STORTINGET

# Innst. 287 S

**(2022–2023)**

Innstilling til Stortinget
fra kontroll- og konstitusjonskomiteen

Dokument 3:7 (2022–2023)

**Innstilling fra kontroll- og konstitusjonskomiteen om Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor**

Til Stortinget

## 1. Sammendrag

### 1.1 Innledning

I den siste samfunnssikkerhetsmeldingen fra 2020 går det fram at digital sikkerhet er helt avgjørende for å ivareta velferdssamfunnet, viktige samfunnsfunksjoner og nasjonale sikkerhetsinteresser.

De nasjonale etterretnings- og sikkerhetstjenestene har over flere år vurdert etterretningstrusselen som den største trusselen mot Norge. Politiets sikkerhetstjeneste viser til at digitale operasjoner har blitt en integrert del av andre lands etterretningstjenester. Det vises også til at statlige etterretningsaktører i andre land har gjennomført sabotasje ved hjelp av digitale angrep. Ifølge Nasjonal sikkerhetsmyndighet har det i perioden 2019 til 2021 vært en tredobling i antall alvorlige digitale hendelser og angrep mot offentlige og private virksomheter i Norge. Både Nasjonal sikkerhetsmyndighet og Politiets sikkerhetstjeneste rapporterer om økt digital trusselaktivitet i Norge som følge av krigen i Ukraina.

En økende grad av digitalisering og samarbeid på tvers av sektorer og landegrenser gjør samfunnet vårt mer sårbart for digitale trusler. Et digitalt angrep kan få store negative konsekvenser for Norge ved at funksjoner som er kritiske for stat og samfunn, rammes. Dette kan for eksempel være betalingssystemer, helsevesenet, kraftforsyningen, elektronisk kommunikasjon eller transport.

Arbeidet med digital sikkerhet berører hele samfunnet og krever derfor samordning av aktører og virkemidler på tvers av sektorene. Det er Justis- og beredskapsdepartementet som siden 2013 har hatt ansvar for samordningen av samfunnssikkerhetsarbeidet og digital sikkerhet i sivil sektor. Departementet har videre et overordnet ansvar for det forebyggende sikkerhetsarbeidet i sivil sektor.

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

- Meld. St. 5 (2020–2021) Samfunnssikkerhet i en usikker verden, jf. Innst. 275 S (2020–2021)
- Meld. St. 38 (2016–2017) IKT-sikkerhet. Et felles ansvar, jf. Innst. 187 S (2017–2018)
- kgl.res. av 10. mars 2017 nr. 312: Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet
- instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen), 2017
- lov om nasjonal sikkerhet (sikkerhetsloven), 2019

Målet med undersøkelsen har vært å vurdere hvorvidt Justis- og beredskapsdepartements samordning av arbeidet med å ivareta den digitale sikkerheten i sivil sektor er effektiv og i tråd med Stortingets vedtak og forutsetninger.

Undersøkelsesperioden er i hovedsak 2018–2021, men Riksrevisjonen har også tatt med relevante data fra 2022 når disse har vært tilgjengelige.

I undersøkelsen har Riksrevisjonen sett nærmere på arbeidet med digital sikkerhet i flere sektorer, der ansvaret i hver enkelt sektor ligger hos det enkelte sektordepartement. Riksrevisjonen påpeker svakheter og utfordringer i enkelte virkemidler og tiltak som disse departementene har ansvar for. Når det er svakheter i samordningen av disse tiltakene, retter Riksrevisjonen kritikken mot Justis- og beredskapsdepartementet på grunn av departementets samordningsansvar for den digitale sikkerheten nasjonalt.

Store deler av undersøkelsesperioden har vært preget av koronapandemien, som kom til Norge i februar 2020. Pandemien har påvirket både myndighetene og samfunnet for øvrig på mange forskjellige måter. Nasjonal sikkerhetsmyndighet viser for eksempel til at utstrakt bruk av hjemmekontorløsninger har skapt nye digitale sårbarheter. Pandemien økte presset mot enkelte sektorer og samfunnsfunksjoner som hadde sentrale oppgaver i pandemihåndteringen. Justis- og beredskapsdepartementet viser til at departementet og underliggende etater over en lengre periode har stått i en ekstraordinær situasjon der sikkerhets- og beredskapsressurser har måttet bistå i pandemihåndteringen. Departementet står nå i en tilsvarende situasjon, med krig i Ukraina og samordning av sivile behov. Andre etater som omfattes av undersøkelsen, har også pekt på at restriksjonene som fulgte av pandemien, har påvirket arbeidet samfunnssikkerhet og digital sikkerhet. Riksrevisjonen bemerker at konsekvensene av svakheter og mangler i arbeidet med digital sikkerhet like fullt er de samme, og at det ofte vil være nødvendig å håndtere flere ulike risikoer og hendelser samtidig.

Rapporten ble forelagt Justis- og beredskapsdepartementet ved brev 13. oktober 2022. Departementet har i brev 11. november 2022 gitt kommentarer til rapporten. Kommentarene er i hovedsak innarbeidet i rapporten og i Riksrevisjonens Dokument 3:7 (2022–2023).

Rapporten, riksrevisorkollegiets oversendelsesbrev til departementet 30. november 2022 og statsrådens svar 16. desember 2022 følger som vedlegg til Riksrevisjonens dokument.

## 1.2 Konklusjoner

- Svak samordning av roller, ansvar og krav gjør arbeidet med digital sikkerhet krevende for virksomhetene.
- Justis- og beredskapsdepartementet har ikke sørget for god nok informasjon om den nasjonale digitale sikkerhetstilstanden.
- Justis- og beredskapsdepartementet har ikke sørget for god nok oppfølging av Nasjonal strategi for digital sikkerhet.
- Justis- og beredskapsdepartementet har ikke lagt godt nok til rette for tverssektoriell hendelseshåndtering.

## 1.3 Overordnet vurdering

Samlet sett er det kritikkverdig at Justis- og beredskapsdepartementet med underliggende etater ikke har ivaretatt samordnings- og pådriveransvaret godt nok til å møte utfordringene på det digitale sikkerhetsområdet.

Det er videre kritikkverdig at

- Justis- og beredskapsdepartementet ikke har ivaretatt sitt pådriveransvar for å bidra til tilstrekkelig framdrift i arbeidet som følger av ny sikkerhetslov.
- Justis- og beredskapsdepartementet ikke har lagt godt nok til rette for tverrsektoriell hendelseshåndtering.
- det gjennomføres få tilsyn med digital sikkerhet, og tilsynsmyndighetene er lite samordnet.

## 1.4 Utdyping av konklusjoner

Justis- og beredskapsdepartementets samordnings- og pådriveransvar på samfunnssikkerhetsområdet innebærer blant annet å initiere og koordinere prosesser på tvers av departementer, veilede departementene i arbeidet de gjør på området, og sørge for at problemstillinger på tvers av sektorer blir håndtert. Videre skal Justis- og beredskapsdepartementet utforme regjeringens politikk for den digitale sikkerheten nasjonalt, blant annet nasjonale strategier. Justis- og beredskapsdepartementet har fullmakt til å stille krav til departementenes samfunnssikkerhetsarbeid, etablere nasjonale krav til den digitale sikkerheten og gi nærmere bestemmelser om sin egen samordningsrolle og tilsynsfunksjon. Samordningsansvaret innebærer også å sørge for at myndighetene har en helhetlig tilnærming til digital sikkerhet, og at kompetansen på digital sikkerhet møter framtidens behov. Nasjonal sikkerhetsmyndighet og Direktoratet for samfunnssikkerhet og beredskap utøver viktige samordningsoppgaver for departementet på samfunnssikkerhetsområdet.

Ifølge Justis- og beredskapsdepartementet har samordningen mellom etatene innenfor området digital sikkerhet hatt en positiv utvikling, både på departements- og etatsnivå. Departementet viser samtidig til at sektorprinsippet, varierende prioritering av sikkerhetsarbeidet i departementene og samarbeidsutfordringer mellom departementene gjør samordningen krevende.

Undersøkelsen viser at det er flere utfordringer med samordningen av arbeidet med digital sikkerhet som ikke har blitt håndtert. Justis- og beredskapsdepartementet har ikke sørget for at samordningen av roller, ansvar og krav er god nok når det gjelder dette arbeidet.

Riksrevisjonen finner også at Justis- og beredskapsdepartementet ikke har tilstrekkelig oversikt over den nasjonale digitale sikkerhetstilstanden, særlig fordi departementenes arbeid med å kartlegge virksomheter som understøtter grunnleggende nasjonale funksjoner, går for sakte. Justis- og beredskapsdepartementet følger i liten grad opp hvilken effekt tiltakene i nasjonale strategier på det digitale sikkerhetsområdet har, og siden 2016 har de ikke sørget for at det på nasjonalt nivå har blitt øvd godt nok på å håndtere alvorlige digitale angrep som treffer flere sektorer.

