Thomas Nergård Pettersen & André Fjellstad Morken

Fremtiden er nå.

En analyse av hvordan endringer i nasjonale trusselvurderinger påvirker departementenes styring av IKT-sikkerhet i underliggende virksomheter.

Masteroppgave i MSL5900-1 23H

OsloMet – storbyuniversitetet

Handelshøyskolen

Fakultet for samfunnsvitenskap

OSLO METROPOLITAN UNIVERSITY
STORBYUNIVERSITETET

Forord

Med en felles interesse for samfunnssikkerhet og beredskap har det ikke vært noen tvil om hva som skulle være tema for vår masteroppgave. Der risikoen for å bli utsatt for terrorisme og organisert kriminalitet fortsatt er en reell bekymring, har utviklingen av teknologi og avhengigheten av internett gjort oss sårbare for nye typer trusler, spesielt i cyberdomenet.

Norge er et av verdens mest digitaliserte samfunn, og graden av elektronisk samhandling og informasjon som deles over internett øker. I en tid hvor trusler i cyberdomenet medfører utfordringer for samfunnssikkerheten, fremstår det som essensielt å skape kunnskap om, og forståelse av hvordan samfunnet skal respondere på slike trusler.

I løpet av studiet og arbeidet med denne masteroppgaven har vi lært mer enn vi hadde forventet. Det er med en veldig god følelse at vi kan si at vi sitter igjen med en økt forståelse av hvordan samfunnet vårt styres og er bygd opp etter dette arbeidet.

Å ta et masterstudium på deltid ved siden av 100 % jobb, tilfang av totalt tre (snart fire) nye samfunnsborgere og tilhørende lite søvn har vært krevende. Uten Silje og Cecilie hadde rett og slett ikke dette blitt noe av - tusen takk for at dere har stilt opp for oss i denne perioden.

I tillegg vil vi rette en stor takk til veileder Ingvild Reymert for konstruktive tilbakemeldinger og råd på veien mot målet.

I en stadig mer kompleks verden håper vi dette kan være et bidrag inn i fremtidige refleksjoner rundt samfunnssikkerhet, beredskap og styring.

"Det vil helst gå godt" - Max Manus.

Oslo, 29. november 2023

Thomas Nergård Pettersen & André Fjellstad Morken

Sammendrag

Cyberdomenets kompleksitet og stadige utvikling stiller krav til relevant og adekvat styring. Økt digitalisering medfører strengere krav til, og bevissthet omkring IKT-sikkerhet. Til tross for at Norge er et av verdens mest digitaliserte land er ledende eksperter og fagmyndigheter kritiske til hvorvidt norske myndigheter er i stand til å ta inn over seg de trusler og utfordringer økt digitalisering representerer. Oppgaven er derfor todelt, a) dokumentere utvikling i nasjonalt trusselbilde med fokus på cybertrusselen over en periode på 13 år, og b) dokumentere hvordan departementers styring av underliggende virksomheter har utviklet seg i samme tidsrom.

Oppgaven har til hensikt å undersøke hvorvidt det foreligger en korrelasjon, eller mangel på sådan, mellom utviklingen i det nasjonale trusselbildet, og styringsutøvelse i det politisk – administrative system, med et eksplisitt fokus på styring relevant for IKT-sikkerhet og cyberdomenet. Et av formålene med oppgaven har vært å avdekke hvorvidt kritikken mot styringsutøvelsen er berettiget, eller om det kan tenkes å være relevante nyanser som bør gis nærmere oppmerksomhet. Videre har oppgaven til hensikt å undersøke hvilken styringsutøvelse som gjør seg gjeldene når det dreier seg om styring av IKT-sikkerhet og øvrige utfordringer som cyberdomenet representerer - hvorvidt styringen kan karakteriseres som detaljstyrende eller ikke, samt om det har vært en endring i denne styringsutøvelsen i det aktualiserte tidsrommet.

I analysearbeidet har vi tatt i bruk dokumentanalyse som forskningsdesign, og datainnsamlingen har bestått av å analysere årlige nasjonale trusselvurderinger utgitt av etterretnings- og sikkerhetsmyndighetene; Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og Etterretningstjenesten, samt analyse av årlige tildelingsbrev utarbeidet av Helse- og omsorgsdepartementet til Folkehelseinstituttet og Olje- og energidepartementet til Norges vassdrags- og energidirektorat. Analysen er gjennomført med utgangspunkt i fastsatte koder, og avgrenset til å gjelde for tidsperioden 2011-2023.

Av interessante funn avdekker oppgaven at det foreligger et økt fokus på trusler i cyberdomenet i de nasjonale trusselvurderingene. Videre antyder oppgaven at departementenes styring relatert til IKT-sikkerhet er noe ulik, men at den i all hovedsak bærer preg av en forskyvning fra målstyring til aktivitetsstyring innenfor den undersøkte tidsperioden. Overordnet belyses det en korrelasjon mellom utviklingen i det nasjonale trusselbilde og departementenes styring av IKT-sikkerhet.

Abstrackt

Complexity and constant progress of the cyber domain imposes strict demands for relevant and adequate governance. Increased digitalisation results in stricter demands to, and awareness of ICT security. Despite Norway being one of the world's most digitally advanced countries, leading experts and authorities are critical as to whether Norwegian governments are capable of fully understanding the threats and challenges posed by increased digitalisation. This thesis, therefore, consists of two parts, a) documenting the development of the national threat landscape with a focus on the cyber threat, and b) documenting how departmental control of subordinate entities has evolved in the same time frame.

The intent of the thesis is to explore whether there is a correlation, or lack thereof, between the development of the national threat landscape, and exercise of governance is in the political-administrative system, with an explicit focus on governance relevant for ICT security and the cyber domain. One purpose of this paper has been to unveil whether the criticism of exercise of governance is justified, or if there appears to be more relevant nuances that warrant further attention. Furthermore, the paper aims to uncover which governance practices are applied in managing ICT security and other challenges of the cyber domain – whether the governance practices can be characterised as detail oriented or not, and if there has been a change in these practices throughout the investigated time frame.

In our analytical work, we have employed document analysis as our research design, and data collection has consisted of analysing yearly national threat assessments published by the intelligence and security authorities; the Norwegian Police Security Service (PST), the Norwegian National Security Authority (NSM) and the Norwegian Intelligence Service, as well as analysis of annual allocation letters written by the Ministry of Health and Care Services to the Norwegian Institute of Public Health, and the Ministry of Petroleum and Energy to the Norwegian Water Resources and Energy Directorate. The analysis is conducted based on predetermined codes and limited to the period of time 2011-2023.

Of interesting finds, the thesis uncovers an increased focus on threat in the cyber domain in the national threat assessments. Furthermore, the thesis implies that the departments' governance related to ICT security is somewhat varied, but it displays a general shift from goal-based to activity-based management within the examined time period. Overall, a correlation between the development of the national threat landscape and the departments' governance of ICT security.

Innholdsfortegnelse

1 Innledning

1.1 Valg av tema

Norge er et av de aller mest digitaliserte samfunnene i Europa, og ifølge Europakommisjonens årlige digitaliseringsindeks lå Norge på en femte plass i 2022 (European Commission, 2022, s. 3). I løpet av 2022 brukte 99 % av alle nordmenn mellom 16 og 79 år internett. Av de under 54 år benyttet så godt som alle seg av internett daglig (Statistisk sentralbyrå [SSB], 2022).

Samtidig som digitaliseringen gir Norge store fordeler i form av en mer effektiv ressursbruk både for private og offentlige virksomheter, gjør den digitale avhengigheten oss mer sårbare. Stadig flere verdier av betydning for nasjonal sikkerhet forvaltes og behandles i det digitale rom. Blant annet er Norge avhengig av at ulike kritiske samfunnsfunksjoner som understøttes av forskjellige digitale systemer, til enhver tid fungerer (Departementene, 2019, s. 15).

At risikobildet er reelt, viser flere cyberangrep[1] mot norske virksomheter de siste årene. Ifølge Næringslivets Hovedorganisasjon har over 55 % av alle norske virksomheter vært rammet av cyberangrep (Næringslivets Hovedorganisasjon [NHO], 2022, avsn. 1). Og ifølge Direktoratet for samfunnssikkerhet og beredskap skjer digitale angrep av ulike slag og ulik alvorlighetsgrad kontinuerlig, og utgjør derfor en økende trussel mot samfunnssikkerheten (Direktoratet for samfunnssikkerhet og beredskap [DSB] , 2019, s. 197).

Angrep, trusler og ondsinnede handlinger i cyberdomenet, setter alt i fra små og store virksomheter, til samfunnet som helhet på store prøvelser. Felles for cyberangrepene er at disse kan lamme viktige norske interesser og/eller avhengigheter, og at det kan være svært ressurskrevende å gjenopprette de eventuelle skadene som oppstår.

Flere ledende eksperter og fagmyndigheter er kritiske til hvorvidt norske myndigheter er i stand til å ta inn over seg de trusler og utfordringer økt digitalisering representerer. I Nasjonal sikkerhetsmyndighet sin pressemelding i forbindelse med publiseringen av deres trusselvurdering for 2022 skriver de at cyberangrep mot virksomheter i verste fall kan få konsekvenser for Norges nasjonale sikkerhet, og at vi for å styrke sikkerheten trenger et betydelig løft i bevissthet og kompetanse om trusselbildet og sikkerhetsarbeidet, fra «øverste ledelse til den enkelte ansatte» (Nasjonal sikkerhetsmyndighet [NSM], 2022a, avsn. 4 og 6).

[1] I oppgaven benyttes cyberangrep, IKT-angrep, nettverksoperasjon, datanettverksoperasjon, datainnbrudd og datatyveri om det samme: digitale angrep mot virksomheter som skjer via ulike datasystemer og/eller internett.

Samtidig ble direktør for NSM, Sofie Nystrøm, sitert på at «norske virksomheter ikke tar denne situasjonen nok på alvor» (NSM, 2022a, avsn. 1).

Videre har både Riksrevisjonen og Totalberedskapskommisjonen levert rapporter i løpet av 2023 hvor det pekes eksplisitt på viktigheten av å prioritere den digitale sikkerheten. Riksrevisjonen retter i sin rapport tydelig kritikk mot myndighetenes arbeid med digital sikkerhet, og gir uttrykk for at manglende og dårlig sikkerhetsarbeid kan få alvorlige konsekvenser for ulike kritiske samfunnsfunksjoner (Riksrevisjonen, 2023, s. 9). Totalberedskapskommisjonen leverte, på oppdrag fra regjeringen, sin rapport den 5. juni 2023 hvor de har vurdert hvordan samfunnets samlede beredskapsressurser kan benyttes best mulig i fremtiden. Totalt presenterte kommisjonen ti hovedanbefalinger hvorav ett av punktene er å «forsterke arbeidet med infrastruktur og digital sikkerhet» (NOU 2023: 17, s. 27). I tillegg pekte kommisjonen på viktigheten av at krav til risikostyring relatert til digital sikkerhet følges opp i virksomheter, og at Justis- og beredskapsdepartementet i kraft av sitt samordningsansvar stiller tydelige krav til øvrige departementers oppfølging av dette innenfor egen sektor, blant annet gjennom styring av underliggende virksomheter (NOU 2023: 17, s. 313).

I Norge preges offentlig styring av å være hierarkisk ved at «øverste ledelse», i dette tilfellet departementene, delegerer oppgaver til underliggende virksomheter gjennom styring. Begrepet *styring* kan defineres som «lederskapets forsøk på å fatte kollektive beslutninger og påvirke atferd gjennom et sett eller system av formelle styringsinstrumenter» (Christensen et al., 2015, s. 123), og beskrives av Byrkjeflot (1997, s. 14) som en prosess eller handling som dreier seg om å sette retning.

Som øverste myndighet er departementene ansvarlige for samfunnssikkerheten. Dette innebærer et ansvar for ivaretakelse av innbyggernes liv og helse, grunnleggende behov, samt opprettholdelse av viktige samfunnsfunksjoner. Justis- og beredskapsdepartementet har samordningsansvar for digital sikkerhet på sivil side, og gir myndighetene nasjonale råd og anbefalinger (Stortingsmelding [St.meld.] nr. 9 (2022-2023), s. 12). Samtidig er øvrige departementer ansvarlige for samfunnssikkerheten (inkludert digital sikkerhet) innenfor egen sektor (Samfunnssikkerhetsinstruksen, 2017). Dette er et ansvar som stiller krav til en styringsutøvelse som tar denne tematikken på alvor.

Til tross for et økt søkelys på digitalisering, finner vi lite informasjon og norsk forskning som konkret ser på utviklingen i det nasjonale trusselbildet med fokus på cybertrusselen, og

departementers eventuelle styring i tilknytning til dette. Forskningslitteraturen inneholder mange eksempler hvor man har sett på norske forhold, og departementers styring, herunder departementers styring innenfor samfunnssikkerhetsfeltet *i stort*. På bakgrunn av dette er det interessant å se mer detaljert på hvordan utviklingen i det nasjonale trusselbildet, herunder hvordan et mulig økt fokus på trusler i cyberdomenet påvirker departementenes styring. I denne oppgaven vil vi derfor analysere hvorvidt det er en sammenheng mellom endringer i det nasjonale trusselbildet og departementenes styring av underliggende virksomheter i et IKT-sikkerhetsperspektiv.

1.2 Problemstilling

I denne oppgaven fremmer vi følgende problemstilling:

Hvordan påvirker nasjonalt trusselbilde departementenes styring av samfunnssikkerhet?

Konkret vil vi analysere hvordan endringer i nasjonale trusselvurderinger påvirker den politiske styringsdialogen med underliggende virksomheter gjennom formidling av mål, styringsparameter og aktivitetskrav i årlige tildelingsbrev.

1.3 Oppgavens formål, omfang og struktur

Innledningsvis i oppgaven er det gjort en innramming og kontekstualisering av oppgavens problemstilling. I kapittel 2 blir det redegjort for det teoretiske rammeverket oppgaven legger til grunn, og oppgavens hypoteser. I kapittel 3 presenteres den vitenskapelige metoden. Da det benyttes dokumentstudier redegjøres det for valg av forskningsobjekter, hvilke dokumenter som blir analysert og hvordan disse har blitt kodet, samt datakvaliteten ved det som blir presentert.

I kapittel 4 redegjør vi for de faktiske funnene som er gjort, og visualiserer disse ved bruk av ulike figurer. Videre drøfter og analyserer vi funnene opp mot det teoretiske rammeverket i kapittel 5. I kapittel 6 fremmer vi våre hovedfunn, samt konkluderer opp imot oppgavens problemstilling. Helt avslutningsvis blir oppgavens begrensninger og tilhørende forslag til videre forskning kort presentert.

2 Teori

Oppgavens problemstilling har til hensikt å undersøke hvorvidt nasjonalt trusselbilde påvirker departementenes styring av samfunnssikkerhet. I den forbindelse er det flere teoretiske perspektiver om styring og styringsutøvelse som er relevant å se nærmere på.

2.1 Styring

Thomas Dye (1972) beskriver politikk som "det myndighetene velger å gjøre, samt det de velger å ikke gjøre» (henvist i Howlett, 2011, s. 15). Styring er derfor en kjerneoppgave i all politisk virksomhet, og både politikere og byråkrater jobber kontinuerlig med oppgaver som innbefatter styring. Ifølge Mulgan (2009) har offentlig strategisk styring stor påvirkning på folks liv, blant annet gjennom sitt potensiale til å påvirke og forhindre kriminalitet (henvist i Johnsen, 2014, s. 274). I en slik kontekst er det derfor interessant å analysere hvorvidt et endret trusselbilde påvirker den politiske styringsdialogen med underliggende virksomheter eller ikke.

Hva gjelder styring av offentlig sektor har den vestlige verden etter andre verdenskrig vært preget av tre ulike styringsparadigmer. Det være seg tradisjonell offentlig styring, ny offentlig styring og ny offentlig samstyring. Tradisjonell offentlig styring var i stor grad basert på hierarkisk og sentralisert regel- og retningsgivende styring. Ny offentlig styring er en markedsinspirert og desentralisert styring hvor produksjon og resultat er i fokus. Når det gjelder ny offentlig samstyring fokuserer denne blant annet på samarbeid mellom offentlige og ikke offentlige aktører hvis intensjon er å løse felles utfordringer (Røiseland & Vabo, 2016, ss. 18-21). Ettersom departemental styring per i dag i stor grad er forenelig med de prinsipper og den tilnærming til styring som man ser i ny offentlig styring som styringsprinsipp (Johnsen, 2007, s. 88), er dette den styringsformen som vil vies oppmerksomhet videre i oppgaven.

På 1990 tallet aktualiserte ny offentlig styring seg ved at man oppmuntret til omfattende spesialisering og desentralisering av virksomheter med intensjon om at ivaretagelsen av komplekse oppgaver og utfordringer ville bedres dersom det ble utført av selvstendige og delvis uavhengige enheter/virksomheter (Hood, 1991, s. 5). Som del av ny offentlig styring ble mål- og resultatstyring innført som obligatorisk for alle statlige virksomheter i 1990 (Johnsen, 2015, s. 36). Mål- og resultatstyring defineres som en metode som «handler om å sette mål, følge opp om målene nås, og bruke informasjonen til læring, styring og kontroll» (Direktoratet for forvaltning og økonomistyring [DFØ], 2023a, avsn. 2).

Det er departementene, med en statsråd som øverste ansvarlig, som har ansvaret for å fastsette og følge opp om målene nås, og bruke denne informasjonen til læring, *styring* og kontroll. Ifølge Kunnskapssektorens tjenesteleverandør, Sikt, er det per juni 2023, 16 departementer og 171 statlige underliggende virksomheter i Norge (Sikt, 2023). Disse underliggende virksomhetene er formelt sett underlagt et departement, med varierende grad av autonomi når det gjelder utøvelse av oppgaver. En slik organisering representerer en systemutforming som defineres som et politisk-administrativt system, hvor intensjonen er at politikere utformer strategi og mål på den ene siden, mens det på den andre siden er administrasjonen og forvaltningen (ikke folkevalgte) som har ansvaret for resultatet, og dermed de samfunnsmessige effekter som kommer til uttrykk gjennom oppnådd (eller fravær av) resultat (Christensen et al., 2015, s. 100).

For at departementene skal kunne styre har de instruksjonsmyndighet overfor underliggende virksomheter (DFØ, 2020, kap. 1.3), hvilket medfører et *hierarkisk* forhold partene imellom. I slike hierarkiske relasjoner antas det ofte at det vil kunne oppstå avvikende interesser mellom under- og overordnet (Bjurstrøm, 2021, s. 3). Det er derfor naturlig å se hen til *prinsipal- agent teori og forvalterteori*, og *delegeringsproblemet* som kan oppstå når samhandling utøves i hierarkiske relasjoner.

2.2 Prinsipal- agentteori og forvalterteori

Et departement (prinsipal) har som nevnt instruksjonsmyndighet overfor underliggende virksomhet (agent) (Røiseland & Vabo, 2016, s. 122). I kraft av at etatsstyring er en kompleks og krevende oppgave stilles det derfor strenge krav til balansegangen mellom underliggende virksomheters behov for autonomi på den ene siden og behovet for politisk kontroll på den andre (Christensen & Lægreid, 2007, ss. 517-518). I tråd med agentteori kan delelegeringsproblem oppstå når agenten ikke handler i tråd med prinsipalens intensjon (Eisenhardt, 1989, s. 58). Prinsipalen har som øverste myndighetsorgan ansvar for blant annet at politikk iverksettes, og bruker agenten til dette, hvilket gjør prinsipalen avhengig av agenten.

