NOTAT

AGENDA

POLITIKK MOT DIGITAL SÅRBARHET

Delrapport i prosjektet *Politikk for totalberedskap*

1/2021

Sammendrag

Stadig mer av livene våre digitaliseres. Dette gjelder også de grunnleggende strukturene i samfunnet. I hverdagen er vi avhengig av komplekse digitale systemer for å kommunisere med hverandre, kjøpe varer og tjenester, få tilgang på informasjon. Jobbene våre blir digitalisert, med digitale styringssystemer, utstyr koblet til internett, satellittbasert navigasjon. I offentlig sektor er saksbehandlingen digital, med skybaserte løsninger for programvare og arkivering i stadig utbredelse. Også beredskapsaktørene er fundamentalt avhengig av blant annet infrastruktur for elektronisk kommunikasjon og en stabil tilgang på kraft. Med en sammenpresset lønnsstruktur og et høyt lønnsgulv tas digitale løsninger i bruk raskere på norske arbeidsplasser enn i andre land, og Norge er i verdenstoppen på bruk av IKT. Det øker produktivitet og innovasjonsevne i både offentlig og privat sektor, men gjør også at arbeidet for å begrense digital sårbarhet blir en stadig viktigere del av totalberedskapen og det samlede beredskapsarbeidet.

Dette notatet peker på to overordnede trender innen digitalisering som også gjør oss sårbare. For det første blir stadig mer av livene våre og de grunnleggende strukturene i samfunnet fundamentalt avhengig av digitale løsninger. For det andre preges digitaliseringen av en økende kompleksitet, avhengighet mellom funksjoner, lange verdikjeder og tjenesteutsetting. Denne kompleksiteten gjør det svært vanskelig å få oversikt over hvilke sårbarheter som finner, og dessuten at sårbarheter ett sted i verdikjeden lett forplanter seg.

Vi tar til orde for følgende politiske grep:

- *Etablere en felles skytjeneste for forvaltningen. Tjenesten og den tilhørende fysiske infrastrukturen eies av staten. Skyløsningen skal i størst mulig grad bygges på åpen kildekode og sikres mot uautorisert tilgang. Løsninger for oppbevaring og prosessering av særlig sensitiv informasjon bør prioriteres først.*
- *Etablere strengere nasjonale krav til IKT-sikkerhet ved tjenesteutsetting. Disse kan bygge på NSMs anbefalte minimumskrav ved tjenesteutsetting og bør utvikles til absolutte krav i samarbeid mellom arbeidslivets parter og sektorekspertise.*
- *Øke robustheten i kjernenettet for elektronisk kommunikasjon gjennom å fullføre etableringen av et alternativt kjernenett*
- *Sette av økte midler over statsbudsjettet til utbygging av bredbånd og mobildekning*
- *Styrke beredskapen for strømbrudd gjennom flere øvelser, å gjøre en nasjonal kartlegging av tilstanden for nød- og reservestrøm i vitale samfunnsfunksjoner og å begrense sentralisering og oppsplitting i kraftsektoren gjennom å unnta nettselskap med færre enn 100.000 kunder fra energilovens bestemmelse om selskapsmessig og funksjonelt skille*
- *Styrke robustheten i de satellittbaserte posisjons-, navigasjons- og tidssystemene (PNT) gjennom aktiv norsk deltakelse i de europeiske satellitt-programmene, opprettholde og sikre installasjoner for visuell og radarbasert navigasjon langs norskekysten og utrede ytterligere back up-løsninger for satellittbortfall*

Innholdsfortegnelse

«Totalberedskap er en helhetlig tilnærming til sikkerhet og beredskap som tar utgangspunkt i de samlede truslene og sårbarhetene – og som har som målsetning å anvende samfunnets totale ressurser best mulig for å skape god beredskap for ulike krisesituasjoner.»

Fra Agenda-notatet Totalberedskap i Norge (2020)

1 Innledning

Trygghet og sikkerhet er myndighetenes fremste og viktigste oppgave. Tryggheten er alt det du slipper å tenke på i hverdagen. Vi kan bare leve gode liv når vi har trygghet for at om vi eller våre nærmeste blir syke, er det hjelp å få. Vi kan bare leve og arbeide når vi er trygge fra vold i hjemmet, innbrudd og overfall på gaten, trygge på at vi har tilgang på sunn mat og livsviktige medisiner.

I et forprosjekt for *Trygghet og totalberedskap 2021*-prosjektet, som dette notatet er en del av, samlet Tankesmien Agenda risikoanalyser fra offentlige etater i Norge, utforsket utviklingstrekk i trusselbildet og drøftet utfordringer i vår totalberedskap.

I disse risikoanalysene skiller pandemi og legemiddelmangel seg ut som utilsiktede kriser med både høy sannsynlighet og store konsekvenser. Blant tilsiktede krisescenarioer kan både vold, digitale angrep og sikkerhetspolitiske scenarioer få store konsekvenser.

Flere trender kan påvirke risikobildet. En av dem er geopolitisk ustabilitet og multilaterale samarbeid under press. En annen er polarisering som følge av blant annet økende ulikhet og migrasjon. En tredje er økt konkurranse om og knapphet av naturressurser, sammen med hyppigere ekstremvær og klimarelaterte naturhendelser.

Notatet fra forprosjektet peker på fire svakheter i vår nasjonale og lokale totalberedskap:

1) Den lokale beredskapen er ikke høyt nok prioritert. Ressursene strekker ikke til for å oppfylle den kommunale beredskapsplikten, politiet er mindre tilstede lokalt, brannvesenet tar oftere helseoppdrag og sivilforsvaret har blitt systematisk underprioritert.
2) Dårlig samarbeid mellom offentlige etater var en sentral del av 22. juli-kommisjonens kritikk. Samvirkeproblemene i beredskapen er ikke løst.
3) Helheten i beredskapen blir undergravet av at styringen består av mange, detaljerte kontrollmål som ikke lar seg prioritere. Antallet mål har økt på beredskapsfeltet siden 22. juli.
4) Oppsplitting og oppgaver som settes ut til det private skaper mer komplekse styringskjeder og økt sårbarhet i en krisesituasjon. Anbudsprosesser skaper sårbarhet i overgang mellom ulike tilbydere.

Totalberedskap er mer enn forsvar. God beredskap forutsetter at vi har tilstrekkelig bevissthet om risiko og trusler vi står overfor, evne til å forebygge mulige farer, og at vi har nødvendig beredskap for raskt å håndtere situasjoner som oppstår. Vi trenger et sterkt militært forsvar som svarer på våre tids trusler, men også erkjennelsen av at totalberedskap favner langt bredere enn Forsvaret. Totalberedskap innbefatter samfunnets samlede beredskapsressurser, herunder blant annet infrastruktur, helse, brann- og redning, politi og justis, samt forvaltningen av disse. Målsetningen er at ressursene i samfunnet organiseres målrettet og koordinert for å møte samfunnets helhetlige risikobilde.