Det er Riksrevisjonens vurdering at Justis- og beredskapsdepartementet med underliggende etater ikke ivaretar pådriver- og samordningsansvaret godt nok til å møte utfordringene på det digitale sikkerhetsområdet. Dette medfører risiko for at funksjoner som er kritiske for både stats- og samfunnssikkerheten, ikke er godt nok beskyttet mot digitale angrep, og at alvorlige digitale angrep ikke håndteres effektivt. Samlet sett vurderer Riksrevisjonen at dette er kritikkverdig.

### 1.4.1 Svak samordning av roller, ansvar og krav gjør arbeidet med forebyggende digital sikkerhet krevende for virksomhetene

Den nasjonale digitale sikkerheten reguleres av flere forskjellige regelverk. Regelverkene forvaltes av en rekke ulike aktører som har ansvar for at det føres tilsyn etter regelverkene, og for at det gis veiledning i hvordan regelverkene skal etterleves.

Ifølge samfunnssikkerhetsmeldingen er det satt et mål om at all rådgivning og veiledning om digital sikkerhet fra myndighetene skal være harmonisert og ensrettet. Justis- og beredskapsdepartementet skal bidra til at rådgivnings- og veiledningsaktiviteter innenfor digital sikkerhet blir bedre koordinert.

Riksrevisjonens undersøkelse viser imidlertid at myndighetenes samordning av arbeidet med veiledning og tilsyn er svak, og at potensialet i sentrale samordningsarenaer ikke utnyttes fullt ut. Den svake samordningen gjør det forebyggende sikkerhetsarbeidet krevende for offentlige og private virksomheter.

#### 1.4.1.1 Sentrale samordningsarenaer er lite forpliktende for deltakerne og bidrar i varierende grad til samordning

Det er etablert en rekke ulike samordningsarenaer som på forskjellige måter skal bidra til å samordne aktører med roller og ansvar knyttet til digital sikkerhet. Undersøkelsen viser imidlertid at disse arenaene i varierende grad bidrar til samordning av aktørene.

I tiltaksoversikten tilhørende Nasjonal strategi for digital sikkerhet (2019) trekkes det fram seks samordningsarenaer som skal understøtte målet om styrket samordning mellom aktørene og målet om å skape et felles situasjonsbilde på det digitale sikkerhetsområdet. De seks arenaene er: Felles cyberkoordineringssenter, Forum for digital sikkerhet, Forum for IKT-tilsyn, Nasjonalt cybersikkerhetssenter, Nettverk for nasjonal IKT-sikkerhet og Nettverk for veiledningsaktører innen styring og kontroll. I tillegg trekkes Samhandlingsarena for sektortilsyn etter sikkerhetsloven i samfunnssikkerhetsmeldingen fram som sentral for samordning av myndigheter med ansvar for å føre tilsyn etter sikkerhetsloven. Tabell 1 fra Riksrevisjonens dokument viser deltakere og formål for de nevnte samordningsarenaene (unntatt Felles cyberkoordineringssenter).

*Tabell 1 Samordningsarenaer innenfor forebyggende digital sikkerhet – deltakere og formål*

| Navn og deltakere | Formål |
|---|---|
| **Forum for digital sikkerhet**<br>Representanter fra myndighetene, næringslivet, organisasjoner og akademia. Ledes av Nasjonal sikkerhetsmyndighet. | Skal legge til rette for diskusjon av strategiske spørsmål knyttet til digital sikkerhet mellom private og offentlige aktører og myndigheter. |
| **Forum for IKT-tilsyn**<br>Digitaliseringsdirektoratet, Direktoratet for strålevern og atomsikkerhet, Finanstilsynet, Kystverket, Luftfartstilsynet, Mattilsynet, Nasjonal kommunikasjonsmyndighet, Norges vassdrags- og energidirektorat, Petroleumstilsynet, Sjøfartsdirektoratet og Statens jernbanetilsyn. Ledes av Nasjonal sikkerhetsmyndighet. | Skal koordinere arbeidet mellom myndigheter som fører tilsyn med digital sikkerhet. |
| **Nasjonalt cybersikkerhetssenter**<br>Virksomheter fra offentlig og privat sektor. Ledes av Nasjonal sikkerhetsmyndighet. | Skal fungere som et nasjonalt responsmiljø for håndtering av digitale hendelser, og som et knutepunkt mellom privat og offentlig sektor i arbeidet med digital sikkerhet. |
| **Nettverk for nasjonal IKT-sikkerhet**<br>Alle departementer. Ledes av Justis- og beredskapsdepartementet. | Skal sørge for at strategiske spørsmål knyttet til internasjonalt samarbeid og digitale sikkerhetsutfordringer blir diskutert og koordinert mellom departementene. |

| Navn og deltakere | Formål |
|---|---|
| **Nettverk for veiledningsaktører innen styring og kontroll**<br>Datatilsynet, Direktoratet for e-helse, Direktoratet for samfunnssikkerhet og beredskap, Nasjonal kommunikasjonsmyndighet, Nasjonal sikkerhetsmyndighet, Kommunesektorens organisasjon og Foreningen Kommunal Informasjonssikkerhet. Ledes av Digitaliseringsdirektoratet. | Skal legge til rette for informasjonsutveksling om pågående samordningsprosjekter og samarbeide om ulike tema under styring og kontroll. |
| **Samhandlingsarena for sektortilsyn etter sikkerhetsloven**<br>Nasjonal kommunikasjonsmyndighet, Nasjonal sikkerhetsmyndighet (leder) og Norges vassdrags- og energidirektorat. | Skal legge til rette for kunnskaps- og erfaringsutveksling for å sikre kvalitet og enhetlig praksis i tilsynsvirksomhet etter sikkerhetsloven. |

Nasjonalt cybersikkerhetssenter har oppgaver knyttet til både forebyggende sikkerhetsarbeid og hendelseshåndtering. Senterets oppgaver knyttet til hendelseshåndtering omtales i punkt 1.4.4. Basert på undersøkelsen vurderer Riksrevisjonen Nasjonalt cybersikkerhetssenter som en velfungerende samordningsarena innenfor forebyggende sikkerhetsarbeid. Senteret arrangerer jevnlige og hyppige møter med relevante tema og legger til rette for erfaringsutveksling mellom deltakerne. Deltakerne opplever begge deler som nyttig.

Når det gjelder Nettverk for nasjonal IKT-sikkerhet, Forum for digital sikkerhet, Forum for IKT-tilsyn og Nettverk for veiledningsaktører innen styring og kontroll, viser undersøkelsen at deltakerne i hovedsak bruker arenaene for å dele informasjon og orientere hverandre om pågående arbeid. Møteaktiviteten har dessuten vært lav. For eksempel har det i Nettverk for veiledningsaktører innen styring og kontroll kun blitt avholdt fire møter siden desember 2020.

Videre har sammensetningen av deltakere i arenaene og deltakernes engasjement og erfaringsgrunnlag vært gjenstand for diskusjon. Da Forum for digital sikkerhet og Nettverk for IKT-sikkerhet ble evaluert i henholdsvis 2019 og 2020, kom det fram at de deltakende virksomhetene varierer med hensyn til hvor forpliktet og engasjert de er i arbeidet, og at deltakerne i Forum for digital sikkerhet i mindre grad evner å diskutere nasjonale sikkerhetsspørsmål på strategisk nivå. Evalueringene påpekte også at sammensetningen av deltakere i forumet ikke var ideell.

Det er positivt at Justis- og beredskapsdepartementet har endret Forum for digital sikkerhets sammensetning og mandat på bakgrunn av evalueringen. Det er også positivt at det i Nettverk for veiledningsaktører innen styring og kontroll har vært gjort en systematisk gjennomgang av deltakerne, og at flere nye, relevante aktører har kommet inn i nettverket siden etableringen.

Basert på evalueringen av Nettverk for nasjonal IKT-sikkerhet ble det besluttet å slå nettverket sammen med Departementenes samordningsråd for samfunnssikkerhet, men sammenslåingen er som følge av pandemien per november 2022 ikke gjennomført.

Slik samordningsarenaenes mandater er utformet i dag, med formål om kunnskaps- og erfaringsutveksling, er det ikke å forvente at deltakerne i arenaene skal drive operativt arbeid for økt samordning av det digitale sikkerhetsarbeidet. Det foregår dessuten mye samarbeid mellom deltakerne i arenaene utover de planlagte møtene. Det er likevel Riksrevisjonens vurdering at de nevnte arenaene i større grad kunne vært benyttet til å styrke samordningen av det forebyggende digitale sikkerhetsarbeidet på nasjonalt nivå gjennom større grad av forpliktelse blant deltakerne og systematikk i arbeidet.