For å unngå at det oppstår delegeringsproblemer kan både prinsipal og agent benytte ulike virkemidler. Røiseland og Vabo (2016, s. 93) trekker blant annet kontroll frem som et virkemiddel som prinsipalen kan benytte. Når det er sagt foreligger det kritikk av agentteorien ved at den presenterer et forholdsvis negativt syn på relasjonen mellom over og underliggende myndighet (Maggetti & Papadopoulos, 2016; Pierre & Peters, 2017; Schillemans & Busuioc,

2015, referert i Bjurstrøm, 2020, s. 14). En tilnærming og forståelse som har ført til utviklingen av det som på norsk omtales som *forvalterteori*, og som representerer et mer positivt syn i relasjonen mellom over og underliggende myndighet.

Forvalterteori legger til grunn at det stort sett er overenskomst mellom agent og prinsipal hvor man har et samarbeid preget av lik forståelse av hva som er gjeldene målsetning. Forvalterteori legger til grunn samme politiske- administrative system som i agentteorien med en overordnet og en underordnet, men hvor man i større grad har tillit til at utøvende part representert ved den underliggende virksomhet handler utlukkende med gode intensjoner. Ifølge Olsen (2015) er dette et resultat av hvordan *institusjonelle omgivelser og normer* hindrer opportunistisk atferd hos den underliggende virksomheten, og snarere stimulerer til at den ønsker å fremstå som en lojal forvalter som handler i den overordnedes beste interesser (referert i Bjurstrøm, 2021, s. 4).

Ved å innta en holdning til at begge teorier kan komme til uttrykk vil man i større grad kunne tilpasse hvorvidt man i styringsutøvelsen fokuserer på kontrollregime eller ikke (Davis et al., 1997, ss. 39-40). Både agent- og forvalterteori stiller krav til hvordan overordnet myndighet strukturerer og utøver sin kontrollvirksomhet, utforming av kontrakter og ulike incentiv og sanksjonsordninger for at agenten eller forvalter skal handle i tråd med prinsipalens ønske (Bjurstrøm, 2020, s. 12).

Ved å legge til grunn agent- og forvalterteori som en måte å forstå kompleksitet i hierarkisk styring og behovet for god vekting mellom kontroll og handlingsrom/autonomi er det avgjørende med gode styringsincentiver og metoder. Et mulig delgeringsproblem som kan oppstå mellom departement og underliggende virksomhet forsøkes løst med mål- og resultatstyring hvor det som tidligere nevnt vises til departementenes ansvar for å sette mål, følge opp om målene nås, og bruke denne informasjonen til læring, *styring* og kontroll.

2.3 Nærmere om mål- og resultatstyring

Økonomiregelverket pålegger departementene å fastsette overordnede mål og styringsparameter for å kunne vurdere resultater og måloppnåelse (DFØ, 2023a, avsn. 2). Ifølge Christensen et al. (2015, s. 111) har mål- og resultatstyring som intensjon å sørge for at målsetninger aktivt benyttes og stimulerer til operasjonell drift av offentlige virksomheter. Dette slik at man skaper forutsetninger for økt effektivitet og bedre utnyttelse av kompetanse, samtidig som man forenkler og skaper mer transparens omkring forventning og resultat som

forbedrer evalueringsprosessene. I tillegg til mål- og resultatstyring kan departementer ved behov benytte andre styringsformer parallelt. Eksempler på slike er budsjettstyring, regelstyring og aktivitets- og oppgavestyring (DFØ, 2023b, kap. 3 & 4).

Budsjettstyringen knyttes som regel sammen med mål- og resultatstyring ved at mål- og resultatstyring dokumenterer hva som er målet og virkningen av en bevilgning. Et slikt samspill krever i følge DFØ (2023b, kap. 3, 3. avsnitt) at styringen understøtter prioriteringer som følger av fastsatte mål. Samtidig trekker Johnsen (2007, s. 106) frem at færre øremerkede midler vil være en måte å redusere føringene på, og dermed detaljstyringen.

Regelstyring er styring basert på krav som kommer frem av blant annet lover som setter rammer for virksomhetene (DFØ, 2023b, kap. 4, 2. avsnitt). Når det gjelder aktivitets- og oppgavestyring innebærer dette at departementet stiller krav til hvilke aktiviteter og oppgaver som skal gjennomføres, og kan ved behov benyttes som en del av mål- og resultatstyringen der det blant annet er behov for å konkretisere spesifikke oppgaver og/eller aktiviteter. Om denne styringen kobles til overordnede mål vil målene fortsatt være retningsgivende for utførelsen av oppgaver i de underliggende virksomhetene. Derimot vil man ved bruk av aktivitetsstyring som ikke er koblet til overordnede mål risikere at disse oppgavene/aktivitetene begrenser underliggende virksomhets mulighet til å prioritere og velge virkemidler som bidrar til måloppnåelse (DFØ, 2023b, kap. 4, 8. avsnitt).

Til tross for at mål- og resultatstyring er en foretrukken og obligatorisk styringsmetode i staten er den ikke fullstendig fri for kritikk. I artikkelen *"for mye detaljstyring, og for lite målstyring"* trekker Johnsen (2015, s. 36) frem at mål- og resultatstyring i perioden etter 2010 har vært gjenstand for kritikk som følge av at den har tendert mot å være for detaljstyrende og for lite opptatt av resultat.

De senere år er det gjort flere analyser tilknyttet mål- og resultatstyring, og departementers styring av underliggende virksomheter i stort. I 2015 ble det blant annet foretatt en analyse av utvikling i detaljstyringen fra 2012-2015 hvor man fant at det hadde vært en viss nedgang i antall mål, styringskrav og aktivitetskrav, og at styringen derfor fremstod mindre detaljorientert (Kjærvik & Askim, 2015, s. 16). Derimot viser Kommunal- og moderniseringsdepartementet (2020, s. 18), i en oppdatert rapport, utarbeidet på bakgrunn av- og med utgangspunkt i Kjærvik & Askim sin rapport fra 2015 at detaljstyring i flere år har vært, og er omfattende, i statlig styring. Dette til tross for at det foreligger et konkret ønske om å redusere den detaljorienterte

styringen (Kommunal- og moderniseringsdepartementet, 2018, s. 2). Kommunal- og moderniseringsdepartementet (2020, s. 16) trekker kompleksitet frem som en mulig årsak på hvorfor det er slik.

Kompleksitet, og komplekse problemstillinger, er også en faktor som Christensen et al. (2015, s. 111) trekker frem som vesentlig ved å vise til en verden i stadig utvikling, noe som fører til at det stilles strenge krav til målformulering. I den forbindelse kan det stilles spørsmålstegn ved om det i det hele tatt er mulig å definere tilstrekkelig konkrete målsetninger på komplekse problemstillinger. På bakgrunn av den åpenbare kompleksiteten som ligger i utviklingen i- og det å skulle gardere seg mot trusler i cyberdomenet fremmes følgende hypotese:

> *Hypotese 1 A: Kompleksitet og utvikling i cyberdomenet preger styringsutøvelsen og bidrar til økt grad av detaljstyring relatert til IKT-sikkerhet.*

Samtidig vil en alternativ hypotese være at man på bakgrunn av kritikken mot mål- og resultatstyring og dens fokus på for mye detaljstyring i perioden etter 2010 ser at konkrete krav knyttet til IKT-sikkerhet er få eller helt fraværende jo nærmere vi kommer dags dato. På bakgrunn av dette fremmes følgende hypotese som et alternativ til hypotese 1 A:

> *Hypotese 1 B: Kritikken av departementenes detaljstyring i perioden etter 2010 preger styringsutøvelsen og gjør seg gjeldende gjennom færre krav knyttet til IKT-sikkerhet jo nærmere vi kommer dags dato.*

Når det gjelder departementenes formidling av mål- og resultatstyring til underliggende virksomheter skjer dette via ulike styringsverktøy. Dette er styringsverktøy og virkemidler som departementene tar i bruk for å utøve makt og dermed skape eller avverge endring i samfunnet (Ladegård & Vabo, 2010, s. 176). De mest sentrale styringsverktøyene på politisk nivå er lover, regler og forskrifter, i tillegg til at det som del av styringsdialogen mellom departement og underliggende virksomheter utarbeides instrukser, tildelingsbrev og årsrapporter som noen eksempler (DFØ, 2020, kap. 1.2). Av disse er det tildelingsbrevene som betraktes som den viktigste kanalen for formidling av styringssignaler (PwC, 2020, s. 29). Ifølge Åge Johnsen (2015, s. 37) kan man ved å analysere tildelingsbrevene få et mer utfyllende bilde på hvilken styring som faktisk utøves, noe som også våre analyser har til hensikt å belyse.

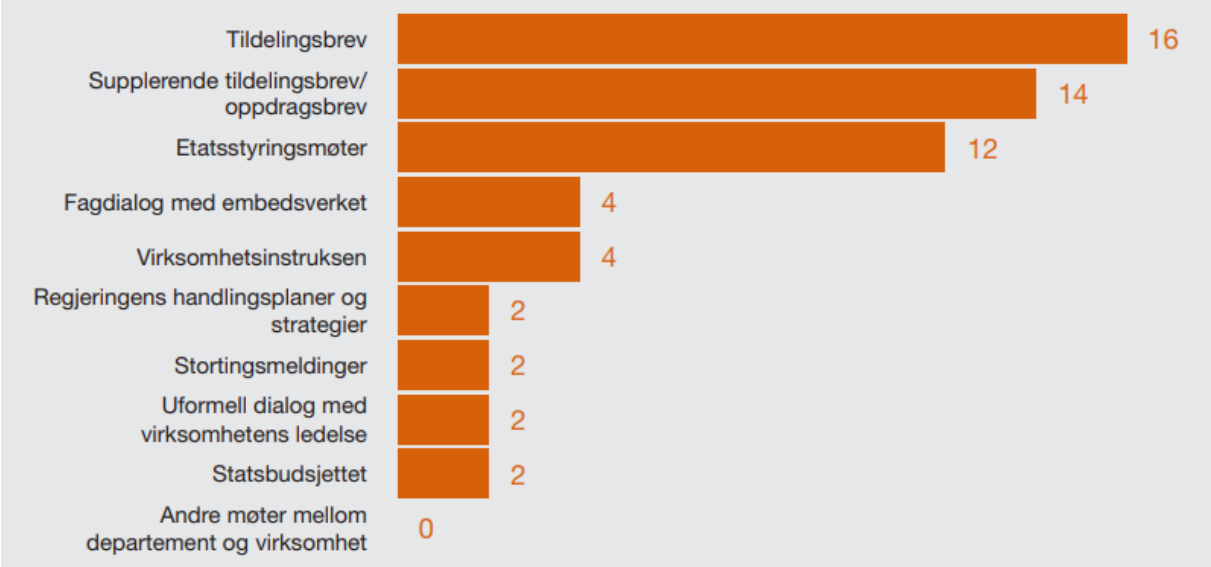
2.4 Tildelingsbrev som styringsinstrument

Tildelingsbrevets formål er å følge opp Stortingets budsjettvedtak, samt være en hovedkanal for departementenes forventninger og krav til underliggende virksomheter som oppfølging på dette for det aktuelle budsjettåret (Finansdepartementet, 2022, s. 18, § 7). Som tidligere beskrevet legger agent- og forvalterteori til grunn et behov for utforming av kontrakter og ulike incentiv slik at agenten skal handle i tråd med prinsipalens intensjon eller ønske. En slik kontrakt er nettopp det årlige tildelingsbrevet ment å være.

Videre vil virksomhetenes egenart gjøre at departementene har ulike behov knyttet til ulike styringsdokumenter, hvilket gjør at det ikke er utarbeidet en mal for hvordan tildelingsbrevet skal utformes. Dette vil potensielt medføre en del ulikheter på tvers av departementer og respektive underliggende virksomheter. Det vil med andre ord ha relevant overføringsverdi til problemstillingen om hvorvidt det er sammenheng mellom gjeldene trusselbilde relatert til cyberdomenet og den politiske styringen som utøves.

At tildelingsbrevet er viktig underbygges av en kvalitativ studie utført av PwC på oppdrag fra DFØ høsten 2020, hvor de hadde til hensikt å kartlegge og analysere departementenes etatsstyring i praksis. På spørsmål til 10 ulike departementer og 7 underliggende virksomheter om hva som er de viktigste styringskanalene pekte nesten samtlige på at tildelingsbrev er den viktigste styringskanalen (PwC, 2020, s. 29).

Figur 1 Fagavdelinger og virksomheters opplevelse av de tre viktigste kanaler for styringssignaler (PwC, 2020, s. 29)



Note. Fra *Etatsstyring i praksis (En kvalitativ studie av departementenes styring av underliggende virksomheter),* av PWC, 2020, DFØ (https://dfo.no/sites/default/files/fagomr%C3%A5der/Rapporter/2021/Etatsstyring-i-praksis-en-komparativ-studie.pdf), Copyright 2020 PWC.

Til tross for at tildelingsbrev er et viktig instrument for offentlig styring er det også gjenstand for kritikk. En kritikk som i hovedsak handler om at tildelingsbrevene i for stor grad er detaljfokusert og mindre resultatfokusert (Johnsen, 2015, s. 36).

Kommunal- og moderniseringsdepartementet (2020) analyserte som henvist til i kapittel 2.3 departementenes styring via tildelingsbrev for perioden 2012-2020. Av interessante funn i denne analysen kan det trekkes frem at man fant at det i perioden 2012-2015 var en reduksjon i antall mål, styringsparameter og aktivitetskrav. I perioden 2015 til 2020 fant man derimot en økning, men en økning som i sum var mindre enn reduksjonen som ble funnet i løpet av den foregående perioden (Kommunal- og moderniseringsdepartementet, 2020, s. 13). Når det gjelder aktivitetskrav holdt disse seg relativt stabile gjennom hele perioden og var samtidig den formen for styringsvirkemiddel som ble hyppigst brukt. Kommunal- og moderniseringsdepartementet (2020, s. 18) beskriver i sin rapport en antydning av at virksomheter som har fått redusert sine mål og styringsparametere til gjengjeld fikk et økt antall aktivitetskrav. Et tegn på en forskyvning fra mål og styringsparameter til aktivitetskrav. Rapporten slo dermed fast at ønsket om færre og tydeligere mål, tydeligere prioriteringer, men samtidig mindre detaljstyring har vist seg å ha noe effekt når det gjelder mål og

styringsparameter, men liten eller ingen effekt når det gjelder aktivitetskrav (Kommunal- og moderniseringsdepartementet, 2020, s. 7). Hvorvidt man ser tilsvarende trender eller ikke i de styringssignal som eventuelt innretter seg mot IKT-sikkerhet vil inngå som del av vår undersøkelse og analyse.

Videre fant Kjærvik & Askim (2015, s. 13) på et mer generelt grunnlag at det foreligger ulik styringspraksis avhengig av hvilken type forvaltningsorgan den underliggende virksomheten representerer. Eksempelvis så vil direktorater (ordinært forvaltningsorgan) utsettes for flere styringskrav sammenlignet med andre underliggende virksomheter. På bakgrunn av dette fremmer vi vår tredje hypotese:

> *Hypotese 2: Det foreligger en ulikhet/skjevhet i styringsutøvelsen av underliggende virksomheter i tråd med teorien om at direktorater tenderer mot å være mer detaljstyrt enn andre underliggende forvaltningsorgan.*

Med utgangspunkt i oppgavens fokus på styring relatert til IKT-sikkerhet, eksplisitt, redegjøres det under kort for myndighetenes arbeid med digital sikkerhet.

2.5 Myndighetenes arbeid med digital sikkerhet

Justis- og beredskapsdepartementet er gitt en samordningsrolle innenfor arbeidet med samfunnssikkerhet, og har i den forbindelse ansvar for nasjonal digital sikkerhet i sivil sektor. Videre fremgår det av Samfunnssikkerhetsinstruksen (2017, kap. III, nr. 1) 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». Dette kalles *ansvarsprinsippet*, og innebærer helt konkret at de ulike departementenes statsråder har et *overordnet ansvar* for å ivareta digital sikkerhet *innenfor egen sektor* (Departementene, 2019, s. 22)

Videre står det i Samfunnssikkerhetsinstruksen (2017) at arbeidet med samfunnssikkerhet skal være basert på risikostyring, og at departementene blant annet skal kunne dokumentere at de systematisk arbeider med risiko- og sårbarhetsanalyser med grunnlag i vurderinger av tilsiktede og utilsiktede hendelser som kan true departementets og sektorens funksjonsevne (kap. IV, nr. 2). Slike analyser skal blant annet ta utgangspunkt i overordnede strategiske dokumenter om risiko, trusler og sårbarhet med henvisning til følgende eksempler: «vurderinger fra Politiets

sikkerhetstjeneste [PST], Etterretningstjenesten [E-tjenesten], Nasjonal sikkerhetsmyndighet (NSM) og andre» (Samfunnssikkerhetsinstruksen, 2017, kap. IV, nr. 2, fotnote 1).

Årlig gir de nasjonale etterretnings- og sikkerhetsmyndighetene i Norge: NSM, PST og E-tjenesten, ut hver sine overordnede, ugraderte (offentlige) rapporter om nasjonalt trusselbilde. Etterretnings- og sikkerhetsmyndighetene samarbeider tett ved utarbeidelse av de ulike rapportene, men har ulike mandater og ansvarsforhold. Kort beskrevet er NSM det nasjonale fagmiljøet for forebyggende sikkerhet og bidrar til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot digitale angrep (NSM, u.d.). PST har ansvar for å samle og analysere informasjon, samt iverksette forebyggende tiltak mot forhold som kan true nasjonens sikkerhet (PST, u.d.), mens E-tjenesten er Norges utenlandsetterretningstjeneste, og skal bistå norske myndigheter med beslutningsstøtte om forhold som ligger utenfor Norges grenser (E-tjenesten, 2022).

2.6 Hendelsers påvirkning på nasjonalt trusselbilde

De årlige ugraderte trusselvurderingene fra de ulike etterretnings- og sikkerhetsmyndighetene er, som navnet tilsier, vurderinger tuftet på innhentet informasjon som videre har vært gjenstand for analyse og vurdering. De er predikative og har blant annet til hensikt å redusere usikkerheten fremtiden representerer, og omtaler i all hovedsak aktuelle trusler for det inneværende året. Pollit og Bouckaert (2017, ss. 31-32) skriver at offentlig forvaltning påvirkes av flere ulike faktorer. En av disse faktorene er «spesielle hendelser og ulykker», eksempelvis terrorhendelser og massedrap, men også naturkatastrofer, pandemier og skandaler som isolert kan være den utløsende faktoren som fører til endring (Pollitt & Bouckaert, 2017, s. 40).