Som en del av vår analyse har vi også etablert det vi mener er grunnleggende og generelle prinsipper for en styrket beredskap. Disse er:

- Tydelig toppforankring og prioritering av beredskapsarbeid og koordinering mellom nivå og sektorer
- Mer helhetlige og kontinuerlige risiko- og sårbarhetsanalyser på tvers av sektorer, mindre smal målstyring
- En sterk offentlig sektor med kontroll på forsyning av kritiske ressurser og kontroll over kritisk infrastruktur, samt hvor trygghet og beredskap blir ilagt større vekt i vurderinger knyttet til hvilke oppgaver som skal løses av det offentlige eller av private
- Ressurser til å både forebygge og å møte kriser når de inntreffer
- Større vekt på øving og styrking av samarbeid mellom offentlige etater, og offentlige etater og frivillige og private aktører
- Sterkere lokalsamfunn med næring, velferd, bosetting og beredskapsressurser over hele landet

Det digitaliserte samfunn er sårbart. Stadig mer av livene våre digitaliseres. Dette gjelder også de grunnleggende strukturene i samfunnet. I hverdagen er vi avhengig av komplekse digitale systemer for å kommunisere med hverandre, kjøpe varer og tjenester, få tilgang på informasjon. Jobbene våre blir digitalisert, med digitale styringssystemer, utstyr koblet til internett, satellittbasert navigasjon. I offentlig sektor er saksbehandlingen digital, med skybaserte løsninger for programvare og arkivering i stadig utbredelse. Også beredskapsaktørene er fundamentalt avhengig av blant annet infrastruktur for elektronisk kommunikasjon og en stabil tilgang på kraft. Ikke-digitale backup-løsninger vil være del av sårbarhetsreduksjonen for vitale samfunnsfunksjoner, men i dette notatet legger vi vekt på noen grep som kan gjøres for å gjøre digitale løsninger mer robuste. Med en sammenpresset lønnsstruktur og et høyt lønnsgulv tas digitale løsninger i bruk raskere på norske arbeidsplasser enn i andre land, og Norge er i verdenstoppen på bruk av IKT. Det øker produktivitet og innovasjonsevne i både offentlig og privat sektor, men gjør også at arbeidet for å begrense digital sårbarhet blir en stadig viktigere del av totalberedskapen og det samlede beredskapsarbeidet.

2 Utfordringene

Trusler og risikoer på det digitale områder kan komme i mange former[i], men grovt sett kan vi dele i *tilsiktede* og *utilsiktede* hendelser.

Tilsiktede hendelser utløst av trusselaktører kan komme i form av elektroniske angrep på nettelementer og drifts- og støttesystemer eller fysiske angrep på infrastruktur[ii]. Trusselaktører leter systematisk etter sårbarheter på det digitale området, med mål om å utnytte dem. Mange av disse truslene kan knyttes til fremmede staters eller andre aktørers etterretning, som søker å fremme egne interesser gjennom å skaffe seg tilgang på sensitiv informasjon om norske forhold, norsk industri, norsk infrastruktur, norsk forsvars- og beredskapsevne. De mer konkrete formålene kan være økonomisk vinning, å påvirke beslutninger i Norge eller å gjøre denne fremmede staten eller aktøren bedre forberedt på en konfliktsituasjon med Norge. Virkemidlene på det digitale området kan være mange, fra bruk av «insidere», til strategiske investeringer og oppkjøp, til en sammensatt vifte av virkemidler for å påvirke et valg, til bruk av droner og forstyrrelser av satellittbaserte systemer. Også IKT-kriminalitet utgjør en betydelig utfordring, hvor for eksempel uautorisert tilgang eller å hindre tiltenkt funksjonalitet til et IKT-system kan omsettes i penger.

Som en illustrasjon på de vidtrekkende konsekvensene tilsiktede hendelser på det digitale området kan ha, kan nevnes de to scenarioene for digitale angrep som er analysert av Direktoratet for samfunnssikkerhet og beredskap[iii]. Under scenarioet «digitalt angrep mot finansiell infrastruktur» blir alle betalingsterminaler, minibanker og nettbanker utilgjengelige i en uke som følge av et koordinert angrep. Under scenarioet «digitalt angrep mot ekom-infrastruktur» blir Telenors transportnett slått ut i fem dager av en fremmed makt, med konsekvens at krisehåndtering og redningsinnsats blir vanskelig, radio, tv og internett faller ut, jernbane- og flytrafikk stopper opp og betalingstjenester svikter.

Også *utilsiktede* hendelser kan ramme oss gjennom våre digitale systemer[iv]. Dette er hendelser hvor krisen ikke skapes av en beregnende aktør. En kategori av slike hendelser er *naturhendelser*. Dette kan komme i form av storm, flom, skred eller andre værhendelser som fører til fiberbrudd og strømbrudd. Det kan også komme i form av det vi kaller «romvær», som først og fremst knyttes til koronamasse slynget ut fra solen mot jorden. Slike solstormer kan både gi strømutfall og forstyrre satellittsignaler. En annen kategori av hendelser er knyttet til *svikt.* Dette kan være menneskelig svikt, hvor rutiner ikke følges, organisatorisk svikt, hvor virksomhetene har gjort et mangelfullt sikkerhetsarbeid, eller systemsvikt, hvor fysiske komponenter bryter sammen eller logiske feil i programkode ender i systemsvikt.

Dette kapitlet peker på to viktige, overordnede trekk ved den digitale utviklingen som gjør oss sårbare. For det første at samfunnet blir stadig mer avhengig av digital infrastruktur, elektronisk kommunikasjon, satellitter og kraft. Også mye av det vi ikke tenker over, er digitalt. For det andre gjør lange verdikjeder – også utover våre landegrenser – gjør at kompleksiteten i det digitale sårbarhetsbildet er økende, og at feil ett sted i verdikjeden kan forplante seg og få enorme konsekvenser.

2.1 Stadig mer av samfunnet digitaliseres

Utviklingen på det digitale området går svært raskt. En av konsekvensene av dette er at mange av de digitale sårbarhetene er ukjente, feilvurderte eller ikke forstått. Dette problemet gjelder i større grad på det digitale området enn for mange andre sårbarheter[v].

Digitaliseringen treffer samfunnet bredt. Eksempler fra tre bransjer kan illustrere hvordan digitaliseringen kan se ut i praksis, og hvordan det skaper nye avhengigheter og sårbarheter.

- I *landbruket* er et økende antall oppgaver som tidligere ble gjort manuelt, i dag digitalisert – som melkeroboter og innmelding av slakt. Det har gitt en effektiviseringsgevinst, men også nye utfordringer i form av datatyveri og digital utpressing.
- I *olje og gass-næringen* har fallende lønnsomhet tvunget fram raskere digitalisering enn tidligere, med større innslag av automatisert utstyr, digitale planleggingsverktøy og mer fjernstyring. I bransjen har det vært uttrykt bekymring over betydningen av fjernstyring for ulykkesrisiko, hvor fjernstyring av prosesser skaper større avstand mellom de som håndterer styringssystemene og de som er tett på den faktiske risikoen[vi], og dessuten at datanettene kan være sårbare for avlytting, inntrenging og manglende tilgjengelighet. Olje- og gassvirksomhet er utsatt for spionasje, for eksempel knyttet til informasjon fra letevirksomhet, og er dessuten en bransje som tydelig illustrerer den fundamentale avhengigheten av samfunnets systemer for elektronisk kommunikasjon, kraft og satellittbaserte tjenester.

