsvarets kommunikasjonsinfrastruktur består av kjernenett, aksessnett, radionett og mobile og deployerbare[2] kommunikasjonsløsninger.

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

Forsvarsdepartementet har ansvar for å utforme og iverksette norsk sikkerhets- og forsvarspolitikk og for den overordnede styringen og kontrollen av underliggende etaters virksomhet. Av departementets fire underliggende etater[3] inngår Forsvaret og Forsvarsmateriell i denne undersøkelsen. I Forsvaret inngår Luftforsvaret, Sjøforsvaret, Hæren, Heimevernet, Cyberforsvaret og Forsvarets operative hovedkvarter i undersøkelsen, mens Etterretningstjenesten og Forsvarets spesialstyrker ikke inngår.

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

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

---

[1] Begrepet *informasjonssystem* kan omfatte både manuelle og digitale systemer. Vi bruker begrepet om digitale systemer og synonymt med IKT-system.
[2] At kommunikasjonsløsninger er deployerbare betyr at de kan flyttes dit behovet er.
[3] Forsvaret, Forsvarsmateriell, Forsvarsbygg og Forsvarets forskningsinstitutt. I tillegg har Forsvarsdepartementet instruksjonsmyndighet overfor Nasjonal Sikkerhetsmyndighet i saker som gjelder forsvarssektoren.

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

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

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

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

2 Konklusjoner

Konklusjoner

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

3 Utdyping av konklusjoner

Da langtidsplanen for forsvarssektoren for perioden 2017–2020 ble behandlet, sluttet Stortinget seg til at Forsvaret må ha evne til å lede og gjennomføre operasjoner gjennom et godt kommando- og kontrollapparat, og at dette krever klare styringslinjer, sikre og effektive kommunikasjonsløsninger og tilpasset infrastruktur. Det skulle videre utvikles en IKT-infrastruktur som gir Forsvaret den nødvendige evnen til å lede og samvirke i fellesoperasjoner.

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

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

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

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 kommando- og kontrollinformasjonssystemer som samvirker effektivt. Det innebærer at systemene må være interoperable slik at de kan levere informasjon til, og ta imot informasjon fra, andre systemer.

Faktaboks 1 Kommandonivåer for militære styrker

Strategisk nivå er det høyeste kommandonivået og deles inn i politisk-strategisk og militærstrategisk nivå. Militærstrategisk nivå omsetter politiske føringer til militærstrategiske mål. Forsvarssjefen representerer det øverste militærstrategiske nivået og har full kontroll over alle de underlagte norske styrkene nasjonalt.
Operasjonelt nivå er det kommandonivået som omsetter strategiske mål til oppdrag for tildelte styrker. Nasjonalt er sjefen for Forsvarets operative hovedkvarter fellesoperativ styrkesjef med ansvar for å planlegge og lede nasjonale operasjoner og med operativ kommando over tildelte styrker.
Taktisk nivå er det kommandonivået som skal utføre oppdrag for å nå militære målsettinger. Det er representert med alle avdelingene under Forsvarets operative hovedkvarter.

Kilde: Forsvarets fellesoperative doktrine (2019)

Undersøkelsen viser at det er mangler i samvirket mellom Forsvarets kommando- og kontrollinformasjonssystemer. Forsvaret har ikke utfordringer med å løse oppdraget i daglige operasjoner men disse manglene gir risiko for redusert effektivitet, og de kan få betydning ved økt konfliktnivå dersom

tid er av avgjørende betydning. Riksrevisjonen kritiserer dette. Kritikken er utdypet i Riksrevisjonens sikkerhetsgraderte rapport.

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

Undersøkelsen viser at Forsvaret har et høyt antall kommando- og kontrollinformasjonssystemer med ulike tekniske løsninger, og at dette bidrar til å gjøre samvirket mellom systemene vanskelig. Mengden av systemer fører også til at det går ekstra ressurser til forvaltning og drift av systemene.

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

Forsvaret har de senere årene anskaffet mye nytt materiell, og det skal etter planen gjøres omfattende materiellinvesteringer både i nåværende og kommende langtidsplanperioder. Nye våpenplattformer, som fly, båter og kjøretøy, leveres ofte med innebygde informasjonssystemer. Enkelte av disse systemene er ikke interoperable med Forsvarets eksisterende informasjonssystemer. Dette kan føre til at materiellet ikke blir utnyttet optimalt. Riksrevisjonen merker seg at sjefen for Luftforsvaret mener at kommando- og kontrollinformasjonssystemene som benyttes i de nye kampflyene, må videreutvikles for at Forsvaret skal kunne utnytte flyene fullt ut operativt.

3.1.2 Ulike sikkerhetsdomener påvirker informasjonsutvekslingen mellom systemer

Stortinget har lagt vekt på at det skal utvikles IKT som støtter interoperabilitet og samvirke med NATO. Dette er viktig fordi mangler i interoperabilitet kan påvirke Forsvarets evne til å gjennomføre fellesoperasjoner og kommunisere med NATO og allierte.