I trusselvurderingene fra etterretnings- og sikkerhetsmyndighetene redegjør de for risikoer for at samfunnet skal rammes av tilsiktede (uønskede) handlinger som kan skade viktige samfunnsinteresser, enten direkte eller indirekte. Slike handlinger kan ses i sammenheng med faktorene Pollitt & Bouckaert (2017) trekker frem. Summen av omtale, fokus og eventuell kritikk er derfor å betrakte som reel påvirkningskraft som potensielt tvinger frem tiltak. Dette gjelder med andre ord også for trusler i cyberdomenet hvor vi i kapittel 1 viste at digitale angrep skjer kontinuerlig, og så ledes er en økende trussel mot samfunnssikkerheten (DSB, 2019, s. 197). På bakgrunn av den økende oppmerksomheten slike angrep får i media, og den stadige

gjentakende kritikken mot norske virksomheters evne til å beskytte seg mot slike angrep fremmes vår tredje hypotese:

> *Hypotese 3: Cyberangrep som har rammet norske virksomheter har hatt en påvirkende faktor på etterretnings- og sikkerhetsmyndighetenes fokus på dette feltet i årlige trusselvurderinger.*

Videre ser vi av Totalberedskapskommisjonens rapport, som henvist til i kapittel 1, peker på viktigheten av at etterretnings- og sikkerhetsmyndighetenes trusselvurderinger kommer til anvendelse i samfunnssikkerhets- og beredskapsarbeidet (NOU 2023: 17, s. 63). Tatt i betraktning at NSM i forbindelse med publiseringen av deres trusselvurdering for 2022 påpeker behovet for et betydelig løft i bevissthet og kompetanse rundt cybersikkerhet, samt kritiserer norske virksomheter for å ikke ta dette nok på alvor (NSM, 2022a, avsn. 1), er det interessant å undersøke hvorvidt departementene som ansvarlige for egne sektorer hensyntar denne utviklingen, og den informasjonen som kommer frem av etterretnings- og sikkerhetsmyndighetenes årlige trusselvurderinger eller ikke. På bakgrunn av NSM sin generelle kritikk av norske virksomheter fremmes derfor følgende hypotese:

> *Hypotese 4: Det er liten grad av korrelasjon mellom utviklingen i nasjonalt trusselbildet og den styringsutøvelse som kommer frem av departementenes årlige tildelingsbrev til underliggende virksomheter.*

3 Metode

3.1 Valg av forskningsdesign

Denne oppgaven søker å redegjøre for utviklingen i det nasjonale trusselbildet fra 2011 til 2023, samt finne svar på hvorvidt, og eventuelt på hvilke måter trusselbildet påvirker departementenes styring av samfunnssikkerhet i underliggende virksomheter, med fokus på styring relatert til cybertrusselen. Oppgaven er derfor todelt, a) dokumentere utvikling i trusselbildet med fokus på cybertrusselen over en periode på 13 år, og b) dokumentere hvordan departementers styring av underliggende virksomheter har utviklet seg i samme tidsrom.

Gitt oppgavens problemstilling inkludert hypoteser fremstod kvalitativ metode med utgangspunkt i dokumentstudier av de nasjonale etterretnings- og sikkerhetsmyndighetene sine årlige trusselvurderinger, samt tildelingsbrev fra Helse- og omsorgsdepartementet til Folkehelseinstituttet og fra Olje- og energidepartementet til Norges vassdrags- og energidirektorat som det beste valget da oppgaven søker å beskrive og forstå spesifikke dokumenters innhold.

3.2 Utvelgelse av departementer og underliggende virksomheter

I oppgaven har det ved flere anledninger blitt henvist til begrepet *kritiske samfunnsfunksjoner*. I henhold til Samfunnssikkerhetsinstruksen (2017, kap. VI, nr. 1, bokstav e) har Justis- og beredskapsdepartementet ansvar for å «utarbeide og vedlikeholde oversikt over hvilke funksjoner som i tverrsektorielt perspektiv er kritisk for samfunnssikkerheten». Videre har Justis- og beredskapsdepartementet pekt ut hvilke departementer som er *hovedansvarlig* for de ulike funksjonene. En av disse funksjonene er «samfunnets funksjonalitet» som blant annet består av kapabilitetene forsyningssikkerhet, vann og avløp, kraftforsyning og elektronisk kommunikasjon (DSB, 2016, ss. 10-18). Dette er kapabiliteter som befolkningen er helt avhengig av, og som ved bortfall kan medføre store konsekvenser for Norges styringsevne, suverenitet og befolkningens sikkerhet (DSB, 2016, s. 74).

Da vi har behov for å nedskalere utvalget av forskningsobjekter har vi valgt å gå videre med funksjonene *vann og avløp*, som Helse- og omsorgsdepartementet er ansvarlig[2] for, og *kraftforsyning*, som Olje- og energidepartementet er ansvarlig for.

De to departementene representerer dermed kun 2 av 16 departementer totalt, og 2 av 5 med hovedansvar innenfor «samfunnets funksjonalitet». Som følge av problemstillingens ordlyd «*departementenes styring ...*» skulle ideelt sett alle departementers tildelingsbrev til underliggende virksomheter i hele tidsperioden vært en del av datasettet. Da det som tidligere omtalt er totalt 16 departementer og 171 underliggende virksomheter per juni 2023 ville ikke dette latt seg gjøre som følge av oppgavens «rammebetingelser» (Sikt, 2023).

Direktoratet for samfunnssikkerhet og beredskap sin analyse av krisescenarioer illustrerer at alle kritiske samfunnsfunksjoner i større eller mindre grad er avhengig av kraftforsyning. Direktoratet for samfunnssikkerhet og beredskap skriver videre at konsekvensene ved bortfall kan bli store, og at det blant annet vil kunne true liv og helse og samfunnets stabilitet (DSB, 2016, s. 89). Ulikt mange andre land er over 20 prosent av boliger i Norge helt avhengige av strøm til oppvarming, hvilket kan medføre konsekvenser for befolkningen (DSB, 2019, s. 163). Når det gjelder vann og avløp, herunder drikkevannsforsyning, er evnen til å levere tilstrekkelig med drikkevann til befolkningen en grunnleggende fysiologisk forutsetning for liv. Eksempelvis er produksjon av mat og helsevesenet avhengige av tilgang på rent vann (DSB, 2016, s. 80). På bakgrunn av dette mener vi at disse to departementene er interessante å se på opp imot hvordan deres styring av henholdsvis Folkehelseinstituttet som ansvarlig for blant annet forvaltningsstøtteoppgaver (eksempelvis vannverksregisteret, analyser etc.) innenfor drikkevannsområdet (Regjeringen.no, 2021), og Norges vassdrags- og energidirektorat som ansvarlig for kraftforsyningen (NVE, 2023), gjør seg gjeldende i tilknytning til det nasjonale trusselbildets utvikling innenfor cyberdomenet.

Et tilleggsargument for å velge å se på disse underliggende virksomhetene knytter seg også til tidligere analyser hvor det har kommet frem ulik styringspraksis opp imot type forvaltningsorgan som den underliggende virksomheten representerer. Folkehelseinstituttet er et institutt og Norges vassdrags- og energidirektorat et direktorat, hvilket gjør det mulig for oss å analysere hvorvidt det foreligger en ulikhet/skjevhet i styringsutøvelsen av disse som ulike forvaltningsorganer eller ikke i samsvar med vår hypotese (hypotese 2).

[2] Ansvarlig for «9.1 Drikkevannsforsyning» (DSB, 2016).

3.3 Nærmere om utvelgelse av dokumenter, koding og analyse

Dokumentanalyse ser på dokumenter som en integrert og sentral del av samfunnets oppbygning og struktur, og setter dokumenter i en bredere kontekst, hvor de vurderes med utgangspunkt i de «prosesser, systemer, apparater og institusjoner» de er en del av (Asdal & Reinertsen, 2020, s. 16). Dokumentstudier vil med andre ord kunne besvare vår problemstilling og våre hypoteser ved å analysere dokumenter knyttet til, a) trusselbildet, og b) styring av underliggende virksomheter, og hvorvidt disse inneholder relevant informasjon, peker på utviklingstrekk, eller anbefaler/iverksetter tiltak avhengig av dette.

Videre i dette kapittelet vil vi beskrive hvordan vi har gått frem i vårt arbeid med å kode og analysere utviklingen i det nasjonale trusselbildet, og utviklingen i departementenes styring av sine underliggende virksomheter gjennom tildelingsbrev.

3.3.1 Nasjonalt trusselbilde

For å belyse utvikling og endringer i nasjonalt trusselbildet fra 2011 til 2023 med fokus på trusler i cyberdomenet blir samtlige av de årlige, overordnede og ugraderte (offentlige) rapportene utgitt av etterretnings- og sikkerhetsmyndighetene, NSM[3], PST og E-tjenesten, analysert.

I dette analysearbeidet har vi også hatt utbytte av å se på funn og analyser i masteroppgaven «Skjevt ut fra hoppkanten? Myndighetenes organisering av sikkerhet i cyberdomenet» hvor masterstudent ved Forsvarets høgskole, Ole Jørgen Arvesen, blant annet kartla «cybersikkerhet i åpne trusselvurderinger i perioden 2011 til 2020» (Arvesen, 2020, ss. 21-28).

I likhet med Arvesen (2020) vil vår analyse av nasjonalt trusselbilde bestå av en overordnet redegjørelse av det som er relatert til cybertrusselen, og i hva slags *omfang* disse truslene *beskrives* og *vies oppmerksomhet* i rapportenes *oppbygning*. Vi vil med andre ord gjøre en selvstendig analyse av sikkerhetsmyndighetenes rapporter, og trekke ut det som anses som mest interessant opp imot denne oppgavens anliggende.

Totalt er 38 trusselvurderinger for tidsperioden 2011-2023 del av denne analysen, og samtlige er hentet fra de respektive etterretnings- og sikkerhetsmyndighetenes hjemmesider: www.pst.no, www.nsm.no, og www.etterretningstjenesten.no. Fordelingen er vist i tabell 1,

[3] NSM sin rapport for 2013 er ikke del av analysen da denne ikke var tilgjengelig under vårt analysearbeid.

under. Videre er samtlige trusselvurderinger opplistet i vedlegg 1 med utgiver, dokumenttittel, utgivelsesdato, samt antall sider de består av.

Etterretnings- og sikkerhetsmyndigheter og det totale antallet trusselvurderinger	
Politiets sikkerhetstjeneste	13 totalt
Nasjonal sikkerhetsmyndighet	12 totalt
Etterretningstjenesten	13 totalt

Tabell 1 Oversikt over antall trusselvurderinger fordelt på de ulike etterretnings- og sikkerhetsmyndighetene.

Ved siden av de årlige trusselvurderingene publiserer etterretnings- og sikkerhetsmyndighetene fortløpende både ugraderte og graderte rapporter og analyser gjennom året som tar for seg trusselbildet, dets utvikling, og sikkerhetsarbeid generelt. Dette er rapporter som virksomheter, ulike myndigheter og politikere kan benytte som del av sin beslutningsstøtte. Som følge av kapasitetsmessige årsaker og oppgavens begrensninger knyttet til ord med mer er ikke slike rapporter del av vår analyse.

Når det gjelder kodingen av de nasjonale trusselvurderingene er det kun PST sine trusselvurderinger innenfor det angitte tidsrommet (2011-2023) som blir kodet i ordets rette forstand. I tillegg til å analysere i hvilket omfang cybertrusselen beskrives og vies oppmerksomhet i oppbygningen av samtlige trusselvurderinger fra de ulike etterretnings- og sikkerhetsmyndighetene, vil PST sine trusselvurderinger bli kodet opp imot omtale av cyberangrep, les: hvor mange ganger PST benytter begrepene «datanettverksoperasjon» og/eller «nettverksoperasjon» per år. Hensikten med å kode PST sine trusselvurderinger har vært å gi et visuelt innblikk i den utvikling samtlige av etterretnings- og sikkerhetsmyndighetene belyser.

3.3.2 Styring

For å belyse en eventuell utvikling i departementenes styring av underliggende virksomheter vil tildelingsbrevene bli analysert med tanke på å undersøke hvorvidt disse benyttes som redskaper til endringer innenfor dette dagsaktuelle samfunnssikkerhetsfeltet, og om de som del av departementenes styringsdialog brukes til å få *noe* til å skje.

Samtidig er det viktig å understreke at disse dokumentene ikke eksisterer alene. Departementene benytter en rekke styringssignaler (verktøy) overfor underliggende

virksomheter. Innenfor samfunnssikkerhetsfeltet hvor digital sikkerhet inngår finnes det en rekke lovverk som regulerer arbeidet med sikkerhet og beredskap. Eksempler på slike er Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) og Lov om elektronisk kommunikasjon (ekomloven). I tillegg er det en rekke forskrifter som har relevans for departementers og underliggende virksomheters arbeid med forebyggende sikkerhet, men også spesielt innenfor de ulike sektorene. Dette er alle styringssignaler som opptrer sammen med tildelingsbrev og som påpekt av Asdal & Reinertsen (2020, s. 95) må vi i en slik kontekst hensynta at vi ikke kan konkludere hundre prosent med våre funn da en tekst (i dette tilfellet tildelingsbrevene) aldri kan forstås helt isolert fra de sammenhengene eller konteksten den inngår i.

Tildelingsbrevene som blir analysert ble i all hovedsak hentet fra departementenes egne sider på www.regjeringen.no. Der tildelingsbrev for aktuelle år ikke lå på regjeringen.no, ble det forespurt om innsyn i disse ved å kontakte departementene direkte. Begjæring om innsyn i Helse- og omsorgsdepartementets tildelingsbrev til Folkehelseinstituttet for tidsperioden 2011-2013, og 2023, ble godkjent. Det samme ble begjæring om innsyn i Olje- og energidepartementets tildelingsbrev til Norges vassdrags- og energidirektorat for tidsperioden 2011-2013.

Det er kun tildelingsbrev fra aktuell tidsperiode som analyseres. Øvrige dokumenter, eksempelvis vedlegg til tildelingsbrev, supplerende tildelingsbrev etc. er ikke del av analysen[4]. Konsekvensene av dette kan være at analysen ikke fanger opp alle føringer som departementene legger i styringen av de underliggende virksomhetene. Samtidig mener vi at avgrensningen er nødvendig gitt oppgavens rammer.

Totalt er 26 tildelingsbrev del av analysen. Fordelingen er vist i tabell 2. Videre er samtlige dokumenter opplistet i kronologisk rekkefølge med brevtittel og dato, samt antall sider de består av i vedlegg 2. I tillegg har vi i vedlegg 2 en egen kolonne med «referansekode» til de ulike tildelingsbrevene. Eksempelvis vil det ved henvisning til Helse- og omsorgsdepartementet sitt tildelingsbrev til Folkehelseinstituttet for 2015 i løpende tekst bli referert til «HODFHI-15, side (s.) XX». Ved henvisning til lik (gjentakende) informasjon i tildelingsbrev flere år på rad vil det kun bli referert til tildelingsbrevets årstall, og ikke sidetall.

[4] Ett unntak er Helse- og omsorgsdepartementets tildelingsbrev til Folkehelseinstituttet for 2021. I «hovedbrevet» som fremgår på regeringen.no vises det til at departementet vil komme tilbake til tildelinger over fagkapitler, fullmakter, samt mål, oppdrag og rapporteringskrav for 2021 i et oppdatert tildelingsbrev på nyåret. Det er derfor tildelingsbrev «supplerende 1» som er del av vår analyse.

Tildelingsbrev	
Helse- og omsorgsdepartementet til Folkehelseinstituttet	2011-2023 (13 totalt)
Olje- og energidepartementet til Norges vassdrags- og energidirektorat	2011-2023 (13 totalt)

Tabell 2 Oversikt over antall tildelingsbrev fra departementer til underliggende virksomheter.

Videre er det nødvendig med noen kriterier, eller koder, for å identifisere om departementene i sine tildelingsbrev til de underliggende virksomhetene «styrer» med fokus på IKT-sikkerhet eller ikke. Miles og Huberman (1984) beskriver kodingen som å ta et utsnitt av en tekst, eksempelvis en setning eller et avsnitt, og klassifisere informasjonen i ulike kategorier på bakgrunn av dette (henvist i Johannessen et al., 2015, s. 174). Videre viser Johannessen et al. (2015, s. 174) til at kodene man begynner med ikke nødvendigvis er presise nok i forhold til det man analyserer; at kodene kan endre seg underveis. Med dette som utgangspunkt valgte vi å ha et åpent og bevisst forhold til dette i vårt arbeid med å analysere departementenes tildelingsbrev.

Økonomiregelverket pålegger departementene å fastsette overordnede mål og styringsparametere i tildelingsbrevene til underliggende virksomheter. I tillegg til overordnede mål med henvisninger til satsningsområder og strategiske utfordringer skal tildelingsbrev inneholde styringsparameter slik at man skal kunne vurdere både måloppnåelse og resultater (DFØ, 2020, kap. 2.5). Som følge av dette vil vi derfor ta utgangspunkt i dokumentenes fokus på mål, styringsparameter og aktivitetskrav, og foreta en kvalitativ analyse, en systematisk gjennomgang og tolkning av meningsinnholdet i dokumentene. I tillegg vil vi vurdere hvorvidt disse målene, styringsparameterne og aktivitetskravene fremstår som IKT-spesifikke eller IKT-uspesifikke.

Under redegjøres det nærmere for hva som er beskrivende for et mål, styringsparameter og aktivitetskrav, samt hensikten med å skille mellom IKT-spesifikke og IKT-uspesifikke krav.

Mål:

Politiske mål blir av departementene operasjonalisert gjennom blant annet tildelingsbrev, og underliggende virksomheter skal innenfor sine ressursrammer realisere de fastsatte målene (DFØ, 2020, kap. 1.5). Da vi er ute etter mål som omhandler IKT-sikkerhet definerer vi mål i denne sammenheng som styringssignaler som gis fra departementene til de underliggende

virksomhetene som konkrete overordnede mål og delmål i tildelingsbrevene, altså at de er eksplisitt omtalt som et mål, eller fremgår under *kapitteloverskrifter* som omhandler mål[5].

Styringsparameter:

Overordnede mål og strategi *konkretiseres* gjennom styringsparameter. Videre fastsettes ambisjonsnivået for hvilke resultater som skal oppnås knyttet til de aktuelle styringsparameterne (Senter for statlig økonomistyring [SSØ][6], 2006, s. 10). Kjærvik og Askim (2015, s. 3) beskrev dette som «et tall eller en vurdering som sier noe om utviklingen til et mål». DFØ (2020, kap. 2.5, avsn. 6) påpeker i sin veileder i etatsstyring at en utfordring kan være at sammenhengen mellom mål og styringsparameter ikke alltid er like klar. Ifølge PWC (2020, s. 4) så har det vist seg at det foreligger en usikkerhet blant de ulike departementene rundt hva som faktisk er å betrakte som et styringsparameter, samt at det er ulik praksis til hva, hvordan, og hvem som utformer de ulike styringsparameterne. På bakgrunn av dette kan man dermed risikere å gå glipp av faktiske/reelle styringsparameter som departementene selv ikke har identifisert/kategorisert.

Til tross for dette har vi i arbeidet med å identifisere relevante styringsparameter i all hovedsak kodet styringsparameter som er definert som nettopp dette i tildelingsbrevene. Dette for å unngå eventuelle misoppfatninger i størst mulig grad. Der hvor ett og samme styringsparameter har tilknyttede resultatkrav, indikatorer, statistikk eller lignende har vi ansett dette som ett styringsparameter.

Aktivitetskrav:

Der mål og styringsparametere gjerne oppgis punktvis, er aktivitetskrav i større grad knyttet til løpende tekst. Ofte oppgis aktivitetskrav i egne delkapitler, ofte avslutningsvis i tildelingsbrevene, og kapitlene tituleres ofte «styring og kontroll» eller «andre føringer og krav» (Kommunal- og moderniseringsdepartementet, 2020, s. 6). Ofte kan slike krav være fellesføringer fra det enkelte departement til samtlige av sine underliggende virksomheter.

Skillet mellom IKT-spesifikke krav og IKT-uspesifikke krav:

[5] Blant annet benytter Helse- og omsorgsdepartementet betegnelsen «spesielle oppdrag» om delmål som knytter seg til et hovedmål. Eksempelvis i tildelingsbrev for 2017 (brev av 12.01.2017), s. 6.