Sikkerhetskultur

Menneskelige feil er en viktig faktor i uønskede IKT-hendelser. I en undersøkelse gjennomført av Næringslivets sikkerhetsråd, svarer 55 % av bedriftene som har opplevd sikkerhetsbrudd at menneskelige feil var en av årsakene og 39 % at manglende sikkerhetsbevissthet var en av årsakene[xiv]. Næringslivets sikkerhetsråd foreslår følgende tiltak for å fremme digital sikkerhetskultur i den enkelte virksomhet:[xv]

- Sørg for at medarbeiderne får opplæring i virksomhetens sikkerhetsrutiner med et spesielt fokus på å motstå sosial manipulering og svindel
- Styrk medarbeidernes sikkerhetskunnskap, eksempelvis ved hjelp av opplæringspakker fra NorSIS og intern trening. Nasjonal sikkerhetsmåned arrangeres hver oktober og kan brukes til å gi medarbeidere innsikt i trusselbildet og hvordan de ved å følge virksomhetens sikkerhetsprosesser kan minske faren for uønskede hendelser
- Kartlegg virksomhetens digitale sikkerhetskultur for å avdekke om det er behov for å igangsette tiltak
- Økonomimedarbeidere bør få opplæring om direktørsvindel, og virksomheten bør innføre rutiner rundt overføringer av større beløp som gjør det vanskeligere for direktørsvindlere å lykkes

På nasjonalt nivå spiller Norsk senter for informasjonssikring (NorSIS) en viktig rolle i å understøtte virksomhetenes IKT-sikkerhetsarbeid, blant annet gjennom bevisstgjøringskampanjen Nasjonal sikkerhetsmåned.

- Innen *sjøfart* er en rekke sentrale systemer nå tuftet på digitale løsninger. Dette gjelder for eksempel digitale kart posisjoneringssystemer som GPS, kommunikasjon og landbaserte systemer for administrasjon av havner, last og passasjerer. Digitalisering i denne bransjen, som i andre bransjer, kan føre til økt sikkerhet – blant annet gjennom å redusere sannsynligheten for menneskelig svikt. Samtidig finnes det flere eksempler på at en overdreven tillit til for eksempel digitale navigasjonssystemer svekker årvåkenheten hos skipsføreren[vii]. Også en mulig utvikling i retning av autonome skip viser hvordan digitalisering og automatisering kan skape nye former for sårbarheter, hvor hacking av en fysisk gjenstand – i dette tilfellet et skip – kan føre til fysiske konsekvenser.

Flere trender vil framover sannsynligvis ytterligere fordype vår avhengighet av digitale systemer og følgelig påvirke det digitale sårbarhetsbildet[viii]. *Kunstig intelligens og maskinlæring* kan automatisere digitale angrep som tidligere var svært arbeidsintensive eller umulige – for eksempel store, målrettede angrep med epost eller å styre svermer med tusenvis av mikrodroner eller persontilpasset desinformasjon. *Tingenes internett,* at alt fra smartklokker, strømmålere, fabrikker og biler blir avhengig av internett, gjør at stadig flere fysiske gjenstander potensielt kan hackes, utsettes for datakrasj eller bli utilgjengelige på grunn av nettfeil. *5G,* neste generasjons internett, vil gjøre det mulig med massiv maskin-til-maskin-kommunikasjon og stabil dekning for mange enheter samtidig, med blant annet ytterligere utbredelse av tingenes internett som sannsynlig konsekvens, og dessuten en sentralisering av driftssentre som krever nye former for sikkerhetstenkning.

2.2 Økende kompleksitet og lange forsyningskjeder

Digitaliseringen fører med seg økt kompleksitet og avhengighet mellom digitale funksjoner. Denne kompleksiteten gjelder for mange samfunnsområder, men er særlig stor for digitale løsninger som går på tvers av sektorer og land, er mer stedløse enn det meste annet, og er så vidtrekkende i bruk at det nesten ikke er mulig å snakke om digitalisering som et samfunnsområde. Kompleksiteten gjør det vanskelig å få oversikt over sårbarheter og å motarbeide dem. Ofte er digitale løsninger avhengig av underleverandører med nye underleverandører i flere lag under seg. Dette svært spesialiserte nettverket av aktører bidrar til effektivitet og gode tjenesteleveranser. Samtidig vil sårbarheter i hos en underleverandør forplante seg oppover i verdikjeden. Trusselaktører vil utnytte sårbarheter ett sted i verdikjeden for å få tilgang til informasjon og funksjoner andre steder i kjeden.

Et eksempel på hvordan dette kan spille seg ut i praksis, var da IT-arbeidere i India med ett driftet det norske Nødnettet, uten autorisasjon og sikkerhetsklarering, i strid med Sikkerhetsloven[ix]. Med denne tilgangen kunne de indiske IT-arbeiderne stengt ned deler av Nødnettet, uten at norske myndigheter kunne forhindret nedstengningen. Eiene av linjer Nødnettet driftes på er Motorola og Broadnet, og Broadnet hadde outsourcet drift til det indiske selskapet Tech Mahindra. Denne outsourcingen skjedde trass i at Broadnet hadde forpliktet seg overfor myndighetene om at Nødnett-linjene skulle driftes fra Norge. Nasjonal kommunikasjonsmyndighet ila Broadnet en bot på 14 millioner kroner som følge av utilstrekkelige risiko- og sårbarhetsanalyser og utilstrekkelig tilgangsstyring[x]. Et annet eksempel fant sted innen infrastrukturmoderniseringen i Helse Sør-Øst i 2017.

Sykehuspartner HF inngår i 2016 etter et anbud en kontrakt om infrastrukturdrift og -modernisering med Hewlet-Packard Norge, som senere overførte kontrakten til Enterprice Services, del av selskapet DXC Technology. NRK avdekker i 2017 at utenlandske IT-arbeidere har fått tilgang på sensitive personopplysninger for pasienter gjennom prosjektet. En granskingsrapport konkluderer med at Sykehuspartner HF ikke hadde kontroll på tilgangsstyring, hadde mangelfulle risikovurdering og at flere varsler ikke nådde fram til ledelsen og styret i Helse Sør-Øst[xi]. Både Helse Sør-Øst- og Nødnett-saken illustrerer sviktende arbeid med IKT-sikkerhet, men også et uttrykk for at lange verdikjeder gjør det komplekst for myndighetene å få oversikt over hvilke sårbarheter som finnes i for et system man kjøper inn.

Tjenesteutsetting er å forstå som et tveegget sverd for den digitale sårbarheten. Det har både fordeler og ulemper ved seg i et IKT-sikkerhetsperspektiv. En tydelig fordel med mange innkjøp av tjenester er at kompetansen på IKT-sikkerhet typisk vil være høy hos en stor og profesjonell aktør, blant annet fordi det å drifte systemer over tid gjør at man oppdager feil og får erfaringer med å være utsatt for angrep. Et stabilt kompetansemiljø som drifter et system over tid vil typisk være mer robust enn det mange virksomheter selv er i stand til å opprettholde over tid.