Forsvaret benytter kommando- og kontrollinformasjonssystemer på ulike sikkerhetsdomener. Dette påvirker informasjonsutvekslingen mellom systemene. Sikkerhetsdomenene er inndelt tilsvarende som nivåene for sikkerhetsgradert informasjon.

Faktaboks 2 Nasjonale – og NATOs sikkerhetsgrader

En virksomhet som tilvirker informasjon skal sikkerhetsgradere informasjonen dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende.

Følgende sikkerhetsgrader benyttes:

a. STRENG HEMMELIG dersom det kan få helt avgjørende skadefølger
b. HEMMELIG dersom det kan få alvorlige skadefølger
c. KONFIDENSIELT dersom det kan få skadefølger
d. BEGRENSET dersom det i noen grad kan få skadefølger

NATO bruker følgende tilsvarende sikkerhetsgrader:

a. COSMIC TOP SECRET
b. NATO SECRET
c. NATO CONFIDENTIAL

Kilde: Sikkerhetsloven (2019) § 5-3; Directive on Security of NATO Classified Information (2020) § 2

3.1.3 Mangler ved taktisk datalink reduserer mulighetene for utveksling av data

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

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

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

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

Ifølge langtidsplan for forsvarssektoren 2017–2020 har NATO slått fast at digitale angrep kan få like alvorlige konsekvenser som konvensjonelle angrep. Angrep i det digitale rom omfattes derfor av NATO-traktatens artikkel 5 om kollektivt forsvar. Også i FN-pakten er det slått fast at digitale angrep kan utløse en stats rett til selvforsvar.

Sikkerhetsloven har krav om at informasjon, informasjonssystemer og infrastruktur som er skjermingsverdige, skal beskyttes. Informasjon er

skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig. Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner (se tekstboks 3). Infrastruktur er skjermingsferdig dersom det kan skade grunnleggende nasjonale funksjoner at infrastrukturen får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.

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

Faktaboks 3 Grunnleggende nasjonale funksjoner

Grunnleggende nasjonale funksjoner er tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Forsvarsdepartementet har identifisert fem grunnleggende nasjonale funksjoner i egen sektor:

1. Evne til etterretning, situasjonsforståelse og rettidig varsling
2. Evne til å håndtere episoder og sikkerhetspolitiske kriser og om nødvendig forsvare norsk eller alliert territorium
3. Evne til kommando og kontroll over norske og allierte styrker
4. Evne til beskyttelse av norske og allierte styrker, kritiske samfunnsfunksjoner og kritiske funksjoner for Forsvaret
5. Forsvarsdepartementets virksomhet, handlefrihet og beslutningsdyktighet.

Kilde: Sikkerhetsloven (2019) §§ 1-5 og 2-1, Prop. 1 S (2021–2022) Forsvarsdepartementet

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

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

3.2.1 Mangler i oversikt og dokumentasjon på IKT-området påvirker muligheten for å ivareta sikkerheten i informasjonssystemene

Sikkerhetsloven stiller krav om at arbeidet med forebyggende sikkerhet skal være risikobasert. En grunnleggende forutsetning for at Forsvaret skal kunne foreta gode risikovurderinger og planlegge og gjennomføre effektive sikkerhetstiltak, er at virksomheten har god oversikt over informasjonssystemer og tilhørende kommunikasjonsinfrastruktur.

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

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

Mangler i oversikt og kunnskap om IKT-porteføljen svekker muligheten for å ivareta sikkerheten i systemene på en effektiv og sikker måte. Riksrevisjonen mener dette er sterkt kritikkverdig.

3.2.2 Forsvaret har skjermingsverdige informasjonssystemer som ikke tilfredsstiller sikkerhetslovens krav

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

Faktaboks 4 Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er en etat under Justis- og beredskapsdepartementet. Faglig er den underlagt både Justis- og beredskapsdepartementet og Forsvarsdepartementet. Nasjonal sikkerhetsmyndighet er fagorgan for forebyggende sikkerhet og sikkerhetsmyndighet etter sikkerhetsloven. I rollen som sikkerhetsmyndighet er Nasjonal sikkerhetsmyndighet godkjenningsmyndighet for skjermingsverdige informasjonssystemer. Nasjonalt cybersikkerhetssenter er en del av Nasjonal sikkerhetsmyndighet, og skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberangrep.

Kilde: nsm.no/om-oss/dette-er-nsm, Prop. 1 S (2021–2022) Forsvarsdepartementet

Et informasjonssystem som ikke er sikkerhetsgodkjent, kan få midlertidig brukstillatelse. Dette forutsetter imidlertid at det benyttes kompenserende tiltak, slik at bruken av systemet er forsvarlig. I særlige tilfeller kan Nasjonal sikkerhetsmyndighet også gi dispensasjon fra krav til midlertidig brukstillatelse. Slik dispensasjon skal kun gis i tilfeller der konsekvensene

ved at systemet ikke tas i bruk, overstiger konsekvensene av sikkerhetsbrudd vurdert opp mot sannsynligheten for slike brudd.