[6] Senter for statlig økonomistyring (SSØ) skiftet navn til Direktoratet for økonomistyring (DFØ) 14. november 2011.

I tillegg til å identifisere hvorvidt mål, styringsparameter og aktivitetskrav omhandler IKT-sikkerhet mener vi at det er relevant å definere hvorvidt disse styringssignalene fremstår som spesifikke eller uspesifikke. Ifølge DFØ (2023c) bør ikke virksomheter motta tildelingsbrev hvor det er behov for å tolke hva departementet *egentlig* mener. Samtidig vil det alltid være både behov og rom for tolkning i enkelte krav som fremstilles. Dette kan eksempelvis knytte seg til prinsipal- agentteori som nevnt i kapittel 2, og styringens skjæringspunkt mellom behovet for tillit og kontroll.

For å understreke skillet mellom IKT-spesifikke krav og IKT-uspesifikke krav kan et *IKT-spesifikt krav* eksemplifiseres slik: «virksomhet XX skal i løpet av 2022 gjennomføre risiko- og sårbarhetsvurderinger knyttet til IKT-sikkerhet», altså et krav hvor IKT-sikkerhet nevnes eksplisitt. Et *IKT-uspesifikt krav* kan derimot lyde: «virksomhet XX skal i løpet av 2022 gjennomføre risiko- og sårbarhetsvurderinger knyttet til relevant trusselbilde». Dette er med andre ord et krav hvor virksomheten selv må vurdere hva «relevant trusselbilde» består av, og hvor IKT-sikkerhet kan *tolkes* inn. Hensikten med dette skillet er med andre ord å kartlegge hvorledes ordlyden i de ulike tildelingsbrevene kan si oss noe om utviklingen i styring over tid, samt at vi unngår å utelate styringskrav relevant for IKT-sikkerhet på bakgrunn av begrepsbruk.

Kodeinstruks:

Under presenteres de konkrete kriteriene som ble brukt for å identifisere hvorvidt mål, styringsparameter eller aktivitetskrav omhandler IKT-sikkerhet:

- Ordene IKT, IKT-sikkerhet, IT-sikkerhet, cybersikkerhet, sikkerhet, driftssikkerhet, beredskap, samfunnssikkerhet, krisehåndtering og hendelseshåndtering er å finne i dokumentene.
- Formuleringer beskriver *forebygging* av uønskede hendelser relatert til cyber og IKT i virksomheten eller innenfor aktuell sektor.
- Formuleringer beskriver *håndtering* av uønskede hendelser relatert til cyber og IKT i virksomheten eller innenfor aktuell sektor.
- Formuleringer beskriver oppgraderinger og/eller videreutvikling av IKT-systemer, og arbeid med digitalisering.

Dersom et eller flere av disse kriteriene ble oppfylt ble det vurdert hvorvidt disse ordene og/eller formuleringene hører innunder mål, styringsparametere eller aktivitetskrav, samt om de

fremstår som IKT-spesifikke eller IKT-uspesifikke. For en mer konkret beskrivelse av kriteriene over er følgende kodeinstruks innarbeidet som eksempel:

Føring	**Forklaring**	**Eksempel (IKT-spesifikk)**	**Eksempel (IKT-uspesifikk)**
Mål	Hva departement ønsker oppnådd. Eksplisitt omtalt som mål, evt. fremgår under *kapitteloverskrift* som omhandler mål.	*Virksomhet XX skal arbeide for å videreutvikle egen evne til å forebygge og håndtere **IKT-hendelser** gjennom regelverk, veiledning, øvelser og tilsyn.*	*Virksomhet XX skal arbeide for å videreutvikle egen evne til å forebygge og håndtere **ulike former for ekstraordinære hendelser** gjennom regelverk, veiledning, øvelser og tilsyn.*
Styringsparameter	Et tall eller en vurdering som sier noe om utviklingen til et mål. Tilknyttede resultatkrav er også kodet som styringsparameter (Kjærvik og Askim 2015, 3).	*Det er for 2015 avsatt 15 mill. kroner til risikoreduserende tiltak innenfor **IKT-sikkerhet**.*	*Det er for 2015 avsatt 15 mill. kroner til risikoreduserende tiltak innenfor **sikkerhet og beredskap**.*
Aktivitetskrav	Konkrete aktiviteter, tiltak og oppdrag. Oppgis ofte under egne delkapitler, eks. titulert «styring og kontroll» eller	*Det forutsettes at virksomhet XX gjennomfører risiko- og sårbarhetsvurderinger knyttet til **IKT-sikkerhet**.*	*Det forutsettes at virksomhet XX gjennomfører risiko- og sårbarhetsvurderinger knyttet til **relevant trusselbilde**.*

	«andre føringer og krav»		

Tabell 3 Kodeinstruks

I forbindelse med koding av samtlige dokumenter i dette forskningsstudiet benyttet vi analyseverktøyet NVivo. Dette er et analyseprogram som blant annet kan benyttes til å telle ord og kategorisere tekst. Tallene vi fikk ved bruk av NVivo flyttet vi manuelt over i Microsoft Excel hvor vi utarbeidet ulike figurer for å visualisere våre funn.

Rapportering i tidsperioder:

Vi har valgt å dele den analyserte tidsperioden, 2011-2023, inn i fire perioder (2011-2013, 2014-2016, 2017-2019 og 2020-2023) og legge sammen gjennomsnittet for antallet funn innenfor hver tidsperiode. På denne måten får vi et relativt tydelig bilde på hvordan funnene fordeler seg, i tillegg til at en slik inndeling bidrar til mer robuste resultater da enkeltår kan bære preg av tilfeldigheter. Samtidig mener vi det er relevant å trekke konkrete eksempler på funn ut i fra enkeltår for å belyse hvordan departementene eventuelt endrer sine styringssignaler fra ett år til et annet. Under redegjør vi for datakvaliteten i vår forskning.

3.4 Reliabilitet og validitet

Reliabilitet omhandler påliteligheten til dataene som undersøkes og analyseres. Nærmere forklart knytter dette seg til «*nøyaktigheten av undersøkelsens data, hvilke data som brukes, den måten de samles inn på og hvordan de bearbeides»* (Johannessen et al., 2015, s. 229). I dette forskningsprosjektet er datagrunnlaget basert på offentlige dokumenter; nasjonale trusselvurderinger utgitt av NSM, PST og E-tjenesten som alle ligger åpent tilgjengelig på de respektives nettsider, samt tildelingsbrev sendt fra to ulike departementer til to ulike underliggende virksomheter. Tildelingsbrevene ligger i all hovedsak åpent tilgjengelig via regjeringen.no. Disse dokumentene vil ikke endre seg over tid, og innholdet vil slik sett alltid være det samme. Tidligere i kapittel 3 har vi etablert kriterier for vår analyse hvilket gjør identifisering av våre funn etterprøvbare. Det må dermed kunne anses som høy pålitelighet ved at samme forskningsprosess på samme grunnlag vil kunne gjentas i fremtiden.

I følge Johannessen et al. (2015, s. 40) er det ulike måter å teste dataens reliabilitet på. En av disse måtene er at ulike forskere undersøker samme fenomen. I dette tilfellet har samtlige dokumenter blitt gjennomlest og kodet etter samme kriterier i sin helhet av to personer. Da det kan oppstå skjevheter i kodingen gikk vi sammen i fellesskap, og sammenliknet våre funn, før vi sammenstilte disse. Dette styrker reliabilitet til metoden. Til tross for «enighet» om sammenstillingene er det viktig å understreke at kodingen er vår subjektive, felles oppfatning, av hva som er et «funn» og ikke. For å sikre best mulig reliabilitet knyttet til koding av tildelingsbrevene har vi også gjennomført en «utsjekk» med departementsansatte som jobber med etatsstyring, og utarbeidelse av blant annet tildelingsbrev, og fått tilbakemeldinger på at vår tilnærming fremstår som fornuftig og god. Vi mener derfor at samme forskningsprosess på samme data vil være avhengig av «øyet som ser», men at det jevnt over bør være samme utvikling som blir belyst.

Validitet innebærer at man virkelig «undersøker det man vil undersøke, og ingenting annet» (Thurén, 2009, s. 32). Vi har tidligere i kapittelet definert mål, styringsparameter og aktivitetskrav, samt konkretisert disse i en kodeinstruks. Samtidig ser vi hvordan de ulike departementene benytter ulike begreper i tildelingsbrevene. Dette gjør at det kan diskuteres hvorvidt begrepsvaliditeten er tilstrekkelig eller ikke. Der det er behov beskrives begreper, og eventuelle ulikheter fortløpende.

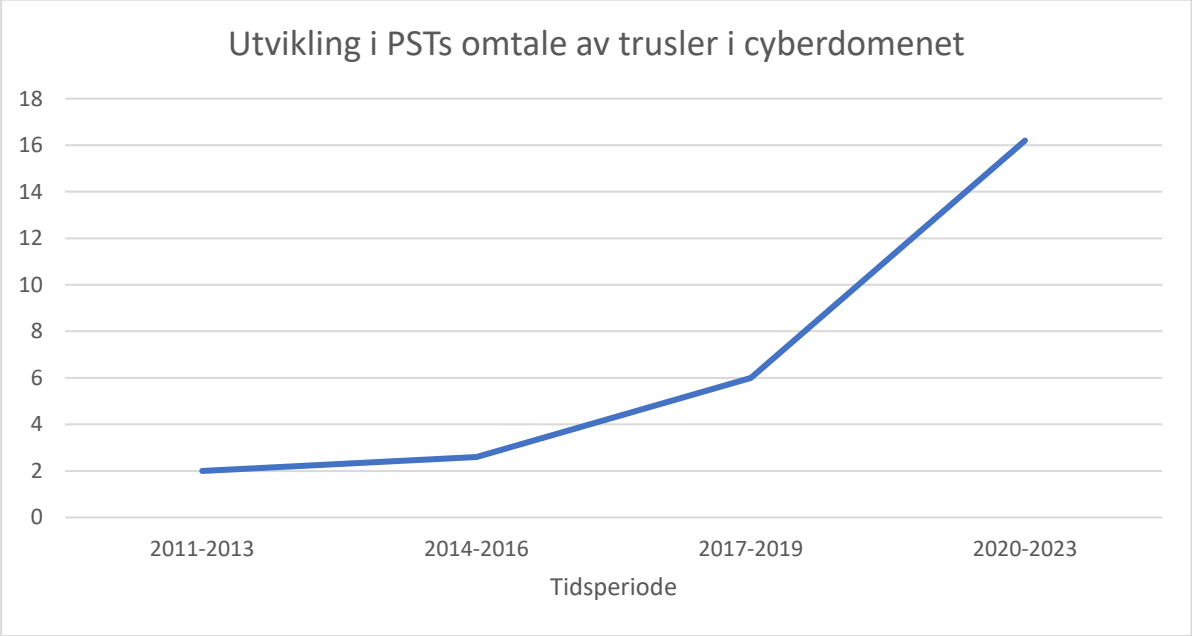
I oppgaven analyseres tildelingsbrev utgitt av to departementer. Som beskrevet i kapittel 2 anses disse som sentrale styringsverktøy. Tatt dette i betraktning er dokumentene relevante for å belyse oppgavens problemstilling. Ifølge Grønmo (2004, s. 231) kan dette innebære god validitet. Videre kan forskerens subjektive oppfatning under analysearbeidet gjøre at dokumentenes informasjon oppfattes annerledes enn hva som var hensikten fra departementenes side. Det understrekes ettertrykkelig at vår oppfatning av temaet for oppgaven (IKT-problematikken), samt departementer og underliggende virksomheter er svært komplekse. Våre funn (og eventuelle «manglende» funn) kan knytte seg til en rekke årsakssammenhenger og forklaringer. For å svare ut oppgavens problemstilling og hypoteser kunne man benyttet flere ulike metoder, blant annet intervjuer av ansatte både i departementer og underliggende virksomheter. Dette kunne i større grad belyst hva departementene har hatt til hensikt å kommunisere til sine underliggende virksomheter, samt hva de underliggende virksomhetene faktisk oppfattet.

Samtidig søker oppgaven blant annet å se på hvorvidt det er korrelasjon mellom utviklingen i nasjonalt trusselbildets fokus på trusler i cyberdomenet og den styringsutøvelse som utøves via tildelingsbrev. Om det i våre funn og analyser viser seg å være en korrelasjon, altså en samvarians, må vi allikevel være bevisste på at dette kun viser til en mulig (sannsynlig) mekanisme mellom fenomenene, og at vi gjennom våre analyser ikke får oversikt over alle variabler (mulige årsakssammenhenger). Johannessen et al. (2015, s. 310) trekker i forbindelse med dette frem at konklusjonene dermed ikke kan sies å være hundre prosent, men mer moderate.

4 Funn

4.1 Utvikling i nasjonalt trusselbilde

Analysen av trusselvurderingene viser en markant økning i omfang hva gjelder fokus på cybertrusler over tid. Figur 2 viser hvor mange ganger begrepene datanettverksoperasjon og nettverksoperasjon nevnes i PSTs trusselvurderinger innenfor hele det analyserte tidsrommet. Særlig er økningen stor fra 2017-2019 og utover, der gjennomsnittet økes fra å ha ligget på 6 ganger i 2017-2019 til over 16 ganger i 2020-2023. Under går vi nærmere inn på hovedfunnene i de ulike etterretnings- og sikkerhetsmyndighetenes trusselvurderinger for hver tidsperiode.



Figur 2 Gjennomsnitt av antall ganger PST bruker begrepene datanettverksoperasjon/nettverksoperasjon i årlige trusselvurderinger

Tidsperiode 2011-2013:

Allerede i 2011 beskrev PST i sin trusselvurdering hvordan flere utenlandske staters etterretningstjenester er aktive i Norge. «Datanettverksoperasjoner» trekkes frem som en metode som blir stadig viktigere for disse tjenestene i deres etterretningsarbeid, samtidig som det understrekes at «cyberetterretning» ikke erstatter tradisjonell etterretningsvirksomhet, men heller fungerer som et supplement til informasjonsinnhentingen (PST, 2011, kap. 4, avsn. 8).

Slike beskrivelser går igjen i trusselvurderingene fra PST, NSM og E-tjenesten i de påfølgende årene. Samtidig viser våre funn at etterretnings- og sikkerhetsmyndighetene gradvis vektlegger

at datanettverksoperasjoner år for år er en etterretningsmetode i rask utvikling og med et stort skadepotensial. NSM er i sine trusselvurderinger svært tydelig på sin bekymring rundt norske virksomheter, og hvordan det norske samfunnet mangler forståelse av risiko knyttet til avhengigheter av IKT og internett. I 2012 understreker NSM at det vil være et stort skadepotensial ved cyberangrep mot samfunnskritiske tjenester og kritisk infrastruktur, og at viktige tiltak som blant annet risikovurderinger og kompetanseheving ikke blir gjennomført (NSM, 2012, s. 4).

Totalt i tidsperioden nevnes datanettverksoperasjon og/eller nettverksoperasjon gjennomsnittlig 2 ganger i PST sine trusselvurderinger.

Tidsperiode 2014-2016:

I tidsperioden 2014-2016 ser vi at PST og E-tjenesten i sine trusselvurderinger vier sitt hovedfokus på beskrivelser av terrororganisasjoner, ulike ekstremistiske miljøer og etterretningsvirksomhet. I denne perioden beskrives cybertrusselen overordnet, og ofte til slutt i vurderingene. Allikevel ligger det et alvor i det som er skrevet om cybertrusselen, hvor angrep mot kritisk infrastruktur innen kraftforsyning, ulike betalingstjenester og politiske beslutningsorganer brukes som gjentakende eksempler på angrep som vil kunne forårsake betydelig skade (Etterretningstjenesten, 2015, s. 85). Fortsatt beskrives cybertrusselen relativt moderat ved at datanettverksoperasjon og/eller nettverksoperasjon i gjennomsnitt er nevnt 2,6 ganger i trusselvurderingene i denne tidsperioden.

Tidsperiode 2017-2019:

Fra og med 2018 vies cybertrusselen mer oppmerksomhet i trusselvurderingene. Dette hever den gjennomsnittlige omtalen av datanettverksoperasjoner og/eller nettverksoperasjon innenfor tidsperioden til 6. I 2019 trekker PST «statlig styrte nettverksoperasjoner» frem for første gang som et eget underkapittel til statlig etterretningsvirksomhet (PST, 2019, s. 8). I tillegg trekkes slike operasjoner frem i vurderingens innledende oppsummering av det nasjonale trusselbildet (PST, 2019, s. 5).

Tidsperiode 2020-2023:

I den siste tidsperioden ser vi den største økningen. I perioden 2020-2023 nevnes datanettverksoperasjon og/eller nettverksoperasjon i gjennomsnitt 16,2 ganger i PSTs trusselvurderinger per år. Dette er en markant økning fra de foregående tidsperiodene.

I nasjonal trusselvurdering for 2020 ser vi at PST har valgt en noe annen struktur i vurderingens oppbygning sammenliknet med de foregående årene. Selv om trusselbildet som beskrives i stor grad fremstår som uendret fra 2019 er det interessant å finne at trusler i cyberdomenet nå beskrives som en trussel som påvirker *samtlige* av PST sine ansvarsområder (PST, 2020b, s. 2).

I NSM sin trusselvurdering for 2022 beskrives en tredobling i antall cyberangrep mot norske virksomheter i tidsperioden 2019-2021 (NSM, 2022b, s. 9). Av eksempler på slike digitale angrep er det flere som kan trekkes frem: i 2019 ble Norsk Hydro utsatt for et stort løsepengevirus, hvorpå det kostet selskapet nærmere en milliard kroner å komme tilbake til normal drift (Stolt-Nielsen & Lysberg, 2021). I 2020 og 2021 ble Stortinget rammet av cyberangrep, hvor flere av de ansattes e-post kontoer ble kompromittert. I etterkant av angrepene på Stortinget informerte PST om at trusselutøveren lyktes i å stjele sensitive data fra ulike e-postkonti. PST vurderte i forbindelse med angrepene at disse hadde til formål å innhente grunnleggende informasjon om norske forhold som kan brukes i nye og mer spissede etterretningsoperasjoner i fremtiden (PST, 2020a). I 2021 ble mediehuset Amedia utsatt for et cyberangrep som førte til at papiraviser ikke ble publisert påfølgende dag (NTB, 2021). I tillegg ble Østre Toten kommune utsatt for et cyberangrep som førte til at omkring 240 virksomhets-systemer i kommunen ble utilgjengelige samtidig som de ble krevd for løsepenger (Østby & Kowalski, 2022, s. 4). Felles for angrepene er at de rammer viktige norske interesser, og at de setter samfunnet på store prøvelser.

NSM peker på at cyberangrep mot virksomheter i verstefall kan få konsekvenser for Norges nasjonale sikkerhet, og at det trengs et betydelig løft i bevissthet og kompetanse om trusselbildet og sikkerhetsarbeidet, fra *«øverste ledelse til den enkelte ansatte»* (NSM, 2022a, avsn. 4 og 6). Dette er interessant gitt tidligere redegjørelse hvor det kommer frem at NSM allerede i 2012 beskrev IKT og internett som en strategisk sikkerhetsutfordring, og hvordan risikoforståelse og gjennomføring av risikovurderinger var fraværende i virksomheter.

Det er med andre ord ingen tvil om at det har vært en markant utvikling i det nasjonale trusselbildet, hvor beskrivelser og advarsler knyttet til trusler i cyberdomenet stadig aktualiseres og vies mer plass i etterretnings- og sikkerhetsmyndighetenes årlige trusselvurderinger i den siste tidsperioden.