Utfordringene med tjenesteutsetting er imidlertid også betydelige. Det regjeringsoppnevnte Lysne-utvalget omtaler komplekse digitale verdikjeder som «en kjerneutfordring» ved vurdering av digital sårbarhet, «et vesentlig hinder» for å kunne fastslå hvilken sårbarhet som finnes og en utfordring som gjelder på tvers av alle sektorer[xii]. «Eierskapsstrukturer og uautorisert tilgang til informasjon kan være vanskelig å kontrollere», er blant utfordringene med tjenesteutsetting Nasjonal sikkerhetsmyndighet trekker fram[xiii]. Utsetting av IKT-tjenester kan også føre til tap av kompetanse på virksomhetens systemer og kontroll med utvikling av systemer over tid, som i seg selv skaper sårbarhet: Da mister svekkes innkjøpers evne til å følge opp IKT-sikkerheten hos tilbyder.

Noen særlige utfordringer gjelder verdikjeder som strekker seg over landegrenser. Ved fysiske lokasjoner i andre land, vil sårbarheten i den fysiske infrastrukturen være vanskeligere å ettergå. Juridisk sett er også norske IKT-sikkerhetsmyndigheter avhengig av at de digitale systemene befinner seg under norsk lovgivning for å kunne bedrive inntrengningstesting på systemene. Dessuten vil tilgangen på data lokalisert på servere i et annet land være underlagt et annet lands lovgivning, med de konsekvenser det kan ha for tilgangen på data. Norske myndigheter har for eksempel ikke mulighet til å sanksjonere tjenesteleverandører utenfor EØS-området.

Det vil i praksis ikke være mulig eller ønskelig med et digitalisert samfunn uten betydelige innslag av lange forsyningskjeder og systemer som strekker seg på tvers av land. Dette trekket ved det digitaliserte samfunnet bør imidlertid være grunnleggende for arbeidet med reduksjon av digital sårbarhet.

3 Politikk for digital sårbarhet

Vi kommer til å bli mer, ikke mindre digitale i årene som kommer. Det betyr at vi må erkjenne sårbarheter, og lage systemer for utvikling, innkjøp og drift som reduserer vår sårbarhet. Vi tar til orde for tre typer grep som kan bidra til dette.

3.1 Skytjenester for det offentlige på statlig eide servere

En viktig digital trend er den økende bruken av skytjenester, altså skalerbare digitale tjenester levert over nett (beskrevet i tekstboksen til høyre[xvi]).

Også for offentlig sektor er bruken av skytjenester økende, for eksempel for bruk av fillagring, dokumentbehandling og videokonferanse. Begrunnelsene er typisk økt fleksibilitet, lavere kostnader og tilpassing til hvilke tjenester som faktisk leveres[xvii].

Sikkerhetsmessig innebærer innkjøp av skytjenester samme slags dilemmaer som annen tjenesteutsetting av IKT, slik forrige kapittel redegjorde for, med på den ene siden høy kompetanse og kapasitet på IKT-sikkerhet de store, internasjonale skytjenesteleverandørene, samtidig som innkjøp kan føre til redusert kontroll.

Hva er skytjenester?

Den amerikanske standardiserings-organisasjonen NIST definerer skytjenester ved hjelp av følgende fem kjennetegn:

- *Behovsbaserte:* Kunden kan selv ta i bruk tjenester etter behov, uten å involvere leverandør
- *Levert over nett:* Kunden får tilgang over nett til tjenester for ulik maskinvare (f.eks nettbrett, PCer)
- *Ressursdeling:* Leverandøren kan fordele dataressursene sine dynamisk etter kundenes behov
- *Umiddelbar fleksibilitet:* Tjenestene kan skaleres opp eller ned etter kundens behov
- *Betaling etter bruk*: Bruken måles på en måte som er transparent for både bruker og leverandør

En problemstilling er knyttet til hvor serverne befinner seg geografisk. Økt bruk av skytjenester vil kunne bety at større deler av den digitale offentlige sektor befinner seg i utlandet. Selv om dette skjer hos selskaper med store, profesjonelle sikkerhetsmiljøer, vil det være flere problematiske sider ved offshoring, og det er ikke alle deler av den digitale offentlige sektor det vil være ønskelig at befinner seg på servere i andre land. For det første vil data som krysser landegrenser også krysse avlyttingssystemene som er bygget inn i andre lands digitale grenseforsvar. For det andre vil det juridisk være slik at det er opp til det landet serveren befinner seg å bestemme lovene som regulerer for eksempel utlevering av data på serveren. For det tredje vil den fysiske sikkerheten knyttet til serverne være vanskeligere å ettergå om de befinner seg i et annet land, og dessuten vanskeligere å eventuelt drive objektsikring. For det fjerde vil den geografiske plasseringen av fysisk infrastruktur kunne ha stor betydning i en krigssituasjon. Disse argumentene taler for at det bør finnes servere for skytjenester for offentlig sektor i Norge. Som Nasjonal sikkerhetsmyndighet formulerer det: «De aller fleste av

skytjenestetilbyderne har ikke installasjoner på norsk jord og må derfor tilby sine tjenester fra utlandet. Dette innebærer en betydelig risiko»[xviii].

I Tyskland blir en statlig skyløsning nå rullet ut, under navnet *Bundescloud.* Begrunnelsene for dette har vært flere. Det er tenkt å være en sikker digital infrastruktur for den føderale administrasjonen, hvor den tyske staten har suverenitet over dataene. Det er også begrunnet med effektivisering, hvor tanken er at det skal bidra til standardisering og til at mer fleksible digitale løsninger blir innført raskere. Bundescloud benytter seg av høysikkerhetsservere som befinner seg flere steder i Tyskland, og hvor de fysiske serverne er eid av staten. Programvaren er satt ut på anbud[xix], herunder utvikling, vedlikehold, support og videreutvikling. Selskapet Nextcloud vant anbudskonkurransen. Et viktig element i utformingen av Bundescloud er at det ble stilt som krav fra myndighetene at programvaren skulle være med åpen kildekode, som betyr at man ikke er bundet til ett selskap sin proprietære programvare, og at man begrenser de lock-in-effektene som ville gjort at man var bundet til ett enkelt selskaps løsninger over tid. Løsningen med åpen kildekode gjør også at en annen leverandør kan videreutvikle og bygge ut programvaren i en senere omgang. Åpen kildekode som løsning står ikke i veien for kryptering eller andre IKT-sikkerhetshensyn.

Bundescloud inkluderer både *Infrastructure as a Service* (f.eks. lagringskapasitet tilgjengelig i skyen), *Software as a Service* (programvare tilgjengelig for å kjøres over internett) og *Platform as a service* (hardware- og software-verktøy tilgjengelig over internett for å utvikle tilpassede applikasjoner i den enkelte virksomhet).

Brukere kan bare få tilgang på skytjenestene med passord gjennom en datamaskin eller smarttelefon utstedt av myndighetene. Bundescloud er utviklet for å være en skytjeneste for det føderale nivåets 200.000 ansatte, men er tiltenkt å kunne inkorporere delstatenes skytjenester på et senere tidspunkt.