#### 1.4.1.2 Tilsynsmyndighetene er lite samordnet, og arbeidet med felles tilsynsmetodikk er ikke kommet i gang

Tilsyn er et sentralt virkemiddel som Justis- og beredskapsdepartementet og øvrige myndigheter kan bruke til å kontrollere at regelverket på det digitale sikkerhetsområdet implementeres og overholdes. Allerede i 2005 pekte Koordineringsutvalget for informasjonssikkerhet på at det var behov for å samordne tilsyn og tilsynsmetodikken på området.

På oppdrag fra Justis- og beredskapsdepartementet skal Nasjonal sikkerhetsmyndighet legge til rette for hensiktsmessig samhandling mellom myndigheter som fører tilsyn med digital sikkerhet. Nasjonal sikkerhetsmyndighet har derfor etablert to ulike samordningsarenaer på tilsynsområdet. Forum for IKT-tilsyn hadde oppstartsmøte i mars 2021, mens Samhandlingsarena for sektortilsyn etter sikkerhetsloven ble etablert i 2019.

Deltakerne i Samhandlingsarena for sektortilsyn etter sikkerhetsloven har inngått samarbeidsavtaler om tilsyn. Det har vært avholdt møter for å legge til rette for mer enhetlige tilsyn etter sikkerhetsloven, og Nasjonal sikkerhetsmyndighet har utarbeidet en veileder, Veile-

der for tilsyn med forebyggende sikkerhetsarbeid, og nettkurs om hvordan virksomheter skal gjennomføre tilsyn. Ettersom Norges vassdrags- og energidirektorat og Nasjonal kommunikasjonsmyndighet ennå ikke har gjennomført tilsyn etter sikkerhetsloven, foreligger det ingen informasjon om hvordan arbeidet i samhandlingsarenaen påvirker tilsynspraksisen.

I Forum for IKT-tilsyn har ikke arbeidet med å utarbeide en enhetlig tilsynsmetodikk kommet ordentlig i gang. Det har kun vært avholdt noen få møter, og arbeidet framstår som lite målrettet. Riksrevisjonen merker seg at det ikke har vært gjort noen systematisk gjennomgang av deltakerne, verken ved etableringen av arenaen eller i ettertid, og at Datatilsynet ikke er representert i forumet.

Mangelen på samordning mellom tilsynsmyndighetene på det digitale sikkerhetsområdet kan føre til ulike oppfatninger av hva som er godt nok for å etterleve samme type regelverkskrav. Dette kan føre til ulike oppfatninger av hva som er godt nok hos tilsynsobjektene, ulik eller manglende etterlevelse av regelverkskrav og dermed ulik grad av digital sikkerhet mellom sektorene.

#### 1.4.1.3 Brukere opplever det krevende å holde oversikt over regelverk og veiledning

Sikkerhetsloven og samfunnssikkerhetsinstruksen legger grunnlaget for arbeidet med nasjonal sikkerhet og samfunnssikkerhet, der digital sikkerhet er en integrert del.

I tillegg til disse er det mange andre regelverk som på ulike måter og i ulik grad omfatter digital sikkerhet, jf. tabell 2 i Riksrevisjonens dokument. Regelverkene forvaltes av ulike aktører, som blant annet er ansvarlige for å tilby veiledning i hvordan regelverkene skal etterleves.

Det har gjennom årene vært nedsatt flere utvalg som har undersøkt lovgivningen på det digitale sikkerhetsområdet. Omfang og overlapp i regelverk har vært trukket fram som en utfordring av flere av utvalgene. Og i 2018 pekte IKT-sikkerhetsutvalget også på overlapp mellom veiledere fra ulike aktører innenfor arbeidet med digital sikkerhet som en utfordring.

Regelverkene på det digitale sikkerhetsområdet, inkludert den nye sikkerhetsloven fra 2019, er endret: Tidligere ble det stilt konkrete krav til hvordan virksomhetene skulle oppnå forsvarlig sikkerhet, mens det i dag hovedsakelig stilles funksjonskrav. Det krever mer kompetanse og kapasitet å etterleve et funksjonsbasert regelverk fordi virksomhetene selv må vurdere risikoen og finne fram til sikkerhetsløsninger som innfrir funksjonskravene.

Da er det – fra et brukerperspektiv – desto viktigere at veiledningen er god og tilgjengelig.

Undersøkelsen viser at omfanget av regelverk fortsatt er stort, og at flere av regelverkene og veilederne på det digitale sikkerhetsområdet overlapper tematisk. Undersøkelsen viser også at det i veiledningsmateriellet brukes ulike standarder og begreper og gis ulike anbefalinger om de samme emnene. Digitaliseringsdirektoratet har søkt å løse noe av utfordringen ved å samle veiledere om regelverk for digital sikkerhet i offentlig sektor på en egen nettside. Fra et brukerperspektiv er det likevel vanskelig å finne fram, og veilederne framstår ikke som samordnet. Direktoratets nettside inneholder kun et utvalg veiledere, og det er ikke gjort noe for å samordne innholdet i veilederne.

Den svake samordningen av roller, ansvar og krav fører til at det er krevende for virksomhetene å avklare hvilke regelverk de omfattes av, hvilke myndighetsaktører de skal forholde seg til, og hvilke veiledere de skal benytte i det forebyggende digitale sikkerhetsarbeidet. Dette gjør at implementeringen av relevant regelverk blir forsinket og mangelfull. I verste fall kan det føre til at viktige verdier ikke sikres tilstrekkelig.

Riksrevisjonen mener myndighetene ikke har lagt godt nok til rette for at virksomhetene kan etterleve regelverket som gjelder digital sikkerhet, gjennom ensartet og tilgjengelig veiledning og veiledningsmateriell.

### 1.4.2 Justis- og beredskapsdepartementet har ikke sørget for god nok informasjon om den nasjonale digitale sikkerhetstilstanden

Som en del av samordningsansvaret på samfunnssikkerhetsområdet skal Justis- og beredskapsdepartementet ha oversikt over den nasjonale sikkerhetstilstanden, herunder den nasjonale digitale sikkerhetstilstanden. Denne oversikten er blant annet en forutsetning for at departementet skal kunne identifisere tverrsektorielle sikkerhetsutfordringer, og for at det skal kunne iverksettes sikkerhetstiltak som reduserer risikoen knyttet til disse.

Justis- og beredskapsdepartementet benytter en rekke ulike kilder for å holde oversikt over den nasjonale digitale sikkerhetstilstanden. Departementenes rapportering på arbeidet som følger av den nye sikkerhetsloven, og arbeidet som følger av samfunnssikkerhetsinstruksen, trekkes blant annet fram som viktige kilder. Andre viktige informasjonskilder er rapporter fra Nasjonal sikkerhetsmyndighet, Direktoratet for samfunnssikkerhet og beredskap og de nasjonale etterretnings- og sikkerhetstjenestene.

Justis- og beredskapsdepartementet mener at de har tilstrekkelig oversikt til å identifisere behov på nasjonalt nivå og til å kunne sette retning og prioritere tverrsektorielle tiltak. Denne undersøkelsen viser imidlertid at det er flere utfordringer med disse kildene, og at det derfor er mangler i departementets informasjonsgrunnlag.

#### 1.4.2.1 Det er ikke etablert en fullstendig oversikt over hvilke verdier og avhengigheter som skal sikres etter sikkerhetsloven

Ny sikkerhetslov trådte i kraft 1. januar 2019. I henhold til denne loven er departementene ansvarlig for å identifisere og holde oversikt over grunnleggende nasjonale funksjoner innenfor sine ansvarsområder. Det enkelte departement er også ansvarlig for å identifisere og holde oversikt over avhengigheter, det vil si virksomheter som har vesentlig eller avgjørende betydning for grunnleggende nasjonale funksjoner. Det er disse funksjonene, og virksomhetene som understøtter dem, som skal sikres i henhold til sikkerhetsloven. Departementene skal melde inn oversikt til Nasjonal sikkerhetsmyndighet, som rapporterer dette til Justis- og beredskapsdepartementet årlig.

Justis- og beredskapsdepartementet utarbeidet og fastsatte i 2019 en milepælsplan for implementering av den nye loven. I henhold til planen skulle alle departementene i løpet av august 2020 ha identifisert grunnleggende nasjonale funksjoner innenfor sitt ansvarsområde. Allerede ved første milepæl ble arbeidet forsinket, og først høsten 2021 hadde alle departementene meldt inn sine identifiserte grunnleggende nasjonale funksjoner.