Samtidig søker denne oppgaven å belyse hvorvidt departementene i deres årlige tildelingsbrev utøver styring i tråd med denne utviklingen eller ikke. Videre i kapittelet vil vi derfor beskrive tildelingsbrevets rolle som styringsverktøy, samt presentere våre funn i analysene av tildelingsbrev fra Helse- og omsorgsdepartementet til Folkehelseinstituttet og Olje- og energidepartementet til Norges vassdrags- og energidirektorat.

4.2 Tildelingsbrevets rolle som styringsverktøy

Både Helse- og omsorgsdepartementet og Olje- og energidepartementet har i sine tildelingsbrev beskrivelser som støtter oppunder tildelingsbrevets funksjon som hovedkanal for departementenes forventninger og krav som oppfølging på Stortingets budsjettvedtak. Tildelingsbrevet blir av Helse- og omsorgsdepartementet beskrevet som et brev der de viktigste og høyest prioriterte oppgaver og målsetninger, samt beskrivelse av nye oppgaver kommer frem. Samtidig presiserer Helse- og omsorgsdepartementet at tildelingsbrevet ikke skal fungere som en aktivitetsplan og dermed ikke er ment å skulle dekke alle oppgaver som underliggende virksomhet skal arbeide med innenfor tidsperioden (Helse- og omsorgsdepartementet, 2015, s. 3). Når det gjelder Olje- og energidepartementet beskriver de at etatsstyringen hovedsakelig skjer gjennom tildelingsbrev, og at det her blant annet formidles og presiseres mål og resultatkrav (Olje- og energidepartementet, 2020, s. 3).

Om vi innledningsvis ser på samtlige tildelingsbrev under ett ser vi at disse er noe ulike i utformingen og at det benyttes ulike begreper av de to departementene, også i de tilfeller hvor innholdet ser ut til å være mye av det samme. Begge departementer ser ut til å benytte en relativt fast struktur gjennom hele tidsperioden, med enkelte endringer underveis.

I all hovedsak kan tildelingsbrevenes utforming belyses gjennom å henvise til hvilke hovedkapitler som stort sett er del av brevene:

Forenklet inndeling av kapitler i analyserte tildelingsbrev	
Helse- og omsorgsdepartementet til Folkehelseinstituttet	Olje- og energidepartementet til Norges vassdrag- og energidirektorat
• Bevilgning • Hovedmål og prioriteringer / samfunnsoppdrag, mål og styringsparameter	• Innledning • Mål, prioriteringer og styringsparameter • Viktige oppgaveområder • Særskilt virksomhet

• Øvrige forventninger / andre føringer • Styringskalender	• Andre forutsetninger og krav • Rapportering og resultatoppfølging • Budsjettildeling og fullmakter • Tildeling

Tabell 4 Forenklet inndeling av kapitler i analyserte tildelingsbrev

Når det gjelder størrelse på brevene ser vi av vedlegg 2 at snittet for antall sider i tildelingsbrevene sendt fra Helse- og omsorgsdepartementet til Folkehelseinstituttet ligger på 14,4 sider, mens det for Olje- og energidepartementets dialog med Norges vassdrags- og energidirektorat ligger på 15,8 sider. Dette er en forskjell på ca. 1,5 side.

Videre i kapittelet presenterer vi våre funn i de aktuelle tildelingsbrevene.

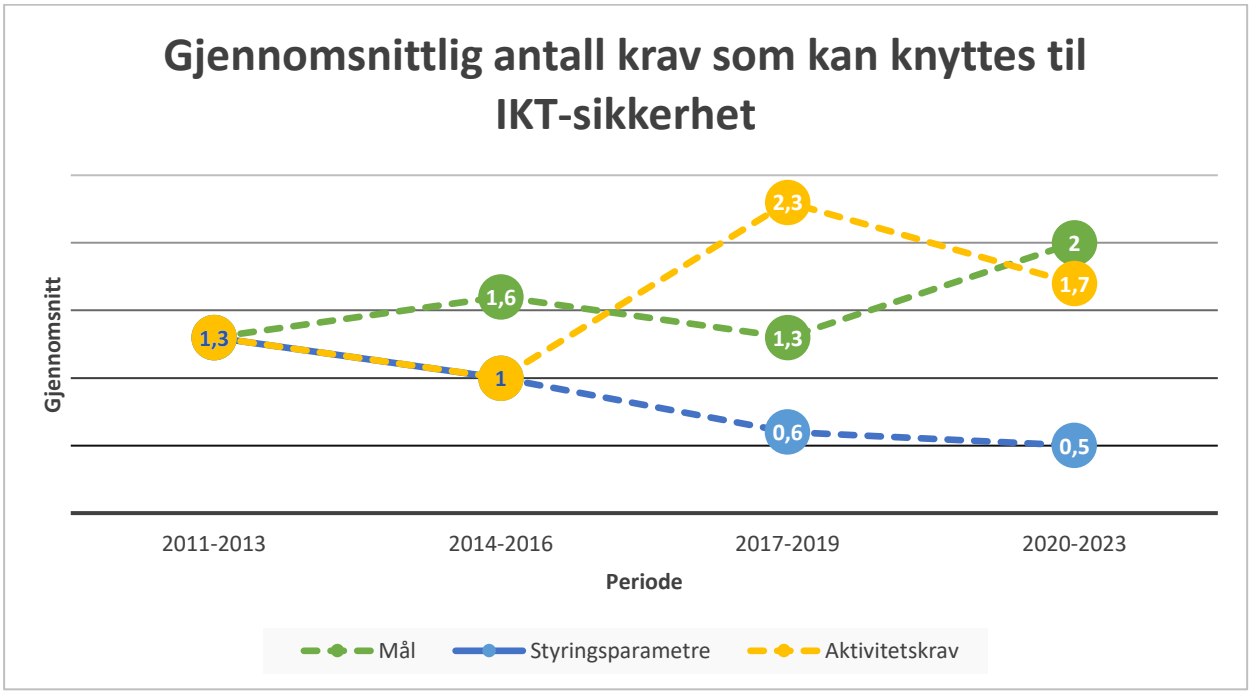
4.2.1 Funn i tildelingsbrev fra Helse- og omsorgsdepartementet til Folkehelseinstituttet

Totalt er det for perioden 2011-2023 identifisert 53 krav tilknyttet IKT-sikkerhet i Helse- og omsorgsdepartementets styring av Folkehelseinstituttet. Ved å dele inn den aktuelle tidsperioden i fire perioder og legge sammen gjennomsnittet for antallet mål, styringsparameter og aktivitetskrav får vi et relativt tydelig bilde på hvordan disse kravene fordeler seg, uavhengig av om de er IKT-spesifikke krav eller om de fremstår som generelle krav knyttet til sikkerhet (IKT-uspesifikke).

Som et resultat av vår analyse og koding av Helse- og omsorgsdepartementet sine årlige tildelingsbrev til Folkehelseinstituttet kan det ut ifra figur 3 blant annet leses at Helse- og omsorgsdepartementet stiller krav til Folkehelseinstituttet innenfor IKT-sikkerhet, og at slike krav tilsynelatende har blitt stilt innenfor hele den analyserte tidsperioden. Samtidig er det på det rene at det foreligger ulikheter i antallet krav knyttet til kategoriene mål, styringsparameter og aktivitetskrav gjennom perioden.

Blant annet viser våre funn at antallet krav knyttet til *styringsparameter har gått jevnt nedover* gjennom hele tidsperioden. Om vi vurderer tidsperioden ut ifra at den består av en første halvdel og en andre halvdel ser vi at for *mål og aktivitetskrav har det vært en betydelig oppgang*, der andre halvdel klart står i kontrast til første halvdel. Dette er funn som kan gi indikasjoner på at

Helse- og omsorgsdepartementet i sin styring av Folkehelseinstituttet har blitt mer detaljfokusert innenfor temaer som omhandler IKT-sikkerhet.



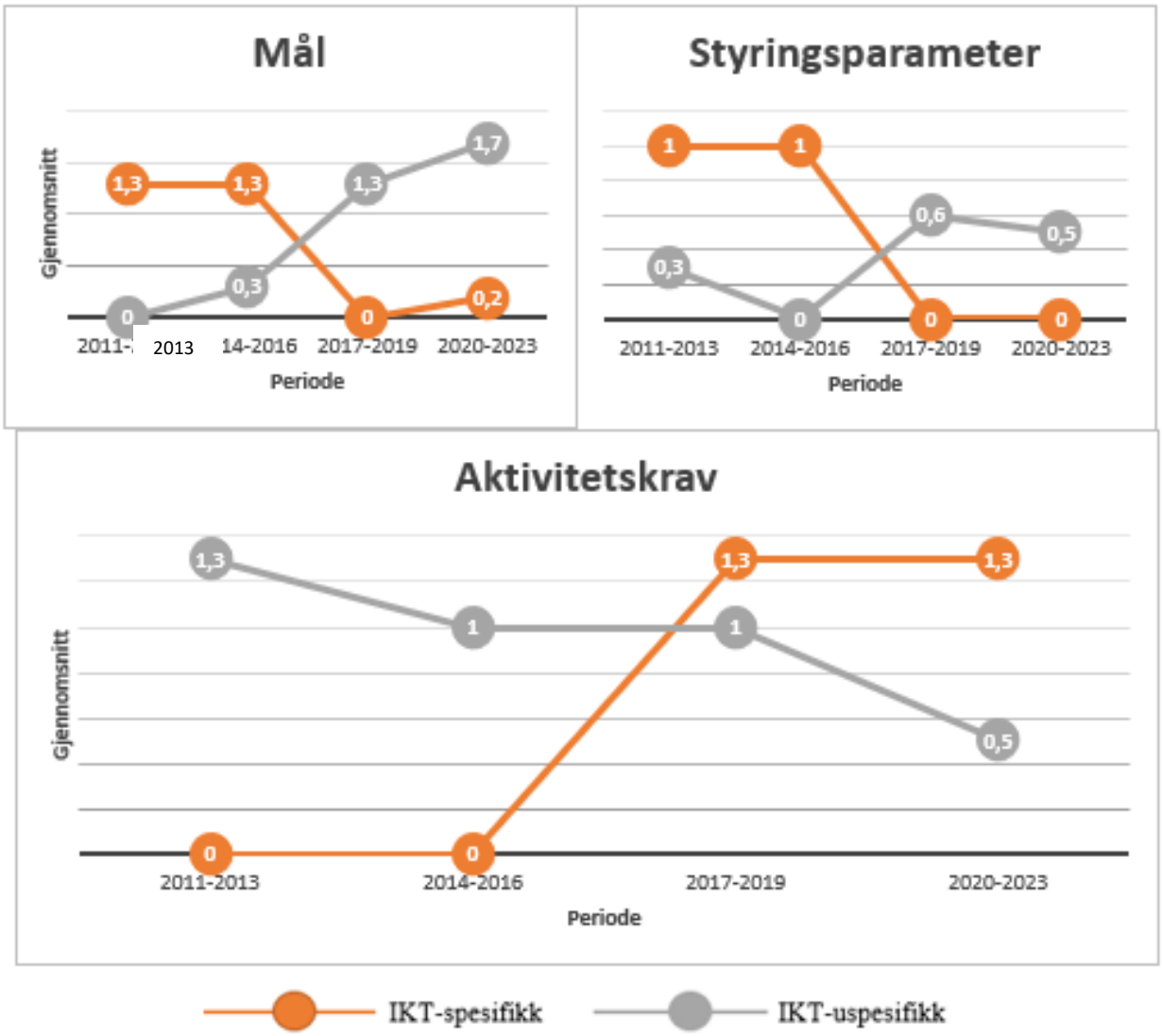
Figur 3 Gjennomsnittlig fordeling av det totale antallet mål, styringsparameter og aktivitetskrav etter sammenslåtte tidsperioder (Helse- og omsorgsdepartementet til Folkehelseinstituttet)

En interessant observasjon er å se at det i første halvdel av den undersøkte perioden (2011-2016) ligger gjennomsnittlig antall aktivitetskrav på ca. 1 per år (totalt 7), mens det i andre halvdel av den undersøkte perioden (2017-2023), ligger gjennomsnittlig antall aktivitetskrav på nærmere 2 (totalt 14). Altså en dobling av antall aktivitetskrav fra første til siste halvdel av aktuell tidsperiode. Om vi gjør samme øvelse for det totale antallet mål, styringsparameter og aktivitetskrav ser vi at det i perioden 2011-2016 var totalt 23 krav, mens det i andre halvdel fra 2017-2023 var 30 krav, altså en økning på ca. 30 %.

I det videre undersøkes det hvorvidt de nevnte kravene fremstår som IKT-spesifikke eller IKT-uspesifikke.

IKT-spesifikke krav versus IKT-uspesifikke krav:

Av figur 4 ser vi en tydelig trend der spesifikke mål og styringsparameter går ned, mens de spesifikke aktivitetskravene går opp. På mange måter skjer det en forskyvning hvor aktivitetskrav tar over for målene.



Figur 4 Gjennomsnittlig fordeling av antallet IKT-spesifikke og IKT-uspesifikke mål, styringsparameter og aktivitetskrav (Helse- og omsorgsdepartementet til Folkehelseinstituttet)

Av figur 4 kan det leses at den gjennomsnittlige fordelingen av antallet *mål* relatert til om disse er IKT-spesifikke eller IKT-uspesifikke viser en stor endring fra første til andre halvdel av den analyserte tidsperioden. De IKT-spesifikke målene går fra å ligge på jevnt over ett mål i første halvdel, for så å tilnærmet forsvinne helt i andre halvdel. For IKT-uspesifikke mål har tendensen vært den stikk motsatte.

I tidsperioden 2011-2016 ser vi at det ble satt IKT-spesifikke mål, med et stabilt gjennomsnitt på 1,3. Målene disse årene dreier seg i all hovedsak om fokus på informasjonssikkerhet, samt at departementet henstiller Folkehelseinstituttet til å følge opp *felles nasjonale IKT-prinsipper*. For tidsperioden 2017-2019 blir derimot disse IKT-spesifikke målene helt borte, og i perioden

2020-2023 blir det kun stilt ett IKT-spesifikt mål. Dette målet stilles i tildelingsbrevet for 2020, og er det eneste tilfellet i det undersøkte datasettet hvor det stilles krav til øvelse: «Folkehelseinstituttet skal delta i planlegging og gjennomføring av Helseøvelsen 2020, som har *IKT-scenario* og ledes av Helsedirektoratet» (HODFHI-20, s. 9).

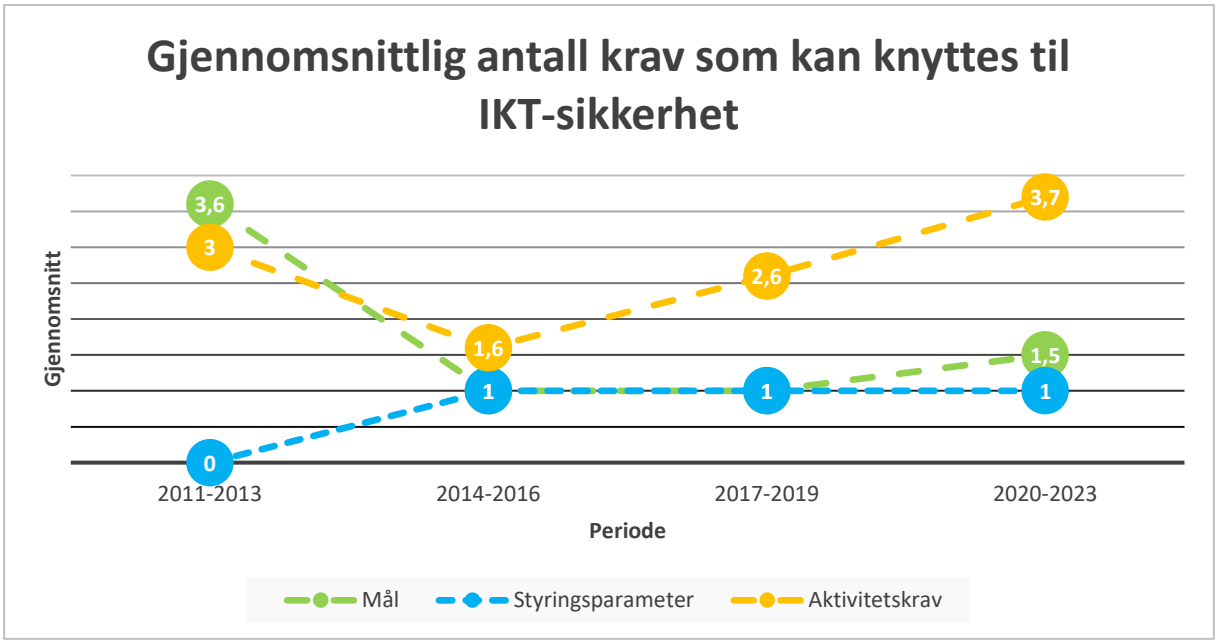
Når det gjelder IKT-spesifikke *styringsparameter* ser vi at disse på lik linje som IKT-spesifikke mål følger noe av den samme trenden, med et stabilt gjennomsnitt på 1 i de to første tidsperiodene. Etter 2016 er det derimot ingen IKT-spesifikke styringsparameter. Av tallene kan vi se et fravær av konsistens og en utvikling som snarere kan beskrives som ujevn. I perioden frem til og med 2016 viser våre funn at det ble brukt flere spesifikke styringsparameter enn i hele den øvrige perioden som inngår i det undersøkte tallmaterialet. I perioden etter 2016, altså 2017-2023 har det hovedsakelig variert mellom 0 og 1 styringsparameter, og i de tilfellene hvor det forelå styringsparameter så er disse å anse som IKT-uspesifikke.

Vedrørende *aktivitetskrav* ser vi som nevnt en til dels motsatt trend enn hva vi finner for mål og styringsparameter. Der både IKT-spesifikke mål og IKT-spesifikke styringsparameter i all hovedsak gjorde seg gjeldende frem til og med år 2016, gjør de IKT-spesifikke aktivitetskravene seg gjeldende fra andre halvdel av den analyserte tidsperioden.

Konkret viser våre funn at det blant annet dukker opp et eget kapittel i tildelingsbrevet for 2017 som tar for seg personvern og informasjonssikkerhet. Dette kapittelet inkluderes i samtlige brev frem til og med 2022. Når det gjelder tildelingsbrevet for 2022 viser departementet også til «krav til digital sikkerhet» hvorpå de skriver at «Folkehelseinstituttet forutsettes å ha forsvarlige rutiner, klar rollebevissthet og aktive planer for de situasjoner som kan oppstå» (HODFHI-22, s. 11).

4.2.2 Funn i tildelingsbrev fra Olje- og energidepartementet til Norges vassdrags- og energidirektorat

Totalt er det for perioden 2011-2023 identifisert 70 krav innenfor IKT-sikkerhet i Olje- og energidepartementets styring av Norges vassdrags- og energidirektorat.