Undersøkelsen viser at Forsvaret har tatt i bruk systemer som ikke tilfredsstiller sikkerhetslovens krav til godkjenning. Den viser også at Forsvaret i enkelte tilfeller har latt hensynet til operative behov veie tyngre enn risikoen ved å bruke systemer uten sikkerhetsgodkjenning. Det er i tillegg ressurskrevende for sektoren å forvalte informasjonssystemer som ikke er sikkerhetsgodkjent.

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

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

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

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

Ifølge Forsvarets egne vurderinger har det ikke har god nok evne til å oppdage og stanse digitale angrep. Forsvaret peker på sårbarheter i Forsvarets informasjonssystemer og tilgangen på personell med riktig kompetanse som årsaker til dette. Det tar lang tid for Cyberforsvaret å få personell opp på et kompetansenivå som er godt nok til at de kan gjennomføre defensive cyberoperasjoner.

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

Forsvarets evne til å oppdage og stanse digitale angrep er avgjørende for å kunne ivareta den operative evnen. Forsvaret må være i stand til å beskytte sine egne skjermingsverdige informasjonssystemer, inkludert kommando- og kontrollinformasjonssystemene. I den nye langtidsplanen for forsvarssektoren 2021–2024 vises det til at digitale angrep i økende grad har blitt en del av militære operasjoner, og at skillelinjene mellom konvensjonell

og irregulær krigføring har blitt mindre klare. Dette innebærer også at de tradisjonelle skillene mellom fred, krise og krig utfordres.

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

3.2.4 Svakheter i sikkerhetsstyringen forsterker utfordringene

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

Undersøkelsen viser at Forsvaret har utfordringer med å ivareta kravene til sikkerhetsstyring. Både Forsvaret selv og Forsvarsdepartementet har erkjent at det er svakheter i sikkerhetsstyringen, og oppgir at svakhetene skyldes mangler i kompetanse, organisering og ressurser. I *Informasjonssikkerhetsstrategi for forsvarssektoren* fra 2017 peker Forsvarsdepartementet på behovet for å integrere informasjonssikkerhets-arbeidet i den helhetlige virksomhetsstyringen. Riksrevisjonens undersøkelse viser at sikkerheten på IKT-området fremdeles ikke er tilstrekkelig ivaretatt i virksomhetsstyringen i Forsvaret. I tillegg har sikkerhetsstyringen i for stor grad blitt ensbetydende med sikkerhetsgodkjenning av informasjonssystemer, snarere enn å være en del av den ordinære styringen.

Ansvaret for å forvalte informasjonssystemene er fordelt på flere aktører i forsvarssektoren. Forsvaret og Forsvarsmateriell har i undersøkelsesperioden lagt stor vekt på å avklare ansvars- og rollefordelingen knyttet til forvaltningen av IKT-materiell og jobber med å styrke forvaltningen ytterligere. Aktørenes forståelse og praktisering av ansvars- og rollefordelingen framstår like fullt som en medvirkende årsak til svakhetene i sikkerhetsstyringen.

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

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

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

IKT ble pekt på som et satsingsområde i langtidsplanen for forsvarssektoren for 2017–2020. IKT-satsingen skulle legge til rette for at Forsvaret skulle kunne løse sine viktigste oppgaver, og bidra til at sektorens ressurser ble utnyttet på en god måte. IKT skulle benyttes som et virkemiddel for å bedre samhandlingen i Forsvarets operasjoner. Målet var å utvikle en IKT-infrastruktur som skulle gi Forsvaret nødvendig evne til å lede og samvirke i et fellesoperativt perspektiv.

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

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

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

Forsvaret har ansvar for at virksomheten har IKT som er effektiv og sikker og kan brukes i Forsvarets operasjoner. Dette betyr også at Forsvaret må ha planer for hvordan virksomheten skal bruke IKT og ivareta sikkerheten i systemene.

Forsvaret mangler en virksomhetsarkitektur som kan legge til rette for gode prioriteringer i oppfølgingen av eksisterende IKT-løsninger og i valgene av nye. En forutsetning for at Forsvaret skal legge hensiktsmessige planer og rammer for videreutviklingen av IKT-porteføljen, er at virksomheten har god oversikt over informasjonsbehovet og informasjonssystemene i sektoren.

Forsvaret har imidlertid ikke god nok oversikt over alle informasjons-systemene som er i bruk. Manglende virksomhetsarkitektur er også trukket fram som en årsak til utfordringene med interoperabilitet mellom kommando- og kontrollinformasjonssystemene og som en av grunnene til at målet om å redusere antallet systemer i Forsvaret, ikke nås.