Fordi identifiseringen av disse funksjonene er en forutsetning for den videre implementeringen, ble også arbeidet ellers forsinket. I henhold til planen skulle kartleggingen av avhengigheter være ferdig i juli 2021, men høsten 2022 arbeider departementene fortsatt med å kartlegge avhengigheter. Myndighetene har heller ikke oversikt over alle avhengighetene mellom de ulike funksjonene.

At myndighetene ikke har denne oversikten, og at det derfor ikke blir stilt krav til sikkerhet gjennom hele verdikjeden til en grunnleggende funksjon, medfører risiko for at virksomheter, systemer og infrastruktur som denne funksjonen er avhengig av, ikke er tilstrekkelig sikret. Grunnleggende nasjonale funksjoner kan dermed settes ut av spill, for eksempel ved at digitale angrep rettes mot sårbare virksomheter, informasjonssystemer eller infrastruktur som befinner seg lenger ut i den digitale verdikjeden.

Både Justis- og beredskapsdepartementet og Nasjonal sikkerhetsmyndighet har uttalt at arbeidet som følger av ny sikkerhetslov, går sakte. Manglende kapasitet og sikkerhetskompetanse i departementer og virksomheter som omfattes av sikkerhetsloven, trekkes fram som en medvirkende årsak. Ifølge Justis- og beredskapsdepartementet kan dette medføre at viktige verdier ikke er tilstrekkelig sikret.

Det er det enkelte departement som har ansvar for samfunnssikkerhet i egen sektor. Samtidig må det være slik at når framdriften i departementenes arbeid som følger av ny sikkerhetslov, går tregt, må Justis- og beredskapsdepartementet følge dette tydelig opp. Riksrevisjonen peker på de alvorlige konsekvensene tregheten i arbeidet kan ha for nasjonal sikkerhet. På grunn av sakens alvorlige karakter er det kritikkverdig at Justis- og beredskapsdepartementet ikke har ivaretatt sitt pådriveransvar mer aktivt, for eksempel gjennom nye krav og frister, for å sikre framdriften i arbeidet som følger av ny sikkerhetslov.

#### 1.4.2.2 Justis- og beredskapsdepartementet har ikke sørget for at sentral rapportering fra departementene kan brukes til å holde oversikt over sikkerhetstilstanden

Som en del av samordningsansvaret for samfunnssikkerhetsområdet skal Justis- og beredskapsdepartementet definere hvilke samfunnsfunksjoner som i et tverrsektorielt perspektiv er å anse som kritiske, og hva som inngår i disse funksjonene. På oppdrag fra departementet har Direktoratet for samfunnssikkerhet og beredskap definert totalt 16 kritiske samfunnsfunksjoner. I henhold til samfunnssikkerhetsinstruksen skal departementet med hovedansvar for en samfunnskritisk funksjon gjennomføre status- og tilstandsvurderinger for funksjonen. Det går også fram at disse status- og tilstandsvurderingene skal være en kilde til Justis- og beredskapsdepartementets oversikt over den nasjonale sikkerhetstilstanden. Justis- og beredskapsdepartementet oppgir vurderingene som en sentral kilde til informasjon om den nasjonale sikkerhetstilstanden, som også omfatter den digitale sikkerheten.

Undersøkelsen viser imidlertid at status- og tilstandsvurderingene er av varierende omfang og kvalitet. I vurderingene framheves det som fungerer bra, men det rettes lite oppmerksomhet mot sårbarhetene i funksjonene som er vurdert. En annen utfordring med vurderingene er at de er overordnede og i liten grad gir konkrete forslag til forbedringer og tiltak. Samlet sett fører dette til at vurderingene ikke gir en tilstrekkelig oversikt over den digitale sikkerhetstilstanden for kritiske samfunnsfunksjoner. En mer enhetlig gjennomføring og rapportering av vurderingene ville gjort dem mer relevante og tilgjengelige. Justis- og beredskapsdepartementet har som mål å komme fram til en ny, enhetlig måte å gjennomføre og rapportere status- og tilstandsvurderinger på. Dette arbeidet er satt i gang, men det er ennå ikke fullført.

I tillegg til de ovennevnte status- og tilstandsvurderingene skal alle departementene i henhold til samfunnssikkerhetsinstruksen gjennomføre risiko- og sårbarhetsanalyser for eget ansvarsområde. Dette inkluderer risiko knyttet til digital sikkerhet. Justis- og beredskapsdepartementet bruker imidlertid ikke disse risiko- og sårbarhetsanalysene for å få oversikt over den nasjonale digitale sikkerhetstilstanden. Ifølge departementet er det fordi de utføres på ulike måter og etter ulik meto-

dikk, noe som gjør en sammenstilling av analysene mer ressurskrevende enn den antatte nytten.

Gjennom samordningsansvaret for samfunnssikkerheten kan Justis- og beredskapsdepartementet gi føringer for hvordan departementene skal gjennomføre risiko- og sårbarhetsanalyser. Departementet har imidlertid valgt å ikke gi slike føringer.

Etter Riksrevisjonens vurdering har ikke Justis- og beredskapsdepartementet sørget for at arbeidet med status- og tilstandsvurderinger og risiko- og sårbarhetsanalyser blir gjennomført på en enhetlig måte. Dersom rapporteringen fra departementene var mer enhetlig, ville det ha vært mulig å sammenstille informasjon og få en bedre oversikt over sikkerhetstilstanden. Det ville også ha gitt et større utbytte av ressursbruken knyttet til analysearbeidet i departementene.

#### 1.4.2.3 Det gjennomføres få tilsyn med digital sikkerhet sett opp mot antall virksomheter det skal og kan føres tilsyn med

Arbeidet med digital sikkerhet er regulert gjennom en rekke regelverk, berører de fleste virksomheter og kontrolleres av flere ulike tilsynsmyndigheter. Tilsyn er et sentralt virkemiddel som Justis- og beredskapsdepartementet og øvrige myndigheter kan bruke til å kontrollere at regelverket på det digitale sikkerhetsområdet implementeres og overholdes. Tilsyn skal bidra til å forbedre arbeidet med digital sikkerhet i virksomhetene. For myndighetene er tilsynsrapportene også en viktig kilde til innsikt i arbeidet på området – i hver enkelt sektor og i samfunnet som helhet. Mangelfull tilsynsvirksomhet kan føre til at den digitale sikkerheten får for lite oppmerksomhet i virksomheter og departementer. Dette kan svekke den digitale sikkerheten i samfunnet. Undersøkelsen viser at det gjennomføres forholdvis få tilsyn med digital sikkerhet som tema.

Det er et stort antall tilsynsobjekter som omfattes av de generelle regelverkene, som sikkerhetsloven og personvernregelverket. Justis- og beredskapsdepartementet har gitt Nasjonal sikkerhetsmyndighet det overordnede ansvaret for å sørge for at sikkerhetstilstanden i alle sektorer kontrolleres, og at virksomhetene oppfyller pliktene de har etter sikkerhetsloven. I kontrollmeldingen for 2020 peker Nasjonal sikkerhetsmyndighet på at antall tilsyn per år er begrenset sammenlignet med antall tilsynsobjekter. Det begrensede antallet tilsyn i 2019 og 2020 skyldes imidlertid sikkerhetsmyndighetenes beslutning om å være tilbakeholdne med undersøkelser så kort tid etter innføringen av den nye sikkerhetsloven. I 2022 har antallet tilsyn økt, og sikkerhetsmyndighetene antar at det vil fortsette å øke framover. I 2019 ble Nasjonal kommunikasjonsmyndighet og Norges vassdrags- og energidirektorat utpekt som sektortilsyn for tilsyn etter sikkerhetsloven. Dette skulle bidra til at tilsynene ble bedre tilpasset de ulike sektorene, og til at antall tilsyn etter sikkerhetsloven økte. Verken Nasjonal kommunikasjonsmyndighet eller Norges vassdrags- og energidirektorat har imidlertid kommet i gang med slike tilsyn.

Datatilsynet gjennomfører tilsyn etter personvernregelverket. I 2021 planla Datatilsynet å gjennomføre 14 egeninitierte tilsyn, men bare 5 ble startet opp, og kun 3 ble gjennomført.

Samfunnssikkerhetsinstruksen og sivilbeskyttelsesloven stiller krav til henholdsvis departementenes og kommunenes samfunnssikkerhetsarbeid, inkludert arbeidet med digital sikkerhet. Ansvaret for å føre tilsyn med departementene er delegert fra Justis- og beredskapsdepartementet til Direktoratet for samfunnssikkerhet og beredskap, mens statsforvalterne fører tilsyn med kommunene. Temaene for tilsynene skal velges ut fra en risiko- og vesentlighetsvurdering. I en tilsynsrapport om Justis- og beredskapsdepartements gjennomføring av tilsyn på området fra 2013 går det fram at tilsynene i større grad framstår som brede gjennomganger enn som tilsyn som er spisset mot risiko og vesentlighet. Også Riksrevisjonens undersøkelse viser at tilsynene med departementene og kommunene omfatter samfunnssikkerhetsarbeid generelt og ikke arbeidet med digital sikkerhet spesielt. Tilsynsrapportene gir dermed ikke informasjon om statusen for arbeidet med digital sikkerhet i departementene og kommunene.