Figur 5 Gjennomsnittlig fordeling av det totale antallet mål, styringsparameter og aktivitetskrav etter sammenslåtte tidsperioder (Olje- og energidepartementet til Norges vassdrags- og energidirektorat)

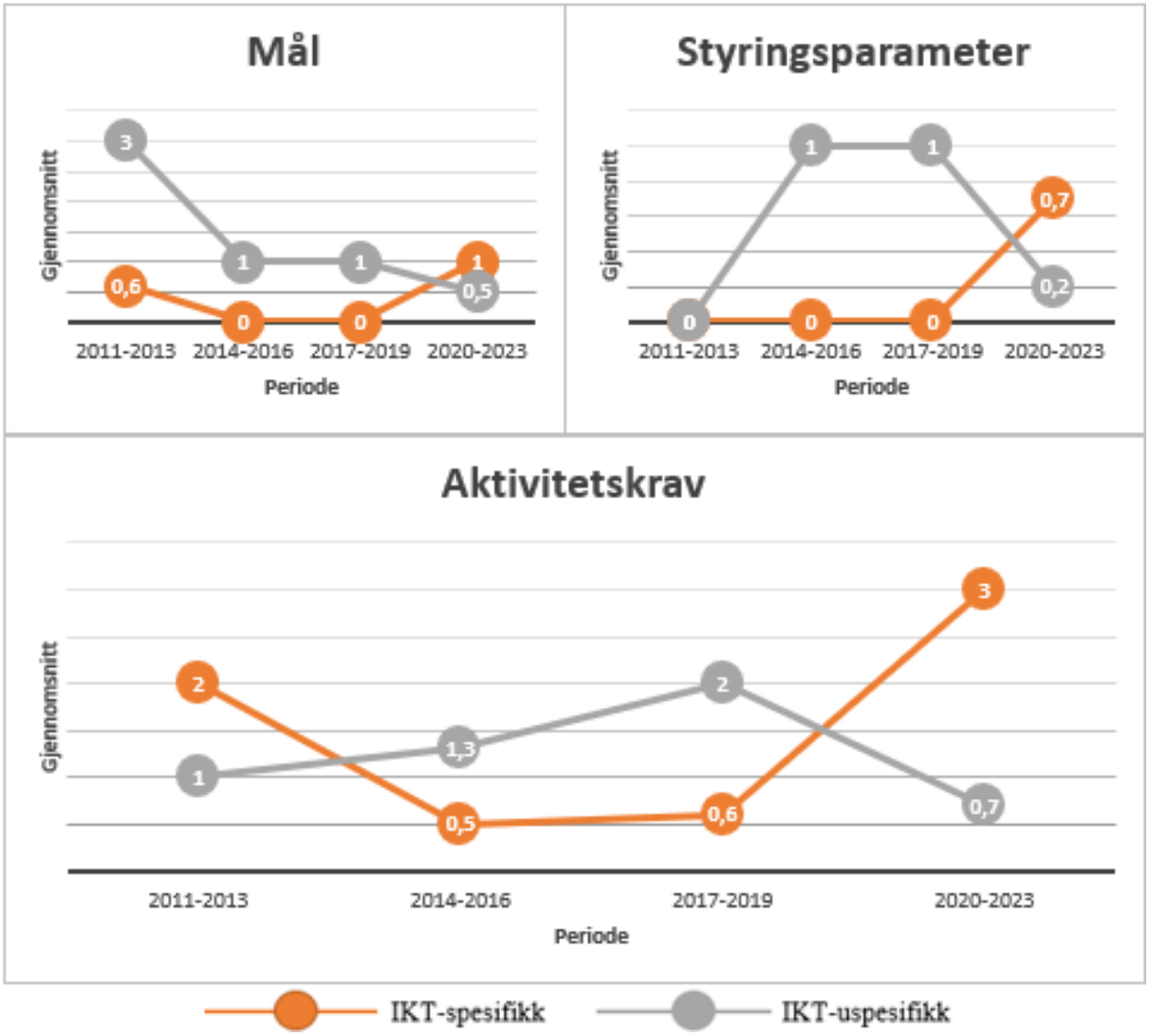
På lik linje med funn i tildelingsbrevene fra Helse- og omsorgsdepartementet til Folkehelseinstituttet er det ingen tvil om at Olje- og energidepartementet innenfor hele den analyserte tidsperioden i sine tildelingsbrev til Norges vassdrags- og energidirektorat har stilt krav innenfor IKT-sikkerhet, og at disse jevnt over har ligget på et noe høyere antall enn i førstnevntes tilfelle. Ved å se på gjennomsnittlig antall krav relatert til mål, styringsparameter og aktivitetskrav, uavhengig av om de er IKT-spesifikke eller IKT-uspesifikke, ser vi at *styringsparameter har ligget stabilt* over flere år. Når det gjelder mål og aktivitetskrav ser vi at antallet *mål i all hovedsak går ned* fra første til andre tidsperiode, mens de deretter holder seg jevnt med styringsparameter i tredje og fjerde periode. *Aktivitetskravene går opp* slik vi så i Helse- og omsorgsdepartementets styring av Folkehelseinstituttet. Også her ser det ut som at aktivitetskravene til en viss grad tar over for målene.

Under vil fordelingen av hvorvidt mål, styringsparameter og aktivitetskrav innenfor gjeldende tidsperiode fremstår som IKT-spesifikk eller IKT-uspesifikke bli redegjort for.

IKT-spesifikke krav versus IKT-uspesifikke krav

Av figur 6 ser vi at mål og styringsparameter fra den andre perioden, 2014-2016, følger hverandre jevnt ut den totale undersøkte perioden. Dette gjelder både de IKT-spesifikke og IKT-uspesifikke kravene. Når det gjelder de spesifikke aktivitetskravene er det en interessant

observasjon å se hvordan disse øker i betydelig grad i siste periode. I de to foregående periodene, 2014-2016 og 2017-2019, har det knapt nok blitt stilt et IKT-spesifikt krav uavhengig av om disse har fremgått som mål, styringsparameter eller aktivitetskrav.



Figur 6 Gjennomsnittlig fordeling av antallet IKT-spesifikke og IKT-uspesifikke mål, styringsparameter og aktivitetskrav (Olje- og energidepartementet til Norges vassdrags- og energidirektorat)

Av figuren ser vi at antallet IKT-uspesifikke *mål* i første periode lå langt høyere enn det totale antallet mål i de øvrige tidsperiodene. I perioden 2014-2023 har det totale antallet mål i gjennomsnitt ligget på 0-1 per tidsperiode. Antallet mål har dermed holdt seg jevnt uavhengig av om disse har vært IKT-spesifikke eller IKT-uspesifikke.

Våre funn viser at det i første tidsperiode ble satt henholdsvis 5 (2011) og 4 (2012) mål relatert til IKT-sikkerhet hvorav 1 av disse målene var IKT-spesifikke innenfor de to aktuelle årene.

Blant annet skrev Olje- og energidepartementet i 2012 at «Norges vassdrags- og energidirektorat skal utrede, stille krav og føre tilsyn med kraftforsyningens økende avhengighet av IKT og de sikkerhetsmessige utfordringer dette medfører (…)» (OEDNVE-12, s. 8).

Videre finner vi at det fra og med 2014 til og med 2022 fremmes kun ett mål per år, hvilket er en markant nedgang fra de to første årene. I tillegg fremgår det av figur 6 at det i tidsperioden 2014-2016 og 2017-2019 ikke stilles ett eneste spesifikt krav til IKT-sikkerhet. På lik linje som vi fant i analysen av Helse- og omsorgsdepartementets tildelingsbrev til Folkehelseinstituttet blir de IKT-spesifikke målene «borte» også her. Samtidig fremmes det ett uspesifikt krav til IKT-sikkerhet i hvert tildelingsbrev innenfor den samme perioden. I brevene skriver Olje- og energidepartementet det samme hvert år, nemlig at et hovedmål for Norges vassdrags- og energidirektorat skal være å «fremme en sikker kraftforsyning» med delmål om at Norges vassdrags- og energidirektorat skal «påse at beredskapen i kraftforsyningen er god og i tråd med gjeldende krav».

Det som videre er interessant å finne er at departementet i tildelingsbrevene for 2021-2023 blir mer spesifikke i sine formuleringer. Under samme hovedmål, og i beskrivelsen av tilsvarende delmål som beskrevet over skriver departementet at «Norges vassdrags- og energidirektorat skal påse at sikkerhet og beredskap i kraftforsyningen er god, gitt ny risiko som følge av klimaendringer, digitalisering og et nytt sikkerhetspolitisk bilde, og at kravene til sikkerhet og beredskap følges». Dette er et godt eksempel på hvordan departementet endrer sin ordlyd fra det «uspesifikke» til det «spesifikke», relatert til IKT-sikkerhet. I tildelingsbrevet for 2023 fremmes det også et mål om at Norges vassdrags- og energidirektorat skal oppgradere og videreutvikle egne IKT-systemer (OEDNVE-23, s. 6).

Når det gjelder *styringsparameter* ser vi at det i perioden 2011-2013 var 0 styringsparameter relevant for IKT-sikkerhet. Dette endret seg imidlertid i den andre tidsperioden, 2014-2016, hvor antallet IKT-relevante styringsparameter stabiliserte seg på 1. Dette har vedvart ut hele den undersøkte tidsperioden. I siste periode, 2020-2023, finner vi en endring ved at styringsparametere endrer karakter fra å være uspesifikke til å bli spesifikke i de tre siste årene.

Når det gjelder *aktivitetskrav* viser våre analyser at det innenfor hele den aktuelle tidsperioden stilles totalt 37 aktivitetskrav, hvorav 21 IKT-spesifikke og 16 IKT-uspesifikke. Til

sammenlikning ble det stilt totalt 23 mål, hvorav 6 IKT-spesifikke og 17 IKT-uspesifikke innenfor samme tidsperiode.

Om vi ser på den gjennomsnittlige fordelingen av aktivitetskrav innenfor de fire tidsperiodene ser vi en relativt jevn fordeling. Samtidig fremgår det av materialet at departementet har hatt et relativt høyt og vedvarende fokus på IKT-sikkerhet. Samtidig ser vi av figur 6 at det i tidsperioden 2014-2016 og 2017-2019 var svært få IKT-spesifikke aktivitetskrav.

Mer konkret finner vi at det i perioden 2011-2014 rettes et spesielt fokus på at risikofaktorer knyttet til driftssikkerheten til IKT må følges spesielt opp. I 2012 skriver departementet blant annet at: «Norges vassdrags- og energidirektorat skal ha (…) rapporteringsrutiner til departementet for hendelser som truer eller kompromitterer IKT-sikkerheten. Samfunnskritisk infrastruktur skal være identifisert, klassifisert og beskyttet. Det tilrås at arbeidet med IKT-sikkerhet følger anerkjente standarder» (OEDNVE-12, s. 14).

I 2020 fremgår det av tildelingsbrevet at departementet mer enn dobler antallet relevante aktivitetskrav sammenliknet med året før, i tillegg til at 4 av 5 krav er IKT-spesifikke. Dette gir et gjennomsnitt på 3 spesifikke krav i tidsperioden 2020-2023. Man går altså fra 0,5 (2014-2016) og 0,6 (2017-2019) til 3 krav i den siste perioden. Dette må sies å være en betydelig oppgang, og et interessant funn for videre drøftelser.

I 2021 og 2022 skriver departementet at «Norges vassdrags- og energidirektorat må styrke arbeidet med IKT-sikkerhet i kraftforsyningen». Videre står det i tildelingsbrevene for 2022 og 2023 at «Norges vassdrags- og energidirektorat må sikre at Riksrevisjonens merknader og anbefalinger[7] følges opp når det gjelder arbeidet med IKT-sikkerhet i kraftforsyningen (…)». I 2023 vises det også for første gang i hele det undersøkte materialet til at departementet tildeler Norges vassdrags- og energidirektorat budsjettmidler til IKT-sikkerhet. Blant annet skriver Olje- og energidepartementet: «Norges vassdrags- og energidirektorat tildeles økte budsjettmidler i 2023 til IKT-drift og til å forsterke digitaliseringsprogrammet (…)» (OEDNVE-23, s. 8). Videre beskrives de nevnte bevilgningene slik:

- «15 mill kroner til å øke beredskapen mot IKT-angrep i kraftforsyningen og IKT-sikkerhetsmiljø i Norges vassdrags- og energidirektorat.

[7] Riksrevisjonens undersøkelse av Norges vassdrags- og energidirektorats arbeid med IKT-sikkerhet i kraftforsyningen. Dokument 3:7 (2020-2021).

- 10 mill kroner til digitaliseringsarbeid, IKT-utvikling og IKT-drift i Norges vassdrags- og energidirektorat» (OEDNVE-23, s. 13).

4.3 Oppsummering av funnene

Oppsummert ser vi at etterretnings- og sikkerhetsmyndighetenes trusselvurderinger i perioden 2011 til 2023 preges av et tydelig økt fokus på trusler i cyberdomenet, og utfordringer knyttet til den stadig økende digitaliseringen.

Videre finner vi at tildelingsbrevet som styringsverktøy har den sentrale rollen og funksjonen som teorien tilsier, men at det ikke foreligger en ensartet praksis på hvordan slike brev utformes, og at det således er noen interessante forskjeller mellom departementene. Overordnet ser vi derimot en tendens hvor begge departementer i løpet av den undersøkte tidsperioden i økt grad benytter aktivitetskrav fremfor mål - at det skjer en tydelig forskyvning i hvilke styringskrav som gjør seg gjeldende - og at disse kravene går fra å være av uspesifikk (generell) karakter til å omhandle IKT-sikkerhet spesifikt.

5 Drøfting og analyse

I dette analysekapittelet vil vi med utgangspunkt i hypotesene drøfte relevante funn opp imot relevant teori.

5.1 Økt fokus på trusler i cyberdomenet i de nasjonale trusselvurderingene

Ved gjennomgang av etterretnings- og sikkerhetsmyndighetenes trusselvurderinger innenfor tidsperioden er det tydelig at beskrivelsen av digitale trusler og digitale angrep har økt i omfang, og at de spesielt fra og med 2018 til 2023 i mye større grad enn tidligere beskrives og vies oppmerksomhet gjennomgående. Dette kan ses i sammenheng med NSM sin observerte tredobling i antallet alvorlige cyberangrep i perioden 2019-2021. I 2019 så vi også at PST for første gang trakk frem «statlig styrte nettverksoperasjoner» som et eget underkapittel til statlig etterretningsvirksomhet. Enkelt sagt er dette en måte for PST å sette søkelyset på problematikken rundt trusler i cyberdomenet.

Samtlige av eksemplene på cyberangrep i kapittel 4, setter alt i fra små og store virksomheter, til samfunnet som helhet på store prøvelser. Felles for eksemplene er at disse cyberangrepene lammet viktige norske interesser og/eller avhengigheter. I den forbindelse ble disse angrepene gjenstand for stor medieoppmerksomhet over lengre tid. At hendelsene i seg selv har hatt stor påvirkning på hvordan vi må jobbe for å beskytte oss mot den typen trusler, og dermed stor påvirkning på hva slags omfang etterretnings- og sikkerhetsmyndighetene beskriver og vier disse oppmerksomhet på i trusselvurderingenes oppbygning er det ingen tvil om. Det er også hensiktsmessig å se dette opp imot Pollit og Boucaert (2017, s. 40) sin teori om at medias fokus er med på å påvirke, og at summen av blant annet omtale og fokus tvinger frem tiltak. Dette gir støtte til vår hypotese (hypotese 3) om at *cyberangrep som har rammet norske virksomheter har hatt en påvirkende faktor på etterretnings- og sikkerhetsmyndighetenes fokus på dette feltet i årlige trusselvurderinger* innenfor den analyserte tidsperioden. Samtidig er det relevant å nevne at dette ikke er et entydig svar, og at det kan være flere relevante faktorer involvert.

5.2 Mer eller mindre detaljstyring relatert til IKT-sikkerhet?

Mål- og resultatstyring ble obligatorisk for alle statlige virksomheter i 1990 (Johnsen, 2015, s. 36). Styringsmetoden har til hensikt å stimulere til strategisk styring mot overordnede mål, så effektivt som mulig. I mål- og resultatstyring er det et viktig prinsipp at man delegerer

myndighet til det utøvende nivået. Dette med intensjon om at man da skaper tilstrekkelig handlingsrom og autonomi hos utøverleddet - "den som kjenner utfordringene best" (DFØ, 2023a, avsn. 7).

Samtidig har vi sett at Johnsen (2015, s. 36) trekker frem at mål- og resultatstyring i perioden etter 2010 har vært gjenstand for kritikk som følge av at den har tendert mot å være for detaljstyrende og for lite opptatt av resultat. Som følge av dette fremmet vi følgende hypotese: *kritikken av departementenes detaljstyring i perioden etter 2010 preger styringsutøvelsen og gjør seg gjeldende gjennom færre krav knyttet til IKT-sikkerhet jo nærmere vi kommer dags dato* (hypotese 1 B).

På den andre siden har det blitt vist til at kompleksitet, og komplekse problemstillinger, er en faktor som Christensen et al. (2015, s. 111) trekker frem som vesentlig i forbindelse med målformuleringer, og som kan medføre økt grad av detaljstyring. Gitt den åpenbare kompleksiteten som ligger i utviklingen i- og det å skulle beskytte seg mot trusler i cyberdomenet har vi fremmet en motstridende hypotese til hypotese 1 B: *kompleksitet og utvikling i cyberdomenet preger styringsutøvelsen og bidrar til økt grad av detaljstyring relatert til IKT-sikkerhet* (hypotese 1 A).

For å besvare hypotesene har vi undersøkt om Helse- og omsorgsdepartementet og Olje- og energidepartementet benytter seg av mål, styringsparameter og aktivitetskrav i sin styring av underliggende virksomheter opp imot IKT-sikkerhet, og hvorvidt styringen er detaljstyrende eller ikke. Vi har som anvist i kapittel 3.3.2 kodet, undersøkt og analysert det som i tildelingsbrevene omtales som IKT-sikkerhet helt eksplisitt (IKT-spesifikk), men har også sett behovet for å innlemme generelle krav knyttet til sikkerhet, som naturligvis også vil innbefatte IKT-sikkerhet, til tross for at det ikke er konkret uttalt (les: IKT-uspesifikk). Dette som følge av at vi vil unngå å havne i en situasjon hvor vi bevisst utelater styringskrav relevant for problemstillingen.

Ettersom vi kun analyserer 2 av 16 departementer finner vi det mest naturlig å drøfte og analysere de to departementene hver for seg, før vi sammenlikner dem i kapittel 5.3 og til dels i kapittel 5.4.

5.2.1 Grad av detaljstyring fra Helse- og omsorgsdepartementet til Folkehelseinstituttet

Det faktum at det første halvdel av den undersøkte perioden (2011-2016) var tilnærmet like mange IKT-spesifikke *mål*, som IKT-uspesifikke, er interessant opp imot en ønsket tilstand

hvor man fra politisk hold har hatt en uttalt målsetning om mindre detaljstyring og økt fokus på handlingsrom. Dette begrunnes med en forståelse av at IKT-spesifikke mål kan tolkes som et uttrykk for detaljstyring ettersom man da spesifikt instruerer og styrer underliggende virksomhet til ha fokus på denne tematikken. På den andre siden kan det være naturlig ettersom IKT-sikkerhetsarbeid har en iboende kompleksitet i seg, og som da *kan* møtes med høyere grad av detaljstyring. Det bemerkes dog at det er noe påfallende at graden av spesifikke mål reduseres jo nærmere vi kommer dags dato, noe som medfører en motsatt, eller negativ korrelasjon med utviklingen i det nasjonale trusselbildet.