Flere land har diskusjoner om lignende løsninger. Den franske statens skystrategi, lansert i 2018, legger opp til å etablere en egen skyløsning for staten, men virksomhetene kan velge å kjøpe inn skytjenester i markedet for mindre sensitive data og programmer[xx]. Nederland startet i 2014 etableringen av en statlig skytjeneste under navnet *Rijkscloud.* Skytjenesten bygger på programvarene OpenStack, KVM og Ceph og er spredt på fysiske servere ulike steder i Nederland[xxi]. I Sverige er diskusjonen åpen om hvorvidt man ønsker en statlig skytjeneste[xxii]. Administrasjonsetaten Statens servicesentral har argumentert for besparelser på flere hundre millioner svenske kroner hvert år ved samordning av IKT-tjenester i en felles statlig sky, sammenlignet med dagens situasjon[xxiii].

Det er mulig å se for seg skytjenester på servere i Norge også uten å etablere en Bundescloud-lignende løsning. Politisk vil dette innebære å tilrettelegge for at de store skyselskapene – som Microsoft, Amazon eller Alibaba – etablerer seg med fysisk infrastruktur i Norge, for så kjøpe tjenester på disse serverne. Da kan man tydeligere dra fordelene av de store selskapenes sikkerhetsmiljø. Ulempen er at man får mindre direkte kontrollinjer knyttet til ivaretakelsen av infrastrukturen. Dessuten er arkiv- og datalagring et sentralt offentlig myndighetsområde som gjennom lov har vært underlagt offentlig eierskap, styring og kontroll. I tillegg er det uklarheter knyttet til utenlandsk lovgivning for utenlandske selskaper i Norge. Amerikanske CLOUD-act er det tydeligste eksempelet. Loven gir

amerikanske myndigheter rett til å be om kundedata fra selskaper som faller under amerikansk jurisdiksjon, selv om serverne er plassert i Norge[xxiv]. En juridisk ekspertgruppe under Esam, et samarbeidsorgan for digitalisering i svensk offentlig sektor, har konkludert med at det ikke kan utelukkes at skytjenester levert av utenlandske selskaper overleverer informasjon fra bruker av skytjenesten til de myndigheter selskapet svarer til[xxv], og Esam advarer mot konsekvensene dette har for informasjon som faller under den svenske *offentlighets- och sekretesslagen*. Lovgrunnlaget for å beskytte data som lagres utenfor landets grenser er dessuten ikke alltid godt nok. Det illustreres tydelig av *Schrems II*-dommen[xxvixxvii] fra sommeren 2020, som slår fast at det trengs strengere regulering av personopplysninger som utleveres mellom EU/EØS-området og USA. Særlig alvorlig blir dette juridisk uklare rommet internasjonalt i møte med stater verre enn USA. Uansett vil rettstilstanden på dette området ikke kunne bestemmes av Norge alene, noe som i seg selv gir mindre kontroll på offentlig sektors data og digitale systemer enn hva vi hadde før overgangen til skytjenester. Nasjonal sikkerhetsmyndighet er bekymret for at

Forslag:

- *Etablere en felles skytjeneste for forvaltningen. Tjenesten og den tilhørende fysiske infrastrukturen eies av staten. Skyløsningen skal i størst mulig grad bygges på åpen kildekode og sikres mot uautorisert tilgang. Løsninger for oppbevaring og prosessering av særlig sensitiv informasjon bør prioriteres først.*

NSMs anbefalte minimumskrav ved tjenesteutsetting

- Et etablert styringssystem for informasjonssikkerhet og sertifisering i henhold til internasjonale standarder, for eksempel ISO/IEC 27001:2017.
- Innsyn i sikkerhetsarkitekturen som benyttes for å levere tjenesten
- Utviklingsplaner for sikkerhet i tjenesteproduksjonen i tråd med utvikling i teknologi og trusselbildet over tid
- En oversikt over hvem som skal ha innsyn i virksomhetens informasjon, hvor og hvordan denne skal behandles og lagres samt grad av mekanismer for segregering fra andre kunder
- Tilgangsstyring som inkluderer kryptering, aktivitetslogging og fysisk og logisk sikkerhet
- Sikkerhetsovervåkning egnet til å avdekke hendelser og handlinger i tråd med virksomhetens trusselbilde og relevante trusselbilde og relevante trusselaktører
- Rutiner for hendelseshåndtering av avviks- og sikkerhetsrapportering
- Krise- og beredskapsplaner som skal harmonisere med virksomhetens egne planer
- Godkjenningsprosedyrer for bruk av underleverandører og deres bruk av underleverandører
- Spesifisert hvilke aktiviteter som skal utføres ved terminering av kontrakten, blant annet tilbakeføring/flytting/sletting av virksomhetens informasjon.

3.2 Strengere krav til IKT-sikkerhet i anskaffelser

Digitalisering er i økende grad en del av kjerneoppdraget for offentlige virksomheter, etter hvert som vi blir mer digitale. Det betyr at det ikke i det enkelte tilfelle er åpenbart riktig å kjøpe inn IKT som en tjeneste fra private leverandører. Offentlige virksomheter vil i også måtte bygge og opprettholde sin egen digitale kompetanse og løsninger. Som vi påpekte i forundersøkelsen til dette prosjektet, er oppsplitting og konkurranseutsetting i mange tilfeller med på å øke vår sårbarhet, fordi helhet og forebygging svekkes. På det digitale området er en tilleggsutfordring at data og operativsystemer kan komme på avveie, også utenfor Norges grenser.

For mange av IKT-tjenestene det offentlige benytter seg av, vil det likevel være hensiktsmessig å løse oppgavene gjennom anskaffelser i markedet. I disse tilfellene må sikkerhet og trygghet få større plass. Gode innkjøp forutsetter også god egen kjernekompetanse. Likevel kan sikkerhetsutfordringer også være vanskelige å forutse og krevende for små innkjøpere å selv forhandle frem. Det bør derfor pålegges å stille strengere og felles krav gjennom anbudskontraktene fra offentlige innkjøpere. Slike strenge krav til tilbydere gjennom anbudskontrakter har for eksempel med stor effekt blitt gjort av flere kommuner og fylkeskommuner for å håndtere useriøse forhold i bygge- og anleggsbransjen, slik Agenda-notatet *Fra Skiensmodell til Oslomodell for hele landet*[xxviii]*.* Også kravene til IKT-sikkerhet ved tjenesteutsetting kan strammes inn. Det finnes i dag ulike reguleringer av IKT-sikkerhet gjennom en rekke lover og forskrifter, for eksempel Beredskapsforskriften for kraftsektoren og IKT-forskriften for finanssektoren. Det regjeringsoppnevnte Holte-utvalget har likevel påpekt at det for mange sektorer i dag ikke gjelder krav til IKT-sikkerhet ved relevante anskaffelser. Også i tilfeller hvor det faktisk stilles krav til IKT-sikkerhet er det uklart hvilke krav som stilles til sikring[xxix]. Et utgangspunkt for tydeligere regulering bør være de ulike standardavtalene, kontraktsmalene og veilederne som finnes på området. Sentral er Nasjonal sikkerhetsmyndighets *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting*[xxx]*.* Her listes det blant annet opp 10 anbefalte minimumskrav for tjenesteutsetting – som også er gjengitt i tekstboks på side 13. Disse anbefalte kravene kan være utgangspunkt for krav offentlige virksomheter *skal* stille ved tjenesteutsetting. Hvis ikke myndighetenes i det enkelte tilfelle er i stand til å ettergå de kravene til IKT-sikkerhet som er satt i kontrakter, må enten kapasiteten myndighetene har til å følge opp IKT-sikkerheten ved tjenesteutsetting oppskaleres, eller så må oppgavene gjøres i offentlig regi.