Nasjonal sikkerhetsmyndighet har framhevet at det er betydelige trusler i det digitale rom, og at antallet digitale angrep øker. Konsekvensen av at det gjennomføres få tilsyn med digital sikkerhet, er en økt risiko for at sårbarheter ikke fanges opp. Riksrevisjonen vurderer det derfor som kritikkverdig at det gjennomføres få tilsyn med digital sikkerhet, og at tilsynsmyndighetene på området er lite samordnet.

### 1.4.3 Justis- og beredskapsdepartementet har ikke sørget for god nok oppfølging av Nasjonal strategi for digital sikkerhet

I 2019 utga Justis- og beredskapsdepartementet Nasjonal strategi for digital sikkerhet og delstrategien Nasjonal strategi for digital sikkerhetskompetanse. Strategiene er utarbeidet i samarbeid med Forsvarsdepartementet og Kunnskapsdepartementet. Dette er fjerde gang det har blitt utgitt en nasjonal strategi for digital sikkerhet (strategier er tidligere utgitt i 2003, 2007 og 2012), og første gang det er utgitt en egen delstrategi for digital sikkerhetskompetanse. I samfunnssikkerhetsmeldingen trekkes strategien fram som et sentralt virkemiddel i myndighetenes arbeid med digital sikkerhet. Etter Riksrevisjonens vurdering utnytter ikke Justis- og beredskapsdepartementet potensialet som ligger i det-

te virkemiddelet, godt nok til å forbedre samordningen av arbeidet med digital sikkerhet nasjonalt.

#### 1.4.3.1 Justis- og beredskapsdepartementets oppfølging av strategien gir ikke grunnlag for å løpende vurdere effekt av tiltakene

Justis- og beredskapsdepartementet viser til at en systematisk og kunnskapsbasert tilnærming ligger til grunn for utarbeidelsen av Nasjonal strategi for digital sikkerhet (2019). Etter at Justis- og beredskapsdepartementet overtok ansvaret for den digitale sikkerheten i 2013, er det utarbeidet flere utredninger og styrende dokumenter. Blant annet har det vært nedsatt to nasjonale utvalg for å utrede særskilte forhold knyttet til den digitale sikkerheten nasjonalt, og i 2017 kom den første stortingsmeldingen som utelukkende omhandler digital sikkerhet. Justis- og beredskapsdepartementet viser også til at det i forkant av utgivelsen av Nasjonal strategi for digital sikkerhet (2019) ble gjennomført en omfattende prosess for å få innspill til strategien fra et så bredt utvalg av aktører som mulig. Riksrevisjonen vurderer dette arbeidet som positivt.

*Utredninger om og styrende dokumenter for digital sikkerhet*[1]

- NOU 2015:13 Digital sårbarhet – sikkert samfunn (Digitalt sårbarhetsutvalg, også omtalt som Lysneutvalget)
- Nasjonalt digitalt risikobilde, rapport som utgis årlig av Nasjonal sikkerhetsmyndighet, og som ble utgitt for første gang i 2015
- Meld. St. 38 (2016–2017) IKT-sikkerhet. Et felles ansvar
- Internasjonal cyberstrategi for Norge (2017)
- Nasjonal strategi for digital sikkerhet (2019)
- Nasjonal strategi for digital sikkerhetskompetanse (2019)
- NOU (2018:14) IKT-sikkerhet i alle ledd (Holteutvalget)
- Risikostyring i digitale verdikjeder (2019), Direktoratet for samfunnssikkerhet og beredskap
- Evaluering av hendelseshåndteringen av IKT-sikkerhetshendelsene hos Helse Sør-Øst Regionalt helseforetak og fylkesmannsembetene 2018 (2020), Forsvarets forskningsinstitutt
- Norsk kryptopolitikk (2020)

Med strategien fra 2019 følger en oversikt over sentrale tiltak som skal understøtte strategiens målsettinger, og som skal revideres ved behov. Justis- og beredskapsdepartementet har imidlertid besluttet at tiltaksoversikten ikke vil bli oppdatert med nye tiltak eller endringer i eksisterende tiltak, til tross for at det er identifisert behov for nye tiltak på det digitale sikkerhetsområdet. Nye tiltak vil i stedet bli presentert på annen måte, for eksempel gjennom proposisjoner til Stortinget.

Våren 2021 innhentet Justis- og beredskapsdepartementet rapportering på ansvarlige departementers og virksomheters arbeid med gjennomføringen og oppfølgingen av tiltakene som tilhørte strategien. I en oppsummering av rapporteringen påpeker Justis- og beredskapsdepartementet at kvaliteten på rapporteringen er varierende, og at den sier lite om tiltakenes effekt på den digitale sikkerheten. Justis- og beredskapsdepartementet har likevel ikke etterspurt ytterligere informasjon fra virksomhetene. Til tross for at de samme utfordringene ble påpekt i forbindelse med oppfølgingen av tiltak som tilhørte strategien fra 2012, har departementet altså ikke endret metoden for statusrapportering.

I henhold til Nasjonal strategi for digital sikkerhetskompetanse (2019) skal Justis- og beredskapsdepartementet og Kunnskapsdepartementet sørge for at det foreligger oppdaterte tall og statistikk, slik at det er mulig å følge med på forholdet mellom samfunnets tilgang til og behov for digital sikkerhetskompetanse. Det er imidlertid ikke innhentet oppdaterte data og analyser om kompetansegapet på det digitale sikkerhetsområdet siden 2017. Grunnen til dette er at departementene mener det er for tidlig å vurdere effekten av tiltakene i kompetansestrategien. Det har for øvrig vist seg å være en risiko for at enkelte tiltak ikke oppfyller målene i strategien. Dette gjelder for eksempel rekruttering til utdanning og forskning innenfor digital sikkerhet. Til tross for dette har ikke de ansvarlige departementene innhentet nok informasjon til å foreta en løpende vurdering av effekten av tiltak i kompetansestrategien der dette hadde vært mulig.

Etter Riksrevisjonens vurdering har ikke Justis- og beredskapsdepartementet sørget for å tilegne seg god nok informasjon om virkningen av Nasjonal strategi for digital sikkerhet (2019) med tilhørende tiltak. Bedre informasjon om statusen for og effekten av tiltakene kunne ha dannet grunnlag for nye tiltak eller endringer i pågående tiltak, slik at man kunne oppfylle strategiens mål i lys av dagens behov.

#### 1.4.3.2 Satsingen på kompetanse er mindre målrettet enn beskrevet i Nasjonal strategi for digital sikkerhet

Behovet for økt digital sikkerhetskompetanse er trukket fram som en av de største utfordringene på det digitale sikkerhetsområdet. Å styrke den digitale sikkerhetskompetansen i samfunnet er derfor et av fem overordnende mål i Nasjonal strategi for digital sikkerhet (2019). Kompetansemålene utdypes i Nasjonal strategi

1. Kilde: Meld. St. 5 (2020–2021) Samfunnssikkerhet i en usikker verden, s. 89.

for digital sikkerhetskompetanse fra samme år. Som følge av at de fleste av tiltakene i kompetansestrategien er rettet mot forsknings- og utdanningsinstitusjoner, er det Kunnskapsdepartementet som har hovedansvaret for gjennomføringen og oppfølgingen av tiltakene.

Undersøkelsen viser at satsingen på digital sikkerhetskompetanse er mindre målrettet enn det som er beskrevet i strategidokumentet. I tiltaksoversikten til Nasjonal strategi for digital sikkerhet (2019) vises det til prioriteringer på kompetanseområdet på over 800 mill. kroner. Også i samfunnssikkerhetsmeldingen vises det til at 800 mill. kroner er satt av til å styrke den digitale sikkerhetskompetansen. Flere av tiltakene i strategien er imidlertid ikke rettet mot å øke den digitale sikkerhetskompetansen, men den digitale kompetansen i samfunnet generelt, og de omtaler i ulik grad digital sikkerhetskompetanse.

### 1.4.4 Justis- og beredskapsdepartementet har ikke lagt godt nok til rette for tverssektoriell hendelseshåndtering

I samfunnssikkerhetsmeldingen trekkes Nasjonalt cybersikkerhetssenter og Felles cyberkoordineringssenter fram som sentrale arenaer for å avdekke, håndtere og koordinere innsatsen ved alvorlige digitale angrep. Riksrevisjonens undersøkelse viser at det er utfordringer knyttet til arbeidet i de to arenaene.