Funnet i andre halvdel av den undersøkte perioden (2017-2023), hvor man ser at de spesifikke IKT-sikkerhetsmålene blir tilnærmet borte, og byttet ut med mål av mer generell karakter (IKT-uspesifikke), kan på den andre siden vitne om at man har bevissthet rundt ønsket om mindre detaljstyring. At man bevisst ønsker mindre grad av spesifikk instruering innenfor det IKT-sikkerhetsrelaterte arbeidet, med intensjon om å utøve lavere grad av detaljstyring. En slik tolkning og forståelse underbygger hypotesen (hypotese 1 B) om at kritikken av departementenes detaljstyring i perioden etter 2010 preger styringsutøvelsen, og gjør seg gjeldende gjennom færre krav knyttet til IKT-sikkerhet jo nærmere vi kommer dags dato. Alternativt kan det også argumenteres for at det kan være et tegn på manglende fokus, eller prioritering av denne typen problemstilling fra departementets side, og at arbeidet med IKT-sikkerhet vies lite oppmerksomhet. Dette vil i så tilfelle være en tilnærming som indikerer at man ikke har tatt innover seg et endret trusselbildet som tilsier behov for økt fokus på IKT-sikkerhet, hvilket kan vitne om at kritikken mot myndighetenes styring relevant for IKT-sikkerhet er berettiget.

År 2020 skiller seg ut fra de øvrige ved å ha klart flest mål knyttet til IKT-sikkerhet, henholdsvis 3 uspesifikke og 1 spesifikt. Når det gjelder det spesifikke målet er dette relatert til øvelse, og at Folkehelseinstituttet skal delta i planlegging og gjennomføring av «Helseøvelsen 2020 med IKT-scenario». Målet i seg selv fremstår mer som en aktivitet eller «oppdragsbestilling» i sin ordlyd enn et mål. Uansett er målet slik det er oppgitt et godt eksempel på hvordan departementet med statsråd i spissen ivaretar sitt ansvar i tråd med Samfunnssikkerhetsinstruksen ved å sette krav til at «den organisasjon som har ansvar for et fagområde i en normalsituasjon, også har ansvaret for nødvendige *beredskapsforberedelser* (…)» (Departementene, 2019, s. 22). Å øve er i dette tilfellet en nødvendig forberedelse i så måte.

Når det gjelder *styringsparametere* har disse til hensikt å kunne bidra til vurdering av måloppnåelse og resultater (DFØ, 2020, kap. 2.5). Videre er de et verktøy for å identifisere delmål, og dermed en indikator på fremdrift (Kommunal- og moderniseringsdepartementet, 2020, s. 5). All den tid det faktisk foreligger mål i perioden etter 2016 (minimum 2 per år) kan det argumenteres for at det bør foreligge minimum 1 til 1 antall styringsparameter. Det er minimum ett mål i perioden 2016-2023 (noen år er det flere). I samme periode mangler det styringsparameter fullstendig for årene 2019, 2021 og 2023. Et faktum som kan betraktes som en svakhet ved styringen, da man ikke i tilstrekkelig grad forsøker å bidra med tydelig retningsangivelse ved å ta i bruk styringsparameter.

Det faktum at man ser en reduksjon i det totale antallet IKT-relaterte styringsparameter, og et fullstendig fravær av IKT-spesifikke styringsparameter i perioden etter 2016 til dags dato kan forklares med at det i sin natur er krevende å definere gode styringsparameter ref. DFØs henvisning til at det kan være utfordrende å se en sammenheng mellom mål og styringsparameter (DFØ, 2020, kap. 2.5, avsn. 6), samt PWC (2020, s. 4) sine undersøkelser som har vist at det foreligger en usikkerhet blant de ulike departementene rundt hva som faktisk er å betrakte som et styringsparameter.

Videre kan det også tenkes at det lave antallet styringsparameter er en konsekvens av tanken om at det er viktig å begrense antall styringsparameter ettersom det ikke er hensiktsmessig å måle alt og at prioritering er viktig (SSØ, 2006). På den andre siden kan det være et uttrykk for at det er mindre viktig sammenlignet med andre oppgaver som skal prioriteres utover IKT-sikkerhet. Det er på det rene at verken departement eller underliggende virksomhet kan prioritere alt likt. Et fullstendig fravær av styringsparameter tenkes dermed å være en konsekvens av graden oppmerksomhet departementet ønsker å legge til arbeid med IKT-sikkerhet.

På den andre siden kan det være et uttrykk for høy grad av tillit mellom departement og underliggende virksomhet hvor man bevisst tilstreber å gi handlingsrom og autonomi innenfor arbeidet med IKT-sikkerhet. At departementet erkjenner egen begrensning med tanke på kunnskap/kompetanse både hva gjelder hva underliggende virksomheter har behov for eller den risiko de selv står ovenfor, en tilnærming i tråd med forvalterteori og ønsket/behovet for mindre detaljstyring.

Når det gjelder *aktivitetskrav* er trenden tydelig. Det faktum at antall aktivitetskrav øker med 100 % i perioden 2017-2023 sammenliknet med perioden 2011-2016 kan skyldes flere ulike faktorer, og kan tenkes å være et uttrykk for endring i styringsutøvelsen. Aktivitetskrav er forbundet med liten grad av handlefrihet og økt grad av kontroll, og står derfor i motsetning til våre drøftelser over vedrørende nedgang i antall mål. I følge DFØ (2023b, kap. 4, 8 avsnitt) vil man ved bruk av aktivitetsstyring som ikke er koblet til overordnede mål risikere at disse oppgavene/aktivitetene begrenser underliggende virksomhets mulighet til å prioritere og velge virkemidler som bidrar til måloppnåelse. I henhold til våre vurderinger knyttes aktivitetskrav i mindre grad til overordnede mål slik det kommer frem av tildelingsbrevenes ordlyd. Samtidig ser vi at departementet i stor grad lener seg på regelstyring i aktivitetskravene ved å blant annet henvise til sikkerhetsloven, og dens krav og rammer for Folkehelseinstituttet som virksomhet. Dette er krav som blant annet knytter seg til virksomhetens generelle arbeid med sikkerhet og beredskap opp imot ulike typer hendelser, og regnes i vår oppgave derfor som IKT-uspesifikke krav.

Kommunal- og moderniseringsdepartementet (2020) belyste som nevnt i kapittel 2 en reduksjon i antall aktivitetskrav i perioden 2012-2015, før man fra 2015 stod ovenfor en økning frem til 2020 som resulterte i at man endte tilbake på samme nivå i 2020 som i 2012. De senere års økning i aktivitetskrav relatert til IKT-sikkerhet, er sammenfallende med den generelle tendensen man så i Kommunal- og moderniseringsdepartementets funn, hvor antall aktivitetskrav hadde økt og det tilsynelatende forelå en utvikling i form av en forskyvning fra mål og styringsparameter over til flere aktivitetskrav (Kommunal- og moderniseringsdepartementet, 2020, s. 15).

Økning og/eller et høyt antall aktivitetskrav er ofte et uttrykk for detaljstyring, og kan også identifisere en styring som i stedet for å være målstyring etter intensjonen og kravet, i stedet er nærmere oppdrag og aktivitetsstyring. Gitt den kompleksitet som forbindes med IKT-sikkerhet og trusler i cyberdomenet kan dette tyde på at vår hypotese (hypotese 1 A) om at nettopp kompleksitet og utvikling i cyberdomenet preger styringsutøvelsen og bidrar til økt grad av detaljstyring relatert til IKT-sikkerhet.

En annen faktor som kan vise seg relevant i arbeidet med å forklare tallene er prinsipal-agentteori. Det kan tenkes at det er usikkerhet fra departementet knyttet til hvorvidt arbeidet med IKT-sikkerhet følges opp etter intensjon så lenge man ikke eksplisitt og tydelig fremmer

krav til handling fra underliggende virksomhet. Det kan tenkes at vektingen mellom kontroll og handlingsrom bidrar til at det er krevende å utøve styring relatert til IKT-sikkerhet.

5.2.2 Grad av detaljstyring fra Olje- og energidepartementet til Norges vassdrags- og energidirektorat

Det faktum at man ser en nedgang i mål relatert til IKT-sikkerhet i perioden 2014-2022 er et interessant funn. Særlig i lys av etterretnings- og sikkerhetsmyndighetenes tiltakende fokus på IKT-sikkerhet i de årlige trusselvurderingene for samme periode. Dermed tegner det seg et bilde av at det ikke foreligger noen klar sammenheng mellom trusselvurderinger og styringsutøvelse. Det bemerkes dog at påstanden isolert kan fremstå unyansert og at det vil være avgjørende å se dette opp imot den helhetlige analysen av det undersøkte materialet.

At det foreligger en økning i antallet aktivitetskrav er på den andre siden noe som kan tenkes å avkrefte antagelsen om fravær av sammenheng mellom trusselvurderinger og styringsutøvelse. Det gjør det dog mer interessant å se nærmere på styringsutøvelsen eksplisitt. Dette ettersom det kan være med å gi en mer nyansert forståelse av om det foreligger en endring eller fravær av styring med fokus på denne typen utfordringer eller om det heller er selve styringsmåten (mindre/mer detaljstyring) som har endret seg og som således kommer til uttrykk i tallene vi finner.

Det faktum at 2011 og 2012 skiller seg markant ut fra de i andre i første halvdel av den angitte perioden datasettet tar for seg er interessant. At det i perioden 2013 til 2020 kun foreligger ett mål, uspesifikt som sådan, for hele perioden kan umiddelbart tenkes å ha sammenheng med lav grad av detaljstyring, og oppmerksomhet på IKT-sikkerhet fra departementets side. På den andre siden kan det være et uttrykk for tillit til, og en forventing om, at underliggende virksomhet selv ivaretar denne problemstillingen på en tilstrekkelig god måte og i tråd med de forventninger som kommer frem av det uspesifikke kravet. En tilnærming og forståelse som vil være i overenstemmelse med forvalterteori, hvor man antar at underliggende virksomheter (agent) har til hensikt å gjøre det departementet (prinsipalen) ønsker.

Som redegjort for i kapittel 4 skriver departementet at et hovedmål for Norges vassdrags- og energidirektorat skal være å «fremme en sikker kraftforsyning» med delmål om at de videre skal «påse at beredskapen i kraftforsyningen er god og i tråd med gjeldende krav». Bruken av «gjeldende krav» fremstår her uspesifikt og lite detaljstyrende, samtidig som dette for Norges

vassdrags- og energidirektorat vil bety at de må se hen til øvrige styringsverktøy, som for eksempel lover, regler og forskrifter som setter krav til nettopp beredskap og deres ansvar for en sikker kraftforsyning. Slik lovgivning kan som nevnt i kapittel 3 helt konkret være Sikkerhetsloven med flere. Dette er et godt eksempel på hvordan departementet benytter seg av regelstyring.

Når denne praksisen endres i siste periode, 2020-2023, hvor målene både blir mer spesifikke og flere, kan dette tenkes å ha sammenheng med både den kontinuerlige utviklingen som har pågått innenfor IKT-sikkerhetsarbeidet, de mange hendelser som har funnet sted i årene forut, og etterretnings- og sikkerhetsmyndighetenes fokus på dette feltet. I tillegg finner vi for første, og eneste gang i det analyserte materialet at Olje- og energidepartementet understøtter disse prioriteringene ved å bevilge penger (budsjettstyre) til Norges vassdrags- og energidirektorat i 2023 for å øke beredskapen mot cyberangrep i kraftforsyningen. Dette står i kontrast til Johnsen (2007, s. 106) sin beskrivelse av at færre øremerkede midler vil være en måte å redusere føringene (detaljstyringen) på. Her skjer det motsatte ved at det bevilges øremerkede midler, hvilket kan være et argument for økt detaljstyring.

Når det gjelder bruken av styringsparameter for årene 2011 og 2012 er det påfallende at disse er ikke-eksisterende gitt at det foreligger flere mål i samme periode. At vi i tillegg finner ett styringsparameter per år i perioden 2014-2023 kan umiddelbart synes å virke noe lavt hvis man tenker på styringsparameter som en funksjon som delmål og indikator. Dette kan dog være et tegn på lav grad av involvering fra departementet og høy tillit til den underliggende virksomheten ref. forvalterteori. I forlengelsen av denne påstanden er det relevant å nevne at Olje- og energidepartementet i forbindelse med *Tillitsreformen,* hvor et av målene er mindre detaljstyring og økt handlingsrom til virksomhetene (Kommunal- og distriktsdepartementet, 2022, s. 4), blant annet har satt seg ambisjon om å forenkle rapporteringen fra underliggende virksomheter. I tilknytning til dette ba Olje- og energidepartementet samtlige underliggende virksomheter om å gå igjennom mål, rapporteringskrav og resultatoppfølging for å identifisere forbedringspunkter i forbindelse med utarbeidelsen av tildelingsbrevene for 2023 (Kommunal- og distriktsdepartementet, 2023, s. 28). Det er mulig det er dette vi finner antydninger av i det siste året for undersøkt tidsperiode. Det er på det rene at styringsparameter oppleves som krevende å utforme hvilket kan tenkes å være en medvirkende årsak til det lave antallet, særlig i en periode hvor fokus på IKT-sikkerhet stadig er økende jf. datasettet for antall mål.

Som tidligere drøftet vet vi at bruken av aktivitetskrav ofte kan sees i sammenheng med økt grad av kontroll og dermed detaljstyring. Konsistensen i styringsutøvelsen og bruken av aktivitetskrav som omhandler IKT-sikkerhet, både spesifikt og uspesifikt, kan være et uttrykk for at fokus på denne typen problemstillinger har vedvart over tid. Økningen av IKT-spesifikke aktivitetskrav i perioden 2020-2023 er signifikant og kan dermed være et uttrykk for et stort fokus på denne typen problemstillinger.

Som beskrevet i kapittel 4 var det flere cyberangrep mot norske virksomheter i perioden 2018-2022 noe som kan tenkes å være en medvirkende årsak til styringsutøvelsen. Av relevante eksempler er blant annet de to angrepene på Stortinget i henholdsvis 2020 og 2021. Dette er konkrete hendelser som fikk mye oppmerksomhet i media og som i tråd med Pollit og Boucards (2017) teori kan ha vært toneangivende for den videre styringen.

En annen faktor som kan bidra til å forklare økt bruk av aktivitetskrav relaterer seg til graden av kompleksitet. Man ser av teorien at det foreligger en sammenheng mellom detaljstyring og graden av kompleksitet man står ovenfor. Det kan også argumenteres for at man ovenfor denne typen problemstillinger ser konturene av det som i agentteorien beskrives som delegeringsproblemet, at departementet ikke har tillit til at Norges vassdrags- og energidirektorat følger opp i tråd med intensjonen deres.

5.3 Norges vassdrags- og energidirektorat detaljstyres i større grad enn Folkehelseinstituttet

I kapittel 2.4 lanserte vi en hypotese om at *det foreligger en ulikhet/skjevhet i styringsutøvelsen av underliggende virksomheter i tråd med teorien om at direktorater tenderer mot å være mer detaljstyrt enn andre underliggende forvaltningsorgan* (hypotese 2). Altså at Olje- og energidepartementet ville være mer detaljstyrende overfor Norges vassdrags- og energidirektorat sammenlignet med hva tilfellet ville være for Helse- og omsorgsdepartementet opp imot Folkehelseinstituttet.

Med 70 styringskrav fra Olje- og energidepartementet til Norges vassdrags- og energidirektorat mot 53 fra Helse- og omsorgsdepartementet til Folkehelseinstituttet, ser denne hypotesen ut til å få støtte av de totale tallene vi her legger til grunn. I tillegg peker vi i kapittel 4.2 på at Olje- og energidepartementet jevnt over utformer lengre tildelingsbrev enn Helse- og omsorgsdepartementet. Våre analyser viser at de i gjennomsnitt har 15,8 sider per tildelingsbrev, hvilket er 1,5 sider mer i gjennomsnitt enn det Helse- og omsorgsdepartementet

har. Dette kan ha ulike forklaringsfaktorer, blant annet virksomhetens egenart, hvilket kan, som forklart i kapittel 2, gjøre at departementene har ulike behov knyttet til styringsdokumenter. Det er også interessant å observere at Olje- og energidepartementet i tildelingsbrevet for 2023 budsjettstyrer Norges vassdrags- og energidirektorat ved å bevilge penger til IKT-spesifikke formål, hvilket er med på å underbygge en økt detaljstyring.

5.4 Er det korrelasjon mellom utvikling i nasjonalt trusselbilde og styringsutøvelsen?

I kapittel 2.6 fremmer vi oppgavens fjerde og siste hypotese: *det er liten grad av korrelasjon mellom utviklingen i nasjonalt trusselbildet og den styringsutøvelse som kommer frem av departementenes årlige tildelingsbrev til underliggende virksomheter.* Hypotesen stilles på bakgrunn av hvordan både PST og E-tjenesten i sine trusselvurderinger i økt grad beskriver og omtaler digitale trusler, samt den generelle kritikken som rettes fra NSM vedrørende norske virksomheters evne til å ta denne utviklingen tilstrekkelig på alvor.

Ved å sammenligne endringene i trusselbildet, og hvordan etterretnings- og sikkerhetsmyndighetene i større grad beskriver og vier oppmerksomhet til cybertrusselen i rapportenes oppbygning år for år, med Helse- og omsorgsdepartementets og Olje- og energidepartementets styring av Folkehelseinstituttet og Norges vassdrags- og energidirektorat ser vi at fokuset er relativt likt.

I kapittel 5.2 har vi drøftet hvordan de to departementene benytter seg av mål, styringsparameter og aktivitetskrav, og vi har diskutert utviklingen og bruken av disse styringssignalene, og hvorvidt de har fremstått IKT-spesifikke eller av mer generell karakter; IKT-uspesifikke. Styringssignalene benyttes ulikt i tidsperioden, men rent overordnet ser vi at styringen følger utviklingen i trusselbildet, særlig fra 2016-2017 og ut den undersøkte tidsperioden. I 2020 har vi blant annet belyst at Helse- og omsorgsdepartementet stiller flest mål knyttet til IKT-sikkerhet, og at et av disse målene setter krav om at Folkehelseinstituttet skal planlegge og gjennomføre en øvelse med *IKT-scenario*. Gitt de eksempler på cyberangrep som fremmes i kapittel 4, hvor det blant annet henvises til angrepet på Norsk Hydro i 2019, er dette et interessant funn å se i sammenheng. Angrepet på Norsk Hydro er omtalt som «Norges største datakrim sak» (Schjetne, 2023), og var av en slik karakter at det genererte massiv medieoppmerksomhet, også utenfor Norges landegrenser. I tråd med Pollitt og Bouckaerts (2017, s. 40) teori omkring medias og store hendelsers influering på styring kan det ikke utelukkes at det er en sammenheng med den utvikling som her beskrives.

Videre trekker blant annet PST flere ganger frem hvordan virksomheter innenfor norsk statsforvaltning og med ansvar for kritisk infrastruktur kan være utsatte etterretningsmål, og derfor må sørge for god datasikkerhet og oversikt over egen nettverksstruktur. Våre funn viser blant annet at Olje- og energidepartementet allerede i 2012 skrev i tildelingsbrevet til Norges vassdrags- og energidirektorat at de skulle utrede og stille krav til kraftforsyningens økende avhengighet av IKT og de sikkerhetsmessige utfordringer dette medfører.

Som nevnt i kapittel 4 har etterretnings- og sikkerhetsmyndighetene hatt stort fokus på hvilke trusler økt digitalisering medfører. Dette kan være en medvirkende faktor til gradvis endring i styring over tid, og det må på bakgrunn av våre analyser kunne sies at det er korrelasjon mellom utviklingen i nasjonalt trusselbildets fokus på trusler i cyberdomenet, og den styringsutøvelse som gjenspeiles i departementenes årlige tildelingsbrev til underliggende virksomheter. Vår fjerde hypotese får således ikke støtte av våre funn. Våre analyser viser at Helse- og omsorgsdepartementet og Olje- og energidepartementet gjør noe med problematikken som ligger i de trusler som fremgår av cyberdomenet ref. vår henvisning til Thomas Dye (1972) i kapittel 2 hvor politikk beskrives som «det myndighetene velger å gjøre, samt det de velger å ikke gjøre».