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

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

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

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

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

Forsvarsdepartementet er ansvarlig for den overordnede styringen og kontrollen av underliggende etater. Departementet bemerker at det har vært utfordrende å styre Forsvaret helhetlig på IKT-området. Forsvarsstaben har etter departementets vurdering ikke hatt tilstrekkelig kapasitet til å fastsette operative krav til IKT, prioritere på tvers av driftsenhetene og mellom investering og drift, eller være et felles kontaktpunkt mot departementet når det gjelder IKT. Sjefen for Forsvarsstaben erkjenner at Forsvarsstabens kompetanse og styring på IKT-området har vært for dårlig, men viser til at det nå er tatt grep for å endre på dette. Kompetansen på IKT i forsvarsstaben er styrket de siste par årene og fra 2021 er ansvaret for

gjennomføringen av *IKT-strategi for forsvarssektoren* overført fra departementet til Forsvaret. Med dette har Forsvaret fått ansvar for IKT-området i forsvarssektoren som helhet. I tillegg er rollen som prosjekteier i investeringsprosjekter overført fra departementet til forsvarssjefen. Både departementet og Forsvaret mener at overføringen av mer ansvar til Forsvaret legger bedre til rette for en helhetlig styring på IKT-området.

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

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

Forsvaret og Forsvarsmateriell er tydelige på at det etter etableringen av Forsvarsmateriell i 2016 var nødvendig å avklare ansvars- og rollefordelingen mellom etatene på IKT-området. I langtidsplanen for 2017–2020 gikk det også fram at Forsvarsdepartementet forventet at ansvars- og rollefordelingen mellom etatene skulle avklares. Forsvarsdepartementet viser til at det ble utarbeidet retningslinjer for rolle- og ansvarsfordelingen mellom Forsvarsmateriell og Forsvaret da Forsvarsmateriell ble etablert, men at det har vært utfordrende å etterleve retningslinjene. Departementet erkjenner at dette har resultert i noe overlappende oppgaveutførelse og lav gjennomføringsevne. Cyberforsvaret viser til at forholdet mellom Forsvaret ved Cyberforsvaret og Forsvarsmateriell er en del av forklaringen på at Forsvaret har brukt betydelige summer på ny teknologi uten å ha fått utnyttet disse investeringene til fulle.

Undersøkelsen viser at det er lagt ned et omfattende arbeid for å avklare ansvars- og rollefordelingen mellom Forsvaret og Forsvarsmateriell. Dette har blant annet ført til at oppgaver og personell er blitt overført mellom etatene. Både Forsvaret, Forsvarsmateriell og departementet mener at ansvarsfordelingen nå er blitt klarere, og at samarbeidet er blitt bedre. Samtidig ser vi at det ved overgangen til den nye langtidsperioden gjenstår en del utfordringer knyttet til ansvarsfordelingen. Blant annet viser Forsvarsmateriell til at etaten fortsatt jobber med å finne sin rolle på enkelte områder, og at det fremdeles er noe overlapp mellom oppgavene som utføres av Forsvaret og Forsvarsmateriell.

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

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

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

Manglende kompetanse er en medvirkende årsak til flere av utfordringene som beskrives i denne undersøkelsen, og til at forsvarssektoren ikke har klart å løse mange av utfordringene på IKT-området. Når det gjelder mangelen på ulike typer IKT-kompetanse, er forsvarssektoren på linje med forvaltningen og samfunnet for øvrig. Sjefen for Cyberforsvaret viser til at det er utfordrende å rekruttere personell som både har riktig IKT- og militærfaglig kompetanse. Vi merker oss imidlertid at Svendsen-utvalget i 2020 påpeker at Forsvaret ikke har klart å henge med i utviklingen eller evnet å omstille seg i takt med behovet for ny kompetanse for å utnytte teknologien og møte den økende trusselen i det digitale rom. Dette er bekymringsfullt med tanke på dagens trusselbilde og på hvor viktige effektive og sikre IKT-systemer er for Forsvarets operative evne.

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

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

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

Faktaboks 5 Programmene Mime og MAST

Mime er et program hvor Forsvarsmateriell har samlet en rekke prosjekter som skal modernisere informasjons- og kommunikasjonssystemene for taktisk ledelse i Forsvaret.
MAST (militær anvendelse av skytjenester) inkluderer investeringsprosjekter for IKT-plattformer for alle formål i Forsvaret, inkludert kommando og kontroll. Målet er at nye skyløsninger skal erstatte og oppgradere Forsvarets eksisterende løsninger. Forsvarsmateriell beskriver MAST som grunnsteinen for digitalisering av Forsvaret. Forsvarsdepartementet presiserer at modellen for skytjenester i Forsvaret ikke innebærer teknologier som forutsetter leveranser over internett.

Kilde: Forsvarsmateriell.no, intervju med Forsvarsdepartementet juni 2021

Programmet Mime skal avsluttes i 2030, mens programmet MAST skal vare til 2028. Etter den innledende etablerings- og oppstartsfasen er begge

programmene forsinket. Flere sentrale spørsmål som har betydning for gjennomføringen og leveransene fra programmene står dessuten ubesvart. Riksrevisjonen mener dette utgjør en risiko for ytterligere forsinkelser og mangelfull gevinstrealisering.