- *Etablere strengere nasjonale krav til IKT-sikkerhet ved tjenesteutsetting. Disse kan bygge på NSMs anbefalte minimumskrav ved tjenesteutsetting og bør utvikles til absolutte krav i samarbeid mellom arbeidslivets parter og sektorekspertise.*

3.3 Sikrere og bedre fysisk infrastruktur

Samfunnets fundamentale avhengighet av digital infrastruktur betyr at bortfall av denne infrastrukturen vil få svært alvorlige konsekvenser for samfunnet. Den økende avhengigheten betyr at konsekvensene blir stadig større.

En viktig del av denne infrastrukturen er *det nasjonale ekomnettet*, nettverket for tele- og datakommunikasjon. I ekomnettet utgjør Telenors kjernenett «motorveien», som andre

nettverk er koblet opp mot. Det betyr at, slik vi så i kapittel 2, bortfall av kjernenettet vil få svært store konsekvenser for nesten all elektronisk kommunikasjon i Norge. Et slikt bortfall er lite sannsynlig og kjernenettet beskrives typisk som svært robust – men konsekvensene av et bortfall rettferdiggjør at det settes inn betydelige tiltak for å ytterligere redusere sannsynligheten for en krise. En av de viktigste anbefalingene fra Lysne-utvalget var å øke robustheten i kjernenettet, fordi «den totale summen av samfunnsverdier [Telenors kjernenett] bærer, er uakseptabelt høy»[xxxi]. Det er overordnet sett to måter å øke robustheten. Den ene er å etablere et alternativt kjernenett, med samme kapasitet og omfang som Telenors kjernenett. Den andre er å i større grad benytte seg av eksisterende infrastruktur og opprette flere samtrafikkpunkter for omruting av trafikk mellom ulike operatørers nett, for å slik redusere den totale sårbarheten[xxxii]. Lysne-utvalget gikk inn for det første, mest ambisiøse av disse. Etter Lysne-utvalget har det blitt satt av midler til pilotprosjekt for alternativt kjernenett, uten at dette foreløpig har ført til konkrete resultater[xxxiii].

Det er imidlertid store geografiske variasjoner i tilgang på tele- og datakommunikasjon. I tettbygde strøk har 98 prosent tilgang på høyhastighetsbredbånd med fiber, mens 59 prosent har det samme i distriktene med spredt bosetting[xxxiv]. Om lag 20 prosent av det norske landarealet er uten dekning for 4G mobildata, med lavest dekning for Sogn og Fjordane og Troms[xxxv]. Tilgang på bredbånd og mobildekning er avgjørende for tilgang på informasjon og kommunikasjon i krisesituasjoner og arbeidet med å utbedre tilgangen på dette bør styrkes gjennom økte midler. Et videre moment som taler for økte midler til utbygging av ekom-tjenester utenfor tettbygde strøk, er at midler til flere alternative ekom-linjer med geografisk atskilte traseer vil bidra til å redusere sårbarheten for regionale eller lokale bortfall ved naturhendelser, strømbrudd eller graveskader på kabler.

En ytterligere problemstilling gjelder *vedlikehold og beredskap for infrastruktur for strøm*. En situasjon med langvarig strømmangel blir svært utfordrende. Samfunnet er fundamentalt avhengig av kraft, og dette gjelder i særdeleshet digitale løsninger. Det bør legges opp til flere øvelser for langvarig strømbrudd, og nødstrømkapasiteten for vitale samfunnsfunksjoner må kartlegges. Det finnes en regional kartlegging gjort av fylkesmennene i Nordland og Vestfold, men ikke en nasjonal ROS-analyse av nødstrømkapasitet. For særlig den regionale og lokale forsyningssikkerheten av kraft er det en forutsetning med lokalkunnskap og å være raskt til stede ved et strømbrudd. Det krever beredskapskapasitet i nettselskapene lokalt. Denne kapasiteten påvirkes av energilovens bestemmelse om selskapsmessig og funksjonelt skille for nettselskaper som innføres januar 2021. Denne bestemmelsen innebærer i korthet at den monopolvirksomheten som ligger i drift av strømnett må driftes som et helt atskilt selskap fra den virksomheten som konkurrerer på ordinære markedsvilkår om for eksempel utbygging av bredbånd og utskifting av gatelys. Argumentasjonen for å skille monopol- og konkurranseutsatt del av virksomheten er å forhindre kryssubsidiering mellom konkurranse- og monopolvirksomhet, og slik legge til rette for mer konkurranse. Et ønske om å konsolidere sektoren i færre, større kompetansemiljøer er også et argument for bestemmelsen[xxxvi]. Konsolidering i færre, større selskaper og/eller redusert bemanning i de lokale nettselskapene er konsekvensen av innføring av bestemmelsen om selskapsmessig og funksjonelt skille. Det vil svekke lokalkunnskapen og den lokale tilstedeværelsen av montører som kjenner terreng og

strømnett. Begge deler er viktig for strømberedskapen. Gjennom EØS-avtalen er alle EU- og EØS-land pålagt å innføre et selskapsmessig og funksjonelt skille for nettselskaper med flere enn 100.000 kunder. Bestemmelsen som innføres januar 2021 i Norge omfatter imidlertid også alle nettselskap med færre enn 100.000 kunder[xxxvii]. Bare et lite mindretall av de største selskapene omfattes av EØS-bestemmelsen.

En siste viktig del av den nasjonale infrastrukturen er *satellittkommunikasjon*. En lang rekke systemer og mye funksjonalitet – også samfunnskritiske systemer og funksjonalitet – er i økende grad avhengig GPS-posisjonering og lignende systemer. Sjøfarten illustrerer dette tydelig, hvor globale posisjoneringssystemer som GPS er helt avgjørende for navigasjon. Bortfall av satellittnavigasjon betyr blant annet økt sannsynlighet for ulykker. Bortfall kan for eksempel skyldes eksplosjoner i solas atmosfære (solstorm), eller tilsiktede hendelser som «jamming» og «spoofing», hvor en trusselaktør henholdsvis blokkerer signaler ved hjelp av en støysender eller sender ut falske posisjoneringssignaler med hensikt å forvirre for eksempel en GPS-mottaker om den faktiske posisjonen.