En annen del av Justis- og beredskapsdepartementets samordningsrolle på samfunnssikkerhetsområdet går ut på å gjennomføre nasjonale øvelser og sørge for at utfordringer på tvers av flere sektorer blir håndtert. Sentrale tiltak omfatter blant annet å få på plass et felles rammeverk for digital hendelseshåndtering og tekniske systemer for varsling av uønsket aktivitet og kommunikasjon mellom beredskapsaktører. Undersøkelsen viser at gjennomføringen av flere av disse tiltakene er forsinket, og at viktige elementer av tverrsektoriell hendelseshåndtering ikke har blitt øvet som planlagt.

Med tanke på utfordringene som er knyttet til å avdekke, håndtere og koordinere innsatsen ved alvorlige digitale hendelser, mener Riksrevisjonen at dette samlet sett er kritikkverdig. Detaljer om utfordringene er omtalt i et eget sikkerhetsgradert vedlegg til Riksrevisjonens rapport.

#### 1.4.4.1 Nasjonal sikkerhetsmyndighets evne til å oppdage og håndtere digitale hendelser har svakheter

I henhold til sikkerhetsloven skal Nasjonal sikkerhetsmyndighet drive en nasjonal responsfunksjon for alvorlige angrep og et nasjonalt varslingssystem for digital infrastruktur. Som en del av den nasjonale responsfunksjonen skal Nasjonal sikkerhetsmyndighet ved behov og basert på samtykke bistå virksomheter i håndteringen av alvorlige digitale angrep. Nasjonal sikkerhetsmyndighet opprettet i 2019 Nasjonalt cybersikkerhetssenter for å ivareta denne funksjonen. Senteret drifter og organiserer sensornettverket Varslingssystem for digital infrastruktur (VDI), som skal oppdage og varsle om digitale trusler. Nasjonal sikkerhetsmyndighet tilbyr også gratistjenesten Allvis NOR, som virksomheter kan abonnere på. Verktøyet skanner de av virksomhetenes datatjenester som er eksponert for sårbarheter gjennom internett.

Riksrevisjonen har intervjuet et utvalg private og offentlige virksomheter som ved hendelser har fått bistand fra Nasjonalt cybersikkerhetssenter. Virksomhetene understøtter en grunnleggende nasjonal funksjon. Disse opplyser til Riksrevisjonen at de gjennomgående har vært fornøyd med bistanden. Nasjonalt cybersikkerhetssenter beskrives av virksomhetene som en aktør som har bidratt til økt informasjonsdeling mellom norske virksomheter forut for, under og i etterkant av alvorlige digitale hendelser.

De intervjuede virksomhetene er tildelt en fast kontaktperson i Nasjonalt cybersikkerhetssenter. Det er imidlertid ikke alle virksomhetene som har en slik kontaktperson. Representanter for kommunesektoren, som understøtter flere kritiske samfunnsfunksjoner, uttaler til Riksrevisjonen at noen kommuner opplever at det er vanskelig å komme i kontakt med og få bistand fra Nasjonalt cybersikkerhetssenter, også ved digitale hendelser.

Undersøkelsen avdekker også at det er utfordringer med Nasjonal sikkerhetsmyndighets tekniske systemer VDI og Allvis NOR. Allvis NOR tilbys virksomheter som er underlagt sikkerhetsloven, og eiere og forvaltere av samfunnskritiske funksjoner. Allvis NOR skanner som nevnt ovenfor tjenester som er eksponert for sårbarheter gjennom internett. Undersøkelsen viser imidlertid at Allvis NOR har begrenset evne til å fange opp sårbarheter. Skanningen gir dermed ikke et fullstendig bilde av en virksomhets digitale sårbarheter. Dette kan potensielt få store konsekvenser for virksomhetene som benytter tjenesten.

VDI består av nettverkssensorer som er utplassert hos virksomheter som anses som en del av norsk kritisk infrastruktur. Sensorene overvåker internettrafikken for å oppdage mistenkelig trafikk. Det er avdekket flere utfordringer knyttet til sensornettverket. Blant annet vil ikke nye og ukjente angrepsmønstre oppdages av VDI, da sensorene kun fanger opp kjente mønstre. I tillegg er mesteparten av dagens nettverkstrafikk kryptert. Sensorene er ikke i stand til å overvåke denne typen trafikk. Flere og flere virksomheter bruker dessuten skyløsninger, men sensorene overvåker heller ikke trafikk som går direkte fra datamaskiner og mobiltelefoner til servere i skyen. Det er både tekniske og regulatoriske utford-

ringer med å få på plass slik funksjonalitet. Det er dermed en stor del av nettverkstrafikken som ikke overvåkes av VDI. Det er også en utfordring at det ikke er utplassert VDI-sensorer i alle relevante virksomheter. Ytterligere detaljer om utfordringene knyttet til VDI og konsekvensene av disse utdypes i et sikkerhetsgradert vedlegg til Riksrevisjonens rapport.

De påpekte svakhetene i VDI gjør i sum at sensornettverket har store blindsoner. Det pågår derfor et større prosjekt der målet er å oppgradere og videreutvikle funksjonaliteten og kapasiteten i sensornettverket. Prosjektet skal etter planen ferdigstilles i 2023. I forbindelse med utbruddet av krigen i Ukraina ble det bevilget ekstra midler til å øke dekningen og analysekapasiteten i VDI. Justis- og beredskapsdepartementet opplyser imidlertid at midlene til å øke omfanget av VDI-sensorer ikke ble videreført for 2023.

Riksrevisjonen vurderer det som positivt at det er satt i gang tiltak for å oppgradere og videreutvikle de tekniske verktøyene VDI og Allvis NOR, men påpeker samtidig at det kreves en betydelig innsats for å løse utfordringene med systemene.

#### 1.4.4.2 Vedvarende utfordringer i Felles cyberkoordineringssenter har ikke blitt godt nok fulgt opp av Justis- og beredskapsdepartementet

På oppdrag fra Justis- og beredskapsdepartementet og Forsvarsdepartementet ble Felles cyberkoordineringssenter etablert i 2017. Felles cyberkoordineringssenter er et permanent, samlokalisert fagmiljø med representanter fra Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos. Det er Nasjonal sikkerhetsmyndighet som er gitt ansvaret for å lede senterets arbeid.

Felles cyberkoordineringssenter skal bidra til å øke den nasjonale evnen til å motstå alvorlige digitale angrep, understøtte strategisk analyseproduksjon og vedlikeholde et helhetlig trussel- og risikobilde for det digitale rom. I henhold til Retningslinjer for cybersamarbeid (2022) skal dette oppnås gjennom senterets åtte hovedoppgaver. Partene i senteret har i hovedsak prioritert fire av disse oppgavene.

Undersøkelsen har blant annet vist at det er utfordringer knyttet til ressurssituasjonen og bemanningen i Felles cyberkoordineringssenter. Utfordringer knyttet til senterets arbeid beskrives mer inngående i et sikkerhetsgradert vedlegg til Riksrevisjonens rapport.

Utfordringene som er identifisert i denne undersøkelsen, kom også fram i partenes egen evaluering av Felles cyberkoordineringssenter i 2019. Partene utarbeidet da en handlingsplan for å håndtere utfordringene, men flere av dem vedvarer. En evalueringsrapport ble sendt til Justis- og beredskapsdepartementet og Forsvarsdepartementet i etterkant av evalueringen. Rapporten inneholdt imidlertid ingen informasjon om utfordringer knyttet til arbeidet eller tiltak for å imøtekomme utfordringene. Justis- og beredskapsdepartementet opplyser at de etterspurte mer informasjon om resultatene av evalueringen, men at enkelte av partene ikke ønsket å dele denne med departementet. Justis- og beredskapsdepartementet fulgte ikke dette opp videre og er ikke blitt gjort kjent med senterets utfordringer.

Justis- og beredskapsdepartementet viser til at det er partene selv som er ansvarlige for ressurssetting av senteret. Videre viser departementet til at Nasjonal sikkerhetsmyndighet er gitt en lederfunksjon for Felles cyberkoordineringssenter. Departementet mener det følger av denne funksjonen blant annet å sørge for at senteret har gode rutiner for hendelseshåndtering.

Det er Riksrevisjonens vurdering at de identifiserte utfordringene begrenser måloppnåelsen med etableringen av Felles cyberkoordineringssenter. Videre mener Riksrevisjonen at Justis- og beredskapsdepartementet skulle ha gjort mer for å sikre seg relevant informasjon om måloppnåelsen i Felles cyberkoordineringssenter.