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

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

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

Programorganiseringen i Mime og MAST skal legge til rette for å kunne se IKT-investeringer i sammenheng og vurdere innbyrdes avhengigheter mellom dem i prioriteringen av ressurser. Ut fra
dette er det bekymringsfullt at ekstern kvalitetssikring av Mime peker på at det er utfordringer med å foreta kost-nyttevurderinger og prioritere ut fra foreliggende styringsinformasjon.

Programorganisasjonen peker på at det både er behov for å avklare ambisjonsnivå og for å se på sammenhengen med investeringer som faller utenfor programmet. Dette forsterker et inntrykk av vesentlige svakheter i styringsinformasjonen og risiko for gjennomføringen av programmene. Programorganisasjonen for Mime og MAST gir så sent som i juni 2021 – ett år etter den formelle oppstarten av prosjektene i Mime – uttrykk for at den mangler verktøyene som trengs for å gjennomføre programmet som forutsatt. Når det gjelder MAST, er programmets virkeområde ikke avklart ved overgangen til gjennomføringsfasen

Forsvarssektoren har trukket fram leveransene fra Mime og MAST som avgjørende for at forsvarssektoren skal nå målene om digitalisering, effektivisering og økt operativ evne. Behovet for mer effektiv og sikker IKT-

støtte i Forsvarets operasjoner bekreftes i denne undersøkelsen. Utsettelser og mangelfull gevinstrealisering fra Mime og MAST er derfor ikke bare et kostnads- og ressursspørsmål. En eventuell manglende realisering av ambisjonene i programmene har konsekvenser for Forsvarets operativ evne, både på kort og lang sikt.

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

4 Anbefalinger

Riksrevisjonen anbefaler at Forsvarsdepartementet

- følger opp arbeidet med å få en fullstendig oversikt over informasjonssystemer i Forsvaret, og at denne blir brukt som grunnlag for Forsvarets styring og investeringer på IKT-området
- sørger for at Forsvaret og Forsvarsmateriell intensiverer arbeidet med variantbegrensning av Forsvarets informasjonssystemer
- i dialog med Forsvaret og Forsvarsmateriell sikrer løsninger for kommunikasjon og informasjonsutveksling som raskere gir full utnyttelse av kapasiteter ved anskaffelser av nytt materiell
- følger opp at sikkerhetsstyringen styrkes og at informasjonssikkerheten ivaretas i nye og eksisterende informasjonssystemer i Forsvaret
- styrker Forsvarets evne til 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

5 Statsrådens svar

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

5.1 Evne til å realisere effektive og sikre informasjonssystemer

Statsråden viser til *IKT-strategi for forsvarssektoren* som ble gitt ut i 2019, og mener at strategiens tiltaksområder står seg som svært relevante i møtet med Riksrevisjonens kritikk, til tross for at implementerte tiltak så langt har hatt begrenset effekt. Statsråden viser til at Forsvarsdepartementet i samråd med Forsvaret og Forsvarsmateriell utarbeider en plan for å øke gjennomføringsevnen med utgangspunkt i IKT-strategien. Statsråden mener

derfor at det på nåværende tidspunkt er for tidlig å avvikle eller reversere besluttede tiltak, og oppgir at hans første prioritering er å følge opp at de grunnleggende premissene for realiseringen av strategien kommer på plass.

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

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

Statsråden viser til at det gjennom virksomhetsprogrammene Mime (kampnær IKT) og MAST (militær anvendelse av skytjenester) etableres en ny operasjonsmodell for IKT i forsvarssektoren, og at Forsvarsdepartementet vil følge opp risikoene som Riksrevisjonen har påpekt og tiltakene som ekstern kvalitetssikrer har anbefalt.

Statsråden opplyser også om at Forsvarsdepartementet forsterker oppfølgingen av IKT-området gjennom etatsstyringen. Dette inkluderer regelmessige fag- og styringsmøter mellom Forsvarsdepartementet og etatene, og krav til utfyllende rapportering på IKT-området.

5.2 Manglende realisering av effektive kommando- og kontrollinformasjonssystemer

Statsråden viser til virksomhetsprogrammet at Mime er sentralt i utbedringen av flere av de konkrete kommunikasjonsutfordringene som Riksrevisjonen viser til i sin undersøkelse. Gjennom toårlige leveranser fram mot 2030 skal programmet levere kampnær IKT til Forsvaret.

Delleveransene som er godkjent av Stortinget, inkluderer en felles, taktisk IKT-plattform, satellitterminaler, bakke-til-luft-radioer, datalinkterminaler og programvare for kommando og kontroll, nye taktiske radioer til landstyrkene og starte fornyelsen av kommando- og kontrollsystemer for luftdomenet. Statsråden viser videre til at Forsvarets evne til å samvirke på tvers av graderingsnivåer er forbedret gjennom en løsning for sikker informasjonsutveksling mellom sikkerhetsdomener, som ble levert av Forsvarsmateriell i 2021–2022.