Det finnes flere måter å navigere på uten satellitt. Skip kan navigere ved hjelp av fyr, lykter, bøyer og andre sjømerker, inkludert radiofyr, fartsmålere, ekkolodd og elektroniske sjøkart[xxxviii]. Også for fly finnes bakkebaserte radionavigasjonssystemer på helt andre frekvenser enn satellittsystemene. Før GPS var det bakkebaserte systemet Loran-C viktig for navigasjon[xxxix]. Fordi bruken falt og få hadde mottakere for dette systemet etter innføringen av GPS, ble de sendemastene i Norge revet på 2010-tallet[xl]. I Storbritannia har man valgt å beholde et videreutviklet Loran-C-system (eLoran), fordi det anses som en nyttig backup til GPS som på grunn av de sterke signalene er særlig rubust mot jamming.

Fordi vi blir stadig mer avhengig av GPS-systemet, blir konsekvensene stadig større dersom GPS faller bort. En ny rapport fra *US Department of Homeland Security* understreker at egenberedskap for kortvarige bortfall er avgjørende, slik det er avgjørende med egenberedskap for kortvarige strømbortfall[xli]. En slik egenberedskap kommer for eksempel i norsk kontekst i form av kompetente sjøfolk med kompetanse til både å navigere etter annet enn satellitt, og kunnskap om lokale vanskelige forhold. Samtidig vil det være fornuftig å stimulere også norsk industri til å utvikle nye løsninger som skaper større navigasjonsrobusthet – for eksempel videreutvikling av systemer for radiofyr og intelligente antenner.

Et helt konkret grep for å gjøre Norge mindre sårbar for GPS-bortfall, er fortsatte norske bidrag til videreutviklingen av det europeiske alternativet til GPS, gjennom de såkalte Galileo- og EGNOS-programmene. Disse systemene har blant annet hatt til hensikt å gi større nøyaktighet enn GPS og bedre dekning i Barentshavet, men det har også vært en viktig hensikt å øke robustheten langs flere akser. For det første: Gjennom egne satellittsystemer er Europa ikke er avhengig av at USA opprettholder GPS-systemet. For det andre vil satellittene være spredt over en større del av himmelen enn hva GPS-satellittene vil være alene. I tillegg inneholder Galileo et kryptert signal (PRS) på andre frekvenser, som er mer robuste mot jamming og spoofing. Disse krypterte signalene er tilgjengelig for ikke bare militære mottakere, som de krypterte signalene i GPS, men også for andre beredskapsaktører (som redningstjeneste, politi, kystvakt, brannvesen og sivilforsvar). Norge

har deltatt i EU-romprogrammene fram til nå gjennom EØS-avtalen. Det har gitt mulighet til medbestemmelse over utformingen, næringsmuligheter for norsk romindustri, tilgang på krypterte signaler for sivile beredskapsaktører, i tillegg til at det har vært et bidrag til det globale fellesgodet satellittnavigasjon er[xlii].

Forslag:

- *Øke robustheten i kjernenettet for elektronisk kommunikasjon gjennom å fullføre etableringen av et alternativt kjernenett*
- *Sette av økte midler over statsbudsjettet til utbygging av bredbånd og mobildekning*
- *Styrke beredskapen for strømbrudd gjennom flere øvelser, å gjøre en nasjonal kartlegging av tilstanden for nød- og reservestrøm i vitale samfunnsfunksjoner og å begrense sentralisering og oppsplitting i kraftsektoren gjennom å unnta nettselskap med færre enn 100.000 kunder fra energilovens bestemmelse om selskapsmessig og funksjonelt skille*
- *Styrke robustheten i de satellittbaserte posisjons-, navigasjons- og tidssystemene (PNT) gjennom aktiv norsk deltakelse i de europeiske satellitt-programmene, opprettholde og sikre installasjoner for visuell og radarbasert navigasjon langs kysten og utrede ytterligere back up-løsninger for satellittbortfall*

Notatet er skrevet av Axel Fjeldavli. Forfatteren står ansvarlig for alle eventuelle feil og mangler i dokumentet. Ta gjerne kontakt dersom du finner slike.

Tankesmien Agenda vil rette en stor takk til flere som har tatt seg tid til å svare på faglige spørsmål underveis.

Prosjektet «Trygghet og sikkerhet 2021», som dette notatet inngår i, er et samarbeid mellom Tankesmien Agenda, Fagforbundet, Fellesforbundet, Fellesorganisasjonen, Industri Energi, LO, LO Stat, Norges Bondelag, Norsk Nærings- og Nytelsesmiddelarbeiderforbund, Norsk Sjømannsforbund, Norsk Sjøoffisersforbund, Norsk Tjenestemannslag, Norges offisers- og spesialistforbund og Pensjonistforbundet.

4 Referanser

Den europeiske unions domsstol. (2020). Schrems II - C-311/18, EU:C:2020:559. Luxembourg: Den europeiske unions domsstol. Hentet fra http://curia.europa.eu/juris/documents.jsf?num=C-311/18

Direktoratet for samfunnssikkerhet og beredskap. (2019). *Analyser av krisescenarioer 2019.* Tønsberg: Direktoratet for samfunnssikkerhet og beredskap.

Ellingsen, B. (2017). Hva gjør vi når GPS-en svikter? *Forskning.no*. Hentet fra https://forskning.no/norsk-romsenter-partner-satellitter/hva-gjor-vi-nar-gps-en-svikter/315512

eSam. (2018). *Rättsligt uttalande om röjande och molntjänster.* Stockholm: eSam.

Fjellvik, E., & Christensen, S. (2013). Oljearbeidere bekymret over fjernstyring. *FriFagbevegelse*. Hentet fra https://frifagbevegelse.no/article-6.158.31177.b08deaa774

Holte-utvalget. (2018). *IKT-sikkerhet i alle ledd.* Oslo: Justis- og beredskapsdepartementet.

ITZBund. (2017). Leistungsbeschreibung: Software und Dienstleistungen für die Bundescloud. Bonn: ITZBund. Hentet fra https://www.itzbund.de/Restricted/DE/Ausschreibungen/O1912-Z4-1519-2017/Leistungsbeschreibung.pdf?__blob=publicationFile&v=2

Kommunal- og moderniseringsdepartementet. (2016). *Nasjonal strategi for bruk av skytjenester.* Oslo: Kommunal- og moderniseringsdepartementet. Hentet fra https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/nasjonal_strategi_for_bruk_av_skytenester.pdf

La direction interninisterielle du numerique. (2018). *Le gouvernement annonce sa stratégie en matière de cloud*. Hentet fra https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-en-matiere-de-cloud/

Lysne-utvalget. (2015). *Digital sårbarhet - sikkert samfunn (NOU 2015: 13).* Oslo: Justis- og beredskapsdepartementet.

Malmqvist, M. (2019a). Myndigheterna fast i molnlimbo. *ComputerSweden*. Hentet fra https://computersweden.idg.se/2.2683/1.715718/myndigheter-moln-ta-sig-vidare

Malmqvist, M. (2019b). Statens servicecenter: "Statlig molntjänst kan spara 850 miljoner varje år". *ComputerSweden*. Hentet fra https://computersweden.idg.se/2.2683/1.715401/statlig-molntjanst-850miljoner

Nasjonal kommunikasjonsmyndighet. (2019a). 86 prosent har tilgang til bredbånd med høy hastighet. *Nasjonal kommunikasjonsmyndighet*. Hentet fra https://www.nkom.no/aktuelt/86-prosent-har-tilgang-til-bredband-med-hoy-hastighet

Nasjonal kommunikasjonsmyndighet. (2019b). *Tilgang til mobildata i Norge ved årsskiftet 2018/19*. Hentet fra Ekomstatistikken: https://ekomstatistikken.nkom.no/#/article/mobildekning_2018

Nasjonal sikkerhetsmyndighet. (2018). *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting.* Kolsås: Nasjonal sikkerhetsmyndighet. Hentet fra https://www.nsm.stat.no/globalassets/dokumenter/temahefter/tjenesteutsetting2018v1.1_web.pdf

Nasjonal sikkerhetsmyndighet. (2020). *RISIKO 2020.* Kolsås: Nasjonal sikkerhetsmyndighet.