#### 1.4.4.3 Det er behov for mer øving av tverrsektoriell håndtering av hendelser på nasjonalt nivå

Justis- og beredskapsdepartementet skal som en del av samordningsansvaret planlegge, gjennomføre og evaluere nasjonale øvelser i sivil sektor. Formålet er å sørge for at aktører ved en reell hendelse vet hva de skal gjøre, og hvem de skal samarbeide med.

Høsten 2020 skulle Øvelse Digital 2020 avholdes, men på grunn av koronarestriksjoner ble den nedskalert. Spilløvelsen, som opprinnelig var en del av et tredelt konsept, ble gjennomført med redusert deltakelse, begrensede scenarioer og kortere varighet. Nedskaleringen innebar at tverrsektoriell hendelseshåndtering på nasjonalt nivå ikke ble øvet.

Direktoratet for samfunnssikkerhet og beredskap var ansvarlig for å evaluere øvelsen. I evalueringsrapporten konkluderer direktoratet med at prosjektet som helhet har oppfylt hensikten med Øvelse Digital 2020, til tross for at nedskaleringen førte til at ikke alle øvingsmålene ble innfridd. Direktoratet viser imidlertid til at det fortsatt er behov for bedre oversikt over aktørbildet, økt samhandling på tvers av sektorer og mer koordinert kommunikasjonshåndtering. Direktoratet ser også at det er behov for flere og hyppigere nasjonale øvelser innenfor digital sikkerhet. Forsvarsdepartementet og Nasjonal sikkerhetsmyndighet har uttalt at det var uheldig at øvelsen ble nedskalert, og at viktige elementer ikke ble øvet.

Det er ikke planlagt å gjennomføre en ny spilløvelse som erstatning for den delen av Øvelse Digital 2020 som ble nedskalert. Justis- og beredskapsdepartementet viser til at det øves på digitale hendelser internt i sektorene, og at Norge deltar i en rekke internasjonale øvelser

på det digitale området. De sentrale hendelseshåndteringsmiljøene håndterer dessuten jevnlig reelle digitale hendelser og har gjennom det fått god erfaring med håndtering av slike hendelser. Videre bemerker departementet at det generiske systemet for sentral krisehåndtering øves ofte, selv om disse øvelsene ikke alltid er knyttet spesifikt til digital sikkerhet.

Det er positivt at Norge deltar i internasjonale øvelser på det digitale området, og at det øves på krisehåndtering på strategisk nivå. Dette er svært viktig for den nasjonale sikkerheten. Undersøkelsen viser imidlertid at scenarioer som omhandler digital sikkerhet, ofte blir nedprioritert ved gjennomføring av øvelser. Dette gjelder særlig i kommunene. Til tross for at Justis- og beredskapsdepartementet uttaler at det gjennomføres en rekke sektorinterne øvelser knyttet til digital sikkerhet, har ikke departementet noen oversikt over dette. Det er derfor usikkerhet knyttet til hvor ofte disse øvelsene faktisk gjennomføres. Sentrale aktører innenfor det digitale sikkerhetsområdet har også etterlyst flere tverrsektorielle øvelser på området.

#### 1.4.4.4 Viktige tverrsektorielle tiltak for å håndtere digitale angrep er forsinket

Flere av tiltakene som tilhører Nasjonal strategi for digital sikkerhet (2019), er iverksatt for å øke den nasjonale evnen og kapasiteten til å forebygge, avdekke og håndtere digitale angrep. Undersøkelsen viser imidlertid at arbeidet har gått tregt, og at det er forsinkelser i gjennomføringen av flere av tiltakene. Forsinkelsene medfører økt risiko for at digitale hendelser ikke håndteres effektivt.

I 2012 ble det bestemt at alle sektorer skulle etablere egne sektorvise responsmiljøer. De sektorvise responsmiljøene skal blant annet fungere som bindeledd mellom Nasjonalt cybersikkerhetssenter og virksomhetene i sektoren. Undersøkelsen viser imidlertid at responsmiljøene i enkelte sektorer bidrar til forsinkelser i håndtering og informasjonsflyt. En evaluering av ordningen med sektorvise responsmiljøer som ble utført av KPMG i 2022, viser til flere utfordringer med ordningen, blant annet uklar ansvars- og rolleforståelse og mangel på tilgang på relevant kompetanse. Riksrevisjonen ser det som positivt at Justis- og beredskapsdepartementet sommeren 2022 satte i gang en prosess for å evaluere og forbedre ordningen med sektorvise responsmiljøer.

Rammeverk for håndtering av IKT-sikkerhetshendelser skal bidra til effektiv håndtering av alvorlige IKT-sikkerhetshendelser. Rammeverket ble utformet i 2017 og skal revideres annethvert år, men har ikke blitt revidert siden 2017. Etter planen skulle bruken av rammeverket øves under Øvelse Digital 2020, og målet var at øvelsen skulle gi innspill til revisjonen av rammeverket. Siden øvelsen ikke ble gjennomført som planlagt, fikk imidlertid ikke Nasjonal sikkerhetsmyndighet noen innspill om hvordan rammeverket fungerer ved håndtering av hendelser. Nasjonal sikkerhetsmyndighet jobber for tiden med en revisjon av rammeverket.

For å øke den nasjonale kapasiteten til å håndtere alvorlige digitale angrep skal Nasjonal sikkerhetsmyndighet utrede mulighetene for en tverrsektoriell cyberreserve. Dette skal være en nasjonal kapasitet bestående av operativt personell som kan bistå ved spesielt store kriser som krever innsats utover ordinær bemanning. Utredningen skulle etter planen ha blitt gjennomført i perioden 2018–2019, men arbeidet er ennå ikke ferdigstilt. Justis- og beredskapsdepartementet forventer en utredning fra Nasjonal sikkerhetsmyndighet i løpet av høsten 2022.

Det har siden 2012 vært iverksatt tiltak for å utvikle et system for høygradert datakommunikasjon mellom departementene, underliggende etater og andre sentrale beredskapsaktører. Manglende muligheter til å kommunisere via sikkerhetsgraderte informasjonssystemer har blitt pekt på som et hinder for effektiv hendelseshåndtering både av Digitalt sårbarhetsutvalg (Lysneutvalget) i 2015 og Forsvarets forskningsinstitutt i 2020. I henhold til Nasjonal strategi for digital sikkerhet (2019) skal Forsvarsdepartementet utvikle og drifte Nasjonalt BEGRENSET nett for lavgradert kommunikasjon og Nasjonalt HEMMELIG nett for høygradert kommunikasjon. Ifølge strategien skulle tiltaket ha blitt gjennomført i 2019. Nasjonalt BEGRENSET nett er etablert og tatt i bruk. Nasjonalt HEMMELIG nett er ikke rullet ut til beredskapsaktørene ennå.

## 1.5 Anbefalinger

Riksrevisjonen anbefaler at Justis- og beredskapsdepartementet

- tar en tydeligere samordnings- og pådriverrolle for nasjonal digital sikkerhet i sivil sektor.
- sørger for at Nasjonal sikkerhetsmyndighet i samarbeid med de andre veiledningsaktørene gjør veiledningen på det digitale sikkerhetsområdet mer samordnet og tilgjengelig.
- sørger for bedre utnyttelse og koordinering av de etablerte arenaene for samordning.
- gjennom pådriverrollen bidrar til at alle departementer har tilstrekkelig framdrift i arbeidet som følger av ny sikkerhetslov.
- sikrer et bedre kildegrunnlag for å holde oversikt over den nasjonale digitale sikkerhetstilstanden.
- sørger for bedre informasjon om resultater av iverksatte tiltak for å kunne vurdere behovet for endringer og nye tiltak på det digitale sikkerhetsområdet.
- styrker arbeidet med å avdekke, håndtere og koordinere innsatsen mot alvorlige digitale hendelser.

## 1.6 Statsrådens svar og Riksrevisjonens uttalelse

Dokument 3:7 (2022–2023) Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor ble oversendt statsråden i Justis- og beredskapsdepartementet. Statsrådens svar følger i vedlegg til Riksrevisjonens dokumentasjon.

Riksrevisjonen har ingen ytterligere merknader.

# 2. Komiteens merknader

Komiteen, medlemmene fra Arbeiderpartiet, Kari Henriksen, Lubna Boby Jaffery og Bente Irene Aaland, fra Høyre, lederen Peter Frølich og Svein Harberg, fra Senterpartiet, Nils T. Bjørke, fra Fremskrittspartiet, Carl I. Hagen, fra Sosialistisk Venstreparti, Audun Lysbakken, fra Rødt, Seher Aydar, og fra Venstre, Grunde Almeland, viser til Dokument 3:7 (2022–2023), Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor.