5.3 Sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer

Statsråden peker på at Forsvarsdepartementet har informert Stortinget om at Forsvaret og Forsvarsmateriell har utfordringer med å beskytte informasjonssystemer i samsvar med sikkerhetslovens krav om et forsvarlig sikkerhetsnivå, og opplyser om at departementet vil videreføre sin særskilte oppfølging av Forsvarets og Forsvarsmateriells arbeid med informasjonssikkerhet så lenge det er behov for dette. Statsråden peker

videre på at sikkerhetstilstanden i IKT-porteføljen påvirkes av andre utfordringer på IKT-området, og at det derfor også fra et sikkerhetsperspektiv er svært viktig at moderniseringen av Forsvarets IKT lykkes.

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

5.4 Personell og kompetanse

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

5.5 Avslutning

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

6 Riksrevisjonens uttalelse til statsrådens svar

Riksrevisjonen har ingen ytterligere merknader.

Saken sendes Stortinget.

Vedtatt i Riksrevisjonens møte 23. august 2022

Karl Eirik Schjøtt-Pedersen Tom-Christer Nilsen

Helga Pedersen Anne Tingelstad Wøien Arve Lønnum

_____

Jens Gunvaldsen

Vedlegg

Vedlegg 1:

Riksrevisjonens brev til statsråden i Forsvarsdepartementet

Riksrevisjonen

Vår saksbehandler
Bente Willumsen 22241488
Vår dato: 22.06.2022
Vår referanse: 2019/01250-20
Deres dato:
Deres referanse:

FORSVARSDEPARTEMENTET
Postboks 8126 DEP
0032 OSLO

Oversendelse av dokument 3 : X Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner

Vedlagt oversendes utkast til Dokument 3:x (2022–2023) *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner.*

Vedlagt oversendes også, etter dialog med departementet, en ugradert versjon av dokumentet.

Dokumentet er basert på rapport oversendt Forsvarsdepartementet ved vårt brev 23. november 2021, og på departementets svar 17. desember 2021.

Statsråden bes redegjøre for hvordan departementet vil følge opp Riksrevisjonens konklusjoner og anbefalinger, og eventuelt om departementet er uenig med Riksrevisjonen. Departementets oppfølging vil bli sammenfattet i det endelige dokumentet til Stortinget. Statsrådens svar vil i sin helhet bli vedlagt dokumentet.

Stortinget vil motta både det graderte og det ugraderte dokumentet til behandling. Vi ber derfor om to svar fra statsråden, ett svar som kan følge det graderte dokumentet og som kan inneholde graderte opplysninger, og ett svar som kan følge det ugraderte dokumentet.

Svarfrist: 1. juli 2022

For riksrevisorkollegiet

Karl Eirik Schjøtt-Pedersen

riksrevisor

Vedlegg:

Dokument 3:x (2022–2023) *Riksrevisjonens undersøkelse av Forsvaret informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner (KONFIDENSIELT).*

Dokument 3:x (2022–2023) *Riksrevisjonens undersøkelse av Forsvaret informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner (UGRADERT).*

Uten vedlegg er dette dokumentet ugradert.

Brevet er godkjent og ekspedert digitalt.

Vedlegg 2:

Statsrådens svar

DET KONGELIGE
FORSVARSDEPARTEMENT

Statsråden

Riksrevisjonen
Postboks 8130 Dep
0032 OSLO

Deres ref.:	Vår ref.:	Dato:
2019/01250-20	2019/50364-78	08.07.2022

Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner - statsrådens uttalelse

Jeg viser til brev fra Riksrevisjonen datert 17. juni 2022, vedrørende utkast til Dokument 3:x (2022-2023) *Riksrevisjonens undersøkelse av Forsvarets informasjonssystemer for kommunikasjon og informasjonsutveksling i operasjoner*.

Målet med Riksrevisjonens undersøkelse har vært å vurdere om Forsvarets kommando- og kontrollinformasjonssystemer understøtter Forsvarets operative evne gjennom effektiv og sikker kommunikasjon og om styringen av IKT-området i forsvarssektoren har lagt til rette for effektive og sikre systemer i tråd med forutsetningene fra Stortingets behandling av Prop. 151 S (2015-2016) *Kampkraft og bærekraft – langtidsplan for forsvarssektoren 2017-2020*, jf. Innst. 62 S (2016-2017). Undersøkelse omfatter primært perioden 2017-2020.

Riksrevisjonen har i sin undersøkelse funnet at Forsvaret ikke har utfordringer med å løse sitt oppdrag i daglige operasjoner, og at kommunikasjon og informasjonsutveksling mellom Forsvarets operative hovedkvarter og de taktiske kommandoene i grenene fungerer godt. Riksrevisjonen konkluderer samtidig med at det finnes mangler i sikkerheten og i samvirket mellom Forsvarets kommando- og kontrollinformasjonssystemer og at dette kan få følger for Forsvarets operative evne. Riksrevisjonen konkluderer også med at Forsvarsdepartementet, Forsvaret og Forsvarsmateriell i liten grad har klart å svare ut forventningene til IKT-porteføljen, styring og organisering som følger av Prop. 151 S (2015-2016) og ikke har greid å realisere effektive og sikre informasjonssystemer som forutsatt i langtidsplanen.