NHO. (2019). *Anbefalte tiltak mot datakriminalitet og cyberangrep*. Hentet fra NHO: https://arbinn.nho.no/hms/sikkerhet-og-beredskap/digital-sikkerhet-og-datakriminalitet/anbefalte-it-sikkerhetstiltak/

NVE. (2017). *Selskapsmessig og funksjonelt skille*. Hentet fra https://www.nve.no/reguleringsmyndigheten/sluttbrukermarkedet/selskapsmessig-og-funksjonelt-skille/

Næringslivets sikkerhetsråd. (2018). *Mørketallsundersøkelsen 2018: Informasjonssikkerhet, personvern og datakriminalitet.* Oslo: Næringslivets sikkerhetsråd. Hentet fra https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketallsunders%C3%B8kelsen%202018%20low.pdf

Oslo Economics. (2015). *Konsekvensutredning - Alternativer for styrket robusthet i landsdekkende kjernenett.* Oslo: Oslo Economics.

Oslo Economics. (2019). *Evaluering av Norges deltakelse i EUs romprogrammer.* Oslo: Oslo Economics.

Persen, K. (2017). *To uker etter at norske fly ble rammet av GPS-svikt, dundret denne 200 meter lange masten i bakken på Jan Mayen*. Hentet fra TV2: https://www.tv2.no/a/9414718

Remen, A., & Tomter, L. (2017). Driftet Nødnettet ulovlig fra India. *NRK*. Hentet fra https://www.nrk.no/norge/driftet-nodnettet-ulovlig-fra-india-1.13358591

Remen, A., & Tomter, L. (2018). Broadnet får 14 millioner i bot. *NRK*. Hentet fra https://www.nrk.no/norge/broadnet-far-14-millioner-i-bot-1.13901965

Statens servicecenter. (2017). *En gemensam statlig molntjänst för myndigheternas it-drift.* Gävle: Statens servicecenter. Hentet fra https://www.statenssc.se/omstatensservicecenter/publikationer/rapporter/arkiv/engemensamstatligmolntjanstformyndigheternasitdrift.2106.html

Statsministerens kontor. (2020). *Meld. St. 12 (2019-2020): Anmodnings og utredningsvedtak i stortingssesjonen 2018-2019.* Oslo: Statsministerens kontor.

Store norske leksikon. (2019). *Loran-C*. Hentet fra snl.no: https://snl.no/Loran-C

Stortinget. (2018). *Møte fredag den 16. mars 2018.* Oslo: Stortinget. Hentet fra https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Referater/Stortinget/2017-2018/refs-201718-03-16?m=2

Storvik, A. (2018). IKT-skandalen: Helse Sør-Øst bryter milliardkontrakt og kansellerer gigantprosjekt. *Dagens Medisin*. Hentet fra https://www.dagensmedisin.no/artikler/2018/062/14/ikt-skandalen-helse-sor-ost-bryter-milliardkontrakt-og-kansellerer-gigantprosjekt/

Tankesmien Agenda. (2019). *Fra Skiensmodell til Oslomodell for hele landet.* Oslo: Tankesmien Agenda. Hentet fra https://tankesmienagenda.no/uploads/documents/post/Webklar-Fra-Skiensmodell-til-Oslomodell-for-hele-landet.pdf

US Department of Homeland Security. (2020). *Report on Positioning, Navigation and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS).* Washington DC: US Department of Homeland Security. Hentet fra https://www.cisa.gov/sites/default/files/publications/report-on-pnt-backup-complementary-capabilities-to-gps_508.pdf

US Department of Justice. (2020). *The Purpose and Impact of the CLOUD Act.* Washington DC: US Department of Justice. Hentet fra https://www.justice.gov/dag/page/file/1153466/download

[i] Nasjonal sikkerhetsmyndighet (2020)
[ii] Lysne-utvalget (2015)
[iii] Direktoratet for samfunnssikkerhet og beredskap (2019)
[iv] Lysne-utvalget (2015)
[v] Ibid.
[vi] Fjellvik & Christensen (2013)
[vii] Lysne-utvalget (2015)
[viii] Holte-utvalget (2018)
[ix] Remen & Tomter (2017)
[x] Remen & Tomter (2018)
[xi] Storvik (Storvik, 2018)
[xii] Lysne-utvalget (2015)
[xiii] Nasjonal sikkerhetsmyndighet (2020)
[xiv] Næringslivets sikkerhetsråd (2018)
[xv] NHO (2019)
[xvi] Kommunal- og moderniseringsdepartementet (2016)
[xvii] Ibid.
[xviii] Nasjonal sikkerhetsmyndighet (2020)
[xix] ITZBund (2017)
[xx] La direction interministerielle du numerique (2018)
[xxi] Statens servicecenter (2017)
[xxii] Malmqvist (2019a)
[xxiii] Malmqvist (2019b)
[xxiv] US Department of Justice (2020)
[xxv] eSam (2018)
[xxvi] Dom fra 16. juli 2020, *Schrems II,* C-311/18, EU:C:2020:559 (Den europeiske unions domsstol, 2020)
[xxvii] Schrems-dommene behandler saken hvor den østerrikske personvernaktivisten Max Schrems krevde at det irske datatilsynet skulle stoppe overføringer av personopplysninger mellom Facebook Irland og Facebook Inc. i USA. Han begrunnet dette med at personopplysningene hans ikke var godt nok beskyttet i USA. Dommene dreide seg altså om hvorvidt Facebook kan lagre data om europeiske borgere utenfor EU. Generelt dreide de seg om forholdet mellom europeisk personvern og amerikanske overvåkingslover når personopplysninger blir overført fra Europa til USA. Hva Schrems II-dommen har å si for andre samfunnsområder, utover Facebook, er uklart.
[xxviii] Tankesmien Agenda (2019)
[xxix] Holte-utvalget (2018)
[xxx] Nasjonal sikkerhetsmyndighet (2018)
[xxxi] Lysne-utvalget (2015)
[xxxii] Oslo Economics (Oslo Economics, 2015)
[xxxiii] Statsministerens kontor (2020)
[xxxiv] Nasjonal kommunikasjonsmyndighet (2019a)
[xxxv] Nasjonal kommunikasjonsmyndighet (2019b)
[xxxvi] Stortinget (2018)
[xxxvii] NVE (2017)
[xxxviii] Ellingsen (2017)
[xxxix] Persen (2017)
[xl] Store norske leksikon (2019)
[xli] US Department of Homeland Security (2020)
[xlii] Oslo Economics (2019)