Komiteen viser til at Riksrevisjonens undersøkelse har tatt utgangspunkt i blant annet følgende vedtak og forutsetninger fra Stortinget:

- Meld. St. 5 (2020–2021) Samfunnssikkerhet i en usikker verden, jf. Innst. 275 S (2020–2021)
- Meld. St. 38 (2016–2017) IKT-sikkerhet. Et felles ansvar, jf. Innst. 187 S (2017–2018)
- kgl.res. av 10. mars 2017 nr. 312: Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet
- instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen), 2017
- lov om nasjonal sikkerhet (sikkerhetsloven), 2019

## 2.1 Om Riksrevisjonens konklusjoner

Komiteen viser videre til at målet med undersøkelsen har vært å vurdere hvorvidt Justis- og beredskapsdepartements samordning av arbeidet med å ivareta den digitale sikkerheten i sivil sektor er effektiv og i tråd med Stortingets vedtak og forutsetninger.

Komiteen viser videre til Riksrevisjonens konklusjoner:

«– Svak samordning av roller, ansvar og krav gjør arbeidet med digital sikkerhet krevende for virksomhetene.
- Justis- og beredskapsdepartementet har ikke sørget for god nok informasjon om den nasjonale digitale sikkerhetstilstanden.
- Justis- og beredskapsdepartementet har ikke sørget for god nok oppfølging av Nasjonal strategi for digital sikkerhet.
- Justis- og beredskapsdepartementet har ikke lagt godt nok til rette for tverssektoriell hendelseshåndtering.»

Komiteen slutter seg til Riksrevisjonens konklusjoner.

## 2.2 Om Riksrevisjonens kritikk

Komiteen viser til Riksrevisjonens kritikk:

«Samlet sett er det kritikkverdig at Justis- og beredskapsdepartementet med underliggende etater ikke har ivaretatt samordnings- og pådriveransvaret godt nok til å møte utfordringene på det digitale sikkerhetsområdet.

Det er videre kritikkverdig at

- Justis- og beredskapsdepartementet ikke har ivaretatt sitt pådriveransvar for å bidra til tilstrekkelig framdrift i arbeidet som følger av ny sikkerhetslov
- Justis- og beredskapsdepartementet ikke har lagt godt nok til rette for tverrsektoriell hendelseshåndtering
- det gjennomføres få tilsyn med digital sikkerhet og tilsynsmyndighetene er lite samordnet»

Komiteen slutter seg til Riksrevisjonens kritikk.

## 2.3 Om Riksrevisjonens anbefalinger

Komiteen viser videre til Riksrevisjonens anbefalinger:

«Riksrevisjonen anbefaler at Justis- og beredskapsdepartementet

- tar en tydeligere samordnings- og pådriverrolle for nasjonal digital sikkerhet i sivil sektor
- sørger for at Nasjonal sikkerhetsmyndighet i samarbeid med de andre veiledningsaktørene gjør veiledningen på det digitale sikkerhetsområdet mer samordnet og tilgjengelig
- sørger for bedre utnyttelse og koordinering av de etablerte arenaene for samordning
- gjennom pådriverrollen bidrar til at alle departementer har tilstrekkelig framdrift i arbeidet som følger av ny sikkerhetslov
- sikrer et bedre kildegrunnlag for å holde oversikt over den nasjonale digitale sikkerhetstilstanden
- sørger for bedre informasjon om resultater av iverksatte tiltak for å kunne vurdere behovet for endringer og nye tiltak på det digitale sikkerhetsområdet
- styrker arbeidet med å avdekke, håndtere og koordinere innsatsen mot alvorlige digitale hendelser»

Komiteen slutter seg til Riksrevisjonens anbefalinger.

Komiteen viser videre til, og tar til etterretning, statsrådens svar om at anbefalingene vil bli fulgt opp i samhandling med andre departementer.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet viser til at Riksrevisjonen i over 15 år har rapportert om utfordringer med digital sikkerhet i sivil sektor, både i den årlige kontrol-

len med forvaltningen av statlige selskaper, i den årlige revisjon og kontroll og i egne rapporter. Sårbarheter i samfunnskritiske systemer og svakheter i virksomheters og foretaks styring av digital sikkerhet har vært løftet fram. Disse medlemmer påpeker at i oppfølgingen av Riksrevisjonens anbefalinger om samordning av digital sikkerhet bør en helhetlig tilnærming til bedret sikkerhet og samordning av arbeidet legges til grunn. Disse medlemmer ser, i henhold til statsrådens svarbrev til Riksrevisjonen, at viktige grep er gjort etter avslutningen av undersøkelsesperioden, men at arbeidet vil ta tid.

Komiteens medlemmer fra Rødt og Venstre er kjent med at det digitale sikkerhetsarbeidet over tid ikke har vært tilstrekkelig i Norge. Disse medlemmer mener like fullt det er nødvendig å understreke at vi nå befinner oss i en svært usikker sikkerhetspolitisk situasjon med et forhøyet konfliktnivå og økende ustabilitet. Samtidig foregår det et teknologikappløp mellom verdens maktsentra. På denne bakgrunn mener disse medlemmer at rapportens funn, konklusjoner og anbefalinger må tas på største alvor og føre til umiddelbare tiltak for forbedring. Disse medlemmer mener man må legge til grunn at sivil norsk infrastruktur og tjenester også vil bli utsatt for digitale angrep i en krise- eller krigssituasjon, og Riksrevisjonens rapport beskriver for alle praktiske formål en vesentlig komponent av Norges totalforsvar. I den forbindelse imøteser disse medlemmer de rapportene som denne våren kommer fra Forsvarskommisjonen og Totalberedskapskommisjonen, og påfølgende offentlig debatt om hvordan vi best skaper digital sikkerhet i sivil sektor.

Disse medlemmer viser til at ansvarsprinsippet, som sier at «den organisasjon som har ansvar for et fagområde i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området», er ett av fire prinsipper som ligger til grunn for sikkerhets- og beredskapsarbeid. Dette er et prinsipp som disse medlemmer støtter. Men disse medlemmer mener at ansvarsprinsippet må være uløselig knyttet sammen med samordningsansvaret til Justis- og beredskapsdepartementet for at det nasjonale sikkerhets- og beredskapsarbeidet skal fungere. Den enkelte virksomhet settes bare i stand til å håndtere egen sikkerhet hvis den får tilstrekkelig informasjon om de til enhver tid gjeldende truslene den skal beskytte seg mot, fra sentrale myndigheter. Av naturlige årsaker er mye av informasjonen om trusselbildet for Norge ikke offentlig tilgjengelig. Men all den tid det daglige sikkerhetsarbeidet er, og må være, delegert til den enkelte virksomhet etter ansvarsprinsippet, er disse medlemmer av den bestemte oppfatning at sentrale myndigheter må tilstrebe løpende, rettidig og åpen informasjonsdeling i henhold til etablerte sikkerhetsprotokoller og andre rutiner. Åpenhet er også beredskap. For det andre mener disse medlemmer at nasjonal sikkerhet bare kan ivaretas dersom den enkelte virksomhets sikkerhetsarbeid ses i sammenheng av et samordningsorgan, en rolle som Justis- og beredskapsdepartementet er utpekt til å ha. Av den grunn er disse medlemmer skuffet over at det kommer fram av Riksrevisjonens rapport at Justis- og beredskapsdepartementet ikke har ivaretatt samordnings- og pådriveransvaret godt nok. Samtidig vil disse medlemmer understreke at det er positivt at Riksrevisjonen finner at Nasjonalt cybersikkerhetssenter (NSCS) er en velfungerende samordningsarena innen forebyggende sikkerhetsarbeid.

Disse medlemmer registrerer like fullt at representanter for kommunesektoren opplever det vanskelig å komme i kontakt med Nasjonalt cybersikkerhetssenter. Kommunesektoren understøtter flere kritiske samfunnsfunksjoner, og tjenestebortfall vil ramme offentlig tjenesteyting og enkeltmennesker i sårbare situasjoner. Løsepengevirusangrepet mot Østre Toten i 2021 førte for eksempel til at sosialhjelpsmottakere har vært nødt til å søke på nytt, og kommunen var uten datasystemer i en måned etter hendelsen. I tillegg kom personsensitiv informasjon på avveie. Totalt kostet angrepet kommunen minst 32 mill. kroner, i tillegg til bot fra Datatilsynet på 4 mill. kroner. Av dette har igjen staten kompensert Østre Toten med 16 mill. kroner. Disse medlemmer hadde forventet at man etter denne hendelsen hadde sørget for at det eksisterte forutsigbare og robuste kommunikasjonslinjer til kommunesektoren.

# 3. Komiteens tilråding

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

vedtak:

Dokument 3:7 (2022–2023) – Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor – vedlegges protokollen.

Oslo, i kontroll- og konstitusjonskomiteen, den 18. april 2023

**Peter Frølich**

leder og ordfører

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets administrasjon