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

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

1. Evne til å realisere effektive og sikre informasjonssystemer

Riksrevisjonen kritiserer Forsvarsdepartementet, Forsvaret og Forsvarsmateriell for å i liten grad møte forventningene som ble stilt i Prop. 151 S (2015-2016), både når det gjelder IKT-porteføljen og styring og organisering. Riksrevisjonen peker også på at forsvarssektoren har bred erkjennelse av utfordringene på området, men at evnen til å løse disse har vært begrenset.

Forsvarsdepartementet fant i 2018 at det var behov for å etablere et mer helhetlig og felles målbilde og en strategi for IKT-området i sektoren, i tillegg til en overordnet plan for utvikling av IKT-virksomheten. *IKT-strategi for forsvarssektoren* ble gitt ut i 2019. Til grunn for tiltaksområdene i strategien ligger det en grundig analyse av utfordringsbildet innenfor IKT-området i forsvarssektoren. I analysen identifiseres mange av de samme forholdene som Riksrevisjonen har funnet i sin undersøkelse. Tiltaksområdene i IKT-strategien omfatter blant annet etablering av en styringsmodell for å oppnå styrket styring, videreutvikling av porteføljestyring, arkitekturstyring og tydeliggjøring av prosesser og ansvar. Tiltakene i IKT-strategien er omfattende og strekker seg over tid. De innebærer gjennomgående endringer både i Forsvarsdepartementet og i etatene når det gjelder hvordan forsvarssektoren forvalter, utvikler, investerer og styrer innenfor IKT-området.

Jeg mener strategiens tiltaksområder står seg som svært relevante i møtet med Riksrevisjonens kritikk, til tross for at implementerte tiltak så langt har hatt begrenset effekt. Erkjennelsen av at situasjonen er alvorlig og tidskritisk er høy, men jeg mener samtidig det er viktig at grunnlagsarbeidet gjøres riktig. Det er avgjørende at de grunnleggende årsakene til at tiltakene ikke har gitt den planlagte effekten identifiseres og adresseres for at strategien kan realiseres. Forsvarsdepartementet utarbeider i samråd med Forsvaret og Forsvarsmateriell en plan for å øke gjennomføringsevnen med utgangspunkt i IKT-strategien. Jeg mener derfor også at det på nåværende tidspunkt også er for tidlig å avvikle eller reversere besluttede tiltak.

Min første prioritering er å følge opp at de grunnleggende premissene for realisering av strategien kommer på plass. Et tydelig, dokumentert og etterlevd styringssystem for IKT-området er sentralt. En justert styringsmodell vil gi tydeligere rammer, prinsipper og etterlevelse av strategiske føringer, øke effekten av allerede iverksatte tiltak og gi bedre forutsetninger for prioriteringer og videre forbedring. Forsvaret har gjennom tildelingsbrevet for 2022 fått et oppdrag som blant annet omfatter forutsetninger for å realisere IKT-strategien og å gi anbefalinger om en styringsmodell for IKT. Forsvarsdepartementet følger opp arbeidet gjennom etatsstyringen og i fagmøter.

Gjennom videreutvikling av investeringsprosessene styrket Forsvarsdepartementet i 2019 den strategiske styringen av investeringsporteføljen. Endringen fra 1. januar 2020 ga forsvarssjefen et tydeligere ansvar for investering, drift og gevinstrealisering innenfor IKT-området.

Det er sivile og kommersielle virksomheter som i dag er de største driverne i den teknologiske utviklingen. Samtidig står forsvarssektoren overfor en omfattende omstilling og

modernisering. Det er i denne prosessen nødvendig at forsvarssektoren har tilgang til oppdatert teknologi, løsninger og kompetanse på områder der industrien er ledende. For å oppnå dette vurderes det også strategisk samarbeid med en eller flere samarbeidspartnere. Det er for virksomhetsprogrammet Mime nylig inngått et slikt strategisk samarbeid med Kongsberg Defence & Aerospace. Gjennom virksomhetsprogrammene Mime (kampnær IKT) og MAST (militær anvendelse av skytjenester) etableres det også en ny operasjonsmodell for IKT i forsvarssektoren.

Det er gjennomført ekstern kvalitetssikring på både program- og leveransebølgenivå for virksomhetsprogrammet Mime. Det vil bli gjennomført tilsvarende kvalitetssikring for fremtidige leveransebølger. Riksrevisjonen peker på risiko forbundet med fremdrift og gevinstrealisering i virksomhetsprogrammene. Forsvarsdepartementet vil følge opp risikoene som er påpekt og tiltakene som ekstern kvalitetssikrer har anbefalt.

Forsvarsdepartementet gjennomfører nå også flere tiltak som forsterker oppfølgingen av IKT-området gjennom etatsstyringen. Dette inkluderer regelmessige fagmøter- og styringsmøter mellom Forsvarsdepartementet og etatene samt krav til utfyllende rapportering på IKT-området.

2. Manglende realisering av effektive kommando- og kontrollinformasjonssystemer

Riksrevisjonen finner, som omtalt innledningsvis, at Forsvaret ikke har utfordringer med å løse sitt oppdrag i daglige operasjoner, og at kommunikasjon og informasjonsutveksling mellom Forsvarets operative hovedkvarter og de taktiske kommandoene i grenene fungerer godt. Riksrevisjonen peker samtidig på at det finnes mangler i interoperabiliteten mellom Forsvarets ulike kommando- og kontrollinformasjonssystemer.

Virksomhetsprogrammet Mime står sentralt i utbedringen av flere av de konkrete kommunikasjonsutfordringene Riksrevisjonen viser til i sin undersøkelse. Gjennom toårlige leveransebølger som blir gjennomført suksessivt frem mot 2030 skal programmet levere kampnær IKT til Forsvaret. Programmets første leveransebølge ble godkjent av Stortinget i forbindelse med behandlingen av Prop. 1 S (2021-2022) og skal ta frem delleveranser som inkluderer en felles, taktisk IKT-plattform, anskaffelse av satellitterminaler, bakke-til-luft radioer, datalinkterminaler og programvare for kommando og kontroll, i tillegg til å anskaffe nye taktiske radioer til landstyrkene og starte fornyelsen av kommando- og kontrollsystem for luftdomenet. Forsvarets evne til samvirke på tvers av graderingsnivåer er også forbedret gjennom en løsning for sikker informasjonsutveksling mellom sikkerhetsdomener, levert av Forsvarsmateriell i 2021-2022.

3. Sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer

Riksrevisjonen peker i sin rapport på at sårbarheter i sikkerheten i Forsvarets kommando- og kontrollinformasjonssystemer kan påvirke Forsvarets operative evne. Forsvarsdepartementet har i Prop. 1 S (2021-2022) informert Stortinget om at Forsvaret og Forsvarsmateriell har

utfordringer knyttet til å beskytte informasjonssystemer i samsvar med sikkerhetslovens krav om et forsvarlig sikkerhetsnivå. Forsvarsdepartementets særskilte oppfølging av Forsvarets og Forsvarsmateriells arbeid med informasjonssikkerhet gir resultater og vil videreføres så lenge det er behov for dette. Sikkerhetstilstanden i IKT-porteføljen påvirkes av andre utfordringer på IKT-området. Det er derfor svært viktig også fra et sikkerhetsperspektiv at moderniseringen av Forsvarets IKT lykkes.

Riksrevisjonen mener det er behov for å styrke Forsvarets evne til å avdekke og håndtere digitale angrep. Gjennom Prop. 14 S (2020-2021) *Evne til forsvar – vilje til beredskap* foreligger det en plan for utvikling av Forsvarets evne på området gjennom styrking av Cyberforsvarets cybersikkerhetssenter (milCERT). Oppbyggingen av milCERT går i henhold til plan og full operativ kapasitet nås i 2024. Som meddelt i Meld. St. 10 (2021–2022) *Prioriterte endringer, status og tiltak i forsvarssektoren* ville Forsvarsdepartementet se nærmere på ytterligere tiltak for å styrke Forsvarets evne i det digitale rom. Forsvarets kapasitet til å oppdage og håndtere uønskede digitale hendelser ble derfor også styrket gjennom Prop. 78 S (2021-2022) *Endringer i statsbudsjettet 2022*.

4. Personell og kompetanse

Riksrevisjonen anbefaler at Forsvarsdepartementet vurderer ytterligere tiltak for å rekruttere, utvikle og beholde nødvendig fagkompetanse på IKT-området i forsvarssektoren. Behovet og etterspørselen etter IKT-sikkerhetskompetanse er større enn tilbudet. Dette forholdet gjør seg gjeldende også for etatene i forsvarssektoren, som har de samme utfordringene med tilgang til kompetanse på IKT-området som samfunnet for øvrig, og som konkurrerer om de samme kandidatene som andre offentlige virksomheter og privat næringsliv. For å øke tilgangen på relevant kompetanse, herunder et særskilt behov for kompetanse innen teknologi og digitalisering, skal Forsvaret i tråd med gjeldende langtidsplan videreutvikle og øke utnyttelsen av verneplikten, lærlingeordningen, reservistordningen og samarbeids-ordninger med allierte, næringslivet, sivile utdanningsinstitusjoner og andre sektorer. Dette er også i tråd med gjeldende politikk på området. Forsvarsdepartementet følger opp kompetanse som en integrert del av styringen av etatene.

5. Avslutning

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

Med hilsen

Bjørn Arild Gram

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