At Norges vassdrags- og energidirektorat var utsatt for flere aktivitetskrav i perioden 2011-2014 sammenliknet med perioden 2015-2019 korrelerer i liten grad med den lineære utviklingen vi har sett når det gjelder fokus på IKT-sikkerhet i det nasjonale trusselbildet. Det kan dog tenkes at den oppmerksomhet som over flere år har blitt viet risiko knyttet til kraftforsyning har medført at både Olje- og energidepartementet og Norges vassdrags- og energidirektorat har vært lengre fremme og «forut for sin tid».

6 Konklusjon

6.1 Hovedfunn

I denne oppgaven har vi forsøkt å kartlegge og analysere hvorvidt Helse- og omsorgsdepartementet og Olje- og energidepartementet utøver styring av Folkehelseinstituttet og Norges vassdrags- og energidirektorat relatert til IKT-sikkerhet og utviklingen i nasjonalt trusselbilde gjennom sine årlige tildelingsbrev i perioden 2011-2023 eller ikke. Vi har undersøkt tildelingsbrevets rolle i departementenes styring, og hvorvidt disse benyttes til å fremme relevante mål, styringsparameter og aktivitetskrav. Videre har vi vært interessert i å belyse hvorvidt kravene har gitt utslag av å være IKT-spesifikke eller IKT-uspesifikke.

Innenfor det analyserte tidsrommet er det tydelig at NSM, som ansvarlig fagmyndighet for forebyggende sikkerhet har fokusert på utfordringer ved vårt stadig mer digitaliserte samfunn, samt mangel på forebyggende tiltak i ulike virksomheter. NSM viser tidlig at man i takt med digitaliseringen skaper nye avhengigheter, som igjen gjør oss som nasjon sårbare. Samtidig viser vår analyse at måten rapportene kommuniserer på har blitt enda mer spesifikke, med henvisninger til at det blant annet aldri har vært viktigere å beskytte Norge mot trusler i cyberdomenet (NSM, 2022a, avsn. 1).

Analysen av etterretnings- og sikkerhetsmyndighetene sine trusselvurderinger bekreftet at trusselbildet i Norge gjennom de siste 13 årene har vært preget av et økende fokus på trusler i cyberdomenet. I samme tidsperioden har det vært flere cyberangrep, både store og små, mot norske virksomheter. At hendelsene er med på å prege trusselvurderingene er det ingen tvil om, og svarer derfor ut hypotese 3 om at cyberangrep som har rammet norske virksomheter har hatt en påvirkende faktor på etterretnings- og sikkerhetsmyndighetenes fokus på dette feltet innenfor den analyserte tidsperioden.

Ifølge NSM må bevisstheten rundt trusselbildet i cyberdomenet økes hos «alle», samtidig som de gir uttrykk for at norske virksomheter ikke tar situasjonen alvorlig nok. Vår analyse viser derimot at det foreligger en samvarians mellom utviklingen man har sett i trusselvurderingene og styringsutøvelsen som uttrykkes gjennom tildelingsbrevene fra Helse- og omsorgsdepartementet og Olje- og energidepartementet i tidsperioden 2011-2023, og at disse departementene således er sitt ansvar bevisst når det gjelder kravene til å følge opp samfunnssikkerhet (inkludert digital sikkerhet) innenfor egen sektor ref. kravene som fremgår av Samfunnssikkerhetsinstruksen (Samfunnssikkerhetsinstruksen, 2017). Man bør dog være

varsom med å trekke generaliserende konklusjoner med utgangspunkt i det undersøkte datamaterialet. Samvariansen viser som beskrevet i kapittel 3 en mulig forklaring, men tar ikke høyde for alle variabler (mulige årsakssammenhenger). Økt fokus på IKT kan knytte seg til andre forklaringsfaktorer, blant annet økt fokus på sikkerhet generelt.

At styringsdialogen har hatt økt fokus på IKT-sikkerhet i de siste årene er i takt med etterretnings- og sikkerhetsmyndighetenes økte fokus på cybertrusselen, og avkrefter således påstander om at styringsmyndighetene ikke tar IKT-sikkerhet på alvor. Hypotesen om at det er liten grad av korrelasjon mellom utviklingen i nasjonalt trusselbildet og den styringsutøvelse som kommer frem av departementenes årlige tildelingsbrev til underliggende virksomheter er derfor feil. Det er dog viktig å understreke at selv om årlige trusselvurderinger ser ut til å bli hensyntatt i styringen så er ikke det ensbetydende med at styringsutøvelsen er god og effektfull opp mot et digitalt trusselbilde i rask utvikling.

Videre tegner styringsutøvelsen et bilde av at styring av IKT-sikkerhet i Helse- og omsorgssektoren og Olje- og energisektoren preges av å være detaljorientert, spesielt i de siste årene. I oppgaven har det blitt lansert to motstridende hypoteser; 1 A) at kompleksitet og utvikling i cyberdomenet preger styringsutøvelsen og bidrar til økt grad av detaljstyring relatert til IKT-sikkerhet. Og, 1 B), at kritikken av departementenes detaljstyring i perioden etter 2010 preger styringsutøvelsen og gjør seg gjeldende gjennom færre krav knyttet til IKT-sikkerhet jo nærmere vi kommer dags dato.

Analysen viser at det i begge departementene i stor grad følges samme trend; i første halvdel av analysert tidsperiode fremmes det flere mål enn aktivitetskrav, mens det i andre halvdel av tidsperioden er omvendt. Analysene viser også at andre halvdel av tidsperioden inneholder enda flere krav enn den første. Det tegner seg dermed et bilde av at detaljstyringen øker, og at hypotese 1 A dermed styrkes, mens hypotese 1 B svekkes. Hvorfor det er slik kan ikke bekreftes hundre prosent, men det er naturlig å tenke seg at nettopp kompleksitet og utviklingen i cyberdomenet er en medvirkende faktor. Dette er også noe som kan underbygges av Totalberedskapskommisjonen ferske rapport hvor det påpekes at blant annet risiko og sårbarheter i kompleks teknologi og sammenkoblete systemer som gjerne driftes av internasjonale teknologiselskaper gjør fagområdet utfordrende å arbeide med (NOU 2023: 17, 2023, s. 34).

Til slutt er det på det rene at det er enkelte ulikheter i styringsutøvelse til de to departementene. For det første er det noe ulikt hvorledes de utformer sine tildelingsbrev. Olje- og energidepartementet har jevnt over lengre tildelingsbrev i den undersøkte tidsperioden, i tillegg til at departementet har langt flere kapitler i sine brev sammenliknet med Helse- og omsorgsdepartementet. Våre undersøkelser viser også at Olje- og energidepartementet totalt stiller flere krav relatert til IKT enn Helse- og omsorgsdepartementet, og dermed er mer detaljstyrende. Dette er med på å underbygge og bekrefte hypotese 2 om at det foreligger en ulikhet/skjevhet i styringsutøvelsen av underliggende virksomheter i tråd med funnene til Kjærvik & Askim (2015, s. 13) som konkluderte med at direktorater tenderer mot å være mer detaljstyrt enn andre underliggende forvaltningsorgan.

6.2 Begrensninger og videre forskning

Som Mulgan (2009) refereres til i kapittel 2 har offentlig styring stor påvirkning på folks liv, blant annet gjennom sitt potensiale til å påvirke og forhindre kriminalitet (henvist i Johnsen, 2014, s. 274). NSM har de siste årene registrert en stor økning i antallet cyberangrep, og har uttalt at om lag 80 prosent av de hendelsene de håndterer kunne vært unngått om grunnleggende sikkerhetstiltak hadde blitt fulgt (St.meld. nr. 9 (2022-2023), s. 13). Det er derfor viktig å fortsette arbeidet med å øke bevisstgjøringen rundt denne typen trusler, og styrke det forebyggende arbeidet.

I arbeidet med denne analysen har det i takt med funn dukket opp flere spørsmål som vi gjerne skulle fulgt opp gjennom videre forskning. Det mest nærliggende er å gjøre de samme undersøkelsene på samtlige departementer og underliggende virksomheter. Videre ville det være svært interessant å løfte blikket ytterligere, og se enda bredere på departementenes styringsutøvelse. Dette med intensjon om å avdekke om det er konsistens i de øvrige styringssignaler man tar i bruk. Det være seg gjennom instruksverk, etatsstyringsmøter etc. Å kombinere dokumentstudier med intervjuer av sentrale personer innenfor etatsstyringen både i departementene og i de underliggende virksomhetene mener vi at kan gi ytterligere verdifull innsikt.

Fra et teoretisk perspektiv er det flere innfallsvinkler som er interessante, og som ble vurdert, men utelatt som følge av oppgavens rammer når det gjelder omfang. Blant annet ville det vært interessant å se problemstillingen i sammenheng med samtlige faktorer som Pollit og Bouckaert

trekker frem som relevante for hvordan styring utøves. Eksempelvis ville «eliters beslutninger» og hvorvidt det foreligger forskjeller mellom konservative og liberale sider av politikken (les: regjeringsskifter) være aktuelt å analysere mer inngående (Pollitt & Bouckaert, 2017, ss. 32-33). Dette kan tenkes å ha innvirkning på den faktiske styringsutøvelsen knyttet til IKT-sikkerhet.

Videre kan man dra det enda lengre ved å se på hvordan vi best kan ruste oss mot trusler i cyberdomenet i samarbeid med våre naboland, eksempelvis Sverige, Danmark og Finland. Kanskje er det gjensidige læringspunkter. I tillegg bør det ses hen til øvrige allierte, eksempelvis NATO, og hvorvidt det er større behov for et internasjonalt samarbeid og samordning i cybersikkerhetsspørsmålet. Dette er i tråd med anbefaling om at Norge er avhengig av et sterkt internasjonalt samarbeid i møte med cybertrusler, hvor NATO og EU nevnes som Norges viktigste samarbeidspartnere opp imot denne typen sikkerhetspolitiske spørsmål (NSM, 2023, s. 7) .

Ifølge DSBs befolkningsundersøkelse for 2023 er en av tre nordmenn bekymret for å bli berørt av en større krise, og cyberangrep på styringssystemer trekkes frem som det nordmenn flest (46 %) er aller mest bekymret for at skal inntreffe de neste fem årene (Ispos, 2023, s. 6). Det er ingen tvil om at Mulgan (2009) har rett når han beskriver at offentlig strategisk styring har stor påvirkning, blant annet gjennom sitt potensiale til å påvirke og forhindre kriminalitet (henvist i Johnsen, 2014, s. 274). For å få til dette i en tid hvor samfunnssikkerheten og det sikkerhetspolitiske landskapet endrer seg raskt må det forskes videre på hvordan vi som nasjon møter trusler i cyberdomenet best mulig.

Vi har ingen tid å miste; *fremtiden er nå.*

Referanser

Arvesen, O. J. (2020). *Skjevt ut fra hoppkanten? Myndighetenes organisering av sikkerhet i cyberdomenet [Masteroppgave].* Forsvarets høgskole. Hentet Oktober 14, 2022 fra https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2716038/2020-10-15%20%28U%29%20Masteroppgave%20Arvesen.pdf?sequence=1&isAllowed=y

Asdal, K., & Reinertsen, H. (2020). *Hvordan gjøre dokumentanalyse - en praksisorientert metode.* Oslo: Cappelen Damm AS.

Bjurstrøm, K. H. (2020). *Principales and agents or principals and stewards? Performance management of agencies in Norwegian state administration [Doktorgradsavhandling].* Universitetet i Oslo.

Bjurstrøm, K. H. (2021, Januar 27). Mål- og resultatstyring og tillitsbasert styring: ulike alternativer eller kunstige motsetninger. *Nordisk administrativt tidsskrift*. Hentet Juni 1, 2023 fra https://doi.org/10.7577/nat.4563

Byrkjeflot, H. (1997). *Fra styring til ledelse.* Bergen: Fagbokforlaget.

Christensen, T., & Lægreid, P. (2007). Regulatory Agencies- The Challenges of Balancing Agency Autonomy and Political Control. *Governance*. https://doi.org/10.1111/j.1468/0491.2007.00368.x

Christensen, T., Egeberg, M., Lægreid, P., Roness, P. G., & Røvik, K. (2015). *Organisasjonsteori for offentlig sektor* (3. utg.). Universitetsforlaget.

Davis, J. H., Schoorman, D. F., & Donaldson, L. (1997). *Toward a Stewardship Theory of Management.* The Academy of Management review. https://doi.org/10.2307/259223

Departementene. (2019). *Nasjonal strategi for digital sikkerhet.* Regjeringen. Hentet Desember 8, 2022 fra https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

DFØ. (2020, Mars). *Veileder i etatsstyring*. Hentet Mars 7, 2023 fra https://dfo.no/fagomrader/etats-og-virksomhetsstyring/etatsstyring/veileder-i-etatsstyring

DFØ. (2023a, Januar 22). *Hva er mål- og resultatstyring*. Hentet Februar 10, 2023 fra https://dfo.no/fagomrader/etats-og-virksomhetsstyring/mal-og-resultatstyring/hva-er-mal-og-resultatstyring#:~:text=M%C3%A5l-%20og%20resultatstyring%20%28MRS%29%20er%20en%20metode%20eller,der%20det%20er%20aktuelt%20%C3%A5%20styre%20mot%20m%C3%A5l.

DFØ. (2023b, Januar 22). *Hvilke krav gjelder for mål- og resultatstyring i staten?* Hentet Juli 7, 2023 fra https://dfo.no/fagomrader/etats-og-virksomhetsstyring/mal-og-resultatstyring/hvilke-krav-gjelder-mal-og-resultatstyring-i-staten

DFØ. (2023c, Januar 22). *Sjekklister for tildelingsbrev*. Hentet November 9, 2023 fra https://dfo.no/fagomrader/etats-og-virksomhetsstyring/etatsstyring/sjekklister-tildelingsbrev

DSB. (2016). *Samfunnets kritiske funksjoner.* Direktoratet for samfunnssikkerhet og beredskap. Hentet Mars 7, 2023 fra https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

DSB. (2019). *Analyser av krisescenarioer 2019.* Direktoratet for samfunnssikkerhet og beredskap. Hentet Desember 8, 2022 fra https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

Eisenhardt, K. M. (1989). *Agency Theory: An Assessment and Review.* The Academy of Management review. https://doi.org/10.2307/258191

E-tjenesten. (2022, Oktober 7). *Om Etterretningstjenesten*. Hentet Januar 7, 2023 fra https://www.etterretningstjenesten.no/om-oss/vanlige-sporsmal

Etterretningstjenesten. (2015). *Fokus.* Hentet Mars 3, 2023 fra https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus%202015.pdf/_/attachment/inline/66fd7ac2-3601-4a99-965a-05d22e59e7cb:4ea88245ef7a52d712a0ff850de0402918ed521a/Fokus%202015.pdf

European Commission. (2022, Juli 28). *Digital Economy and Society Index (DESI) 2022 Norway.* Hentet Mars 15, 2023 fra file:///C:/Users/LMD5788/Downloads/DESI_2022__Norway__eng_75V8QcGT6KC53tEy1zS0Xfhuxi8_88980%20(2).pdf

Finansdepartementet. (2022, Desember 20). Reglement for økonomistyring i staten . Hentet Mai 10, 2023 fra https://www.regjeringen.no/globalassets/upload/fin/vedlegg/okstyring/reglement_for_okonomistyring_i_staten.pdf

Grønmo, S. (2004). *Samfunnsvitenskapelige metoder.* Fagbokforlaget.

Helse- og omsorgsdepartementet. (2015). *Instruks for Folkehelseinstituttet fastsatt av Helse- og omsorgsdepartementet 17.12.2015.* Hentet Juli 26, 2023 fra https://www.regjeringen.no/globalassets/departementene/hod/tildeling-oppdrag-og-arsrapporter/instrukser/hovedinstruks-fhi.pdf

Hood, C. (1991). A public management for all seasons? *Public Administration*. https://doi.org/10.1111/j.1467-9299.1991.tb00779.x

Howlett, M. (2011). *Designing Public Policies.* Routledge .

Ispos. (2023). *Befolkningsundersøkelse: Om norske husholdningers bevissthet og atferd knyttet til egenberedskap.* DSB. Hentet Mars 15, 2023 fra https://www.dsb.no/globalassets/dokumenter/egenberedskap/egenberedskap-2023/rapport---husholdningens-egenberedskap-2023_med-viken.pdf

Johannessen, A., Tufte, P., & Christoffersen, L. (2015). *Introduksjon til samfunnsvitenskapelig metode.* Abstrakt forlag.

Johnsen, Å. (2007). *Resultatstyring i offentlig sektor.* Fagbokforlaget.

Johnsen, Å. (2014). *En strategisk offentlig sektor.* Fagbokforlaget Vigmostad & Bjørke AS.

Johnsen, Å. (2015, Juni 10). For mye detaljstyring, og for lite målstyring. *Stat og styring*. Hentet Mai 22, 2023 fra https://www.idunn.no/doi/10.18261/ISSN0809-750X-2015-02-15

Kjærvik, J., & Askim, J. (2015). *Etatsstyring i praksis: En kartlegging av departementenes målstyring av underliggende virksomheter.* Hentet Mars 16, 2023 fra https://www.slideshare.net/JonasKjrvik/etatsstyringipraksisenkartleggingavdepartementenesmlstyringavunderliggendevirksomheter

Kommunal- og distriktsdepartementet. (2022). *Om tillitsreformen.* Hentet November 23, 2023 fra

https://www.regjeringen.no/contentassets/c93c9caad6d44466bff45b8fd6b85ed2/no/pdfs/h-2535-om-tillitsreformen.pdf

Kommunal- og distriktsdepartementet. (2023). *Tillitsreformen - Eksempler på tiltak.* Hentet Juli 27, 2023 fra https://www.regjeringen.no/contentassets/f83d579eaa1f4ce485270b875d2d848d/oppdatert_-tillitsreformen-tiltaksoversikt-per-27-juni-2023.pdf

Kommunal- og moderniseringsdepartementet. (2018). *Program for bedre styring og ledelse i staten 2014-2017.* Hentet Mai 6, 2023 fra https://files.nettsteder.regjeringen.no/wpuploads01/blogs.dir/90/files/2018/04/Program-for-bedre-styring-og-ledelse-sluttrapport-endelig.pdf

Kommunal- og moderniseringsdepartementet. (2020). *Etatsstyring i praksis: En analyse av departementenes tildelingsbrev til underliggende virksomheter (2012-2020).* Hentet November 17, 2022 fra https://www.regjeringen.no/contentassets/6f762ceef1c24afba42b28a5ca3b0694/etatsstyring-i-praksis_en-analyse-av-departementenes-tildelingsbrev.pdf

Ladegård, G., & Vabo, S. I. (2010). *Ledelse og styring.* Fagbokforlaget.

NHO. (2022). *Cyber insurance*. Hentet Mars 6, 2023 fra https://www.nho.no/en/nho-membership/nho-insurance/cyber-insurance2/

NOU 2023: 17. (2023). *Nå er det alvor.* Justis- og beredskapsdepartementet.

NSM. (u.d.). Hentet Januar 7, 2023 fra Dette er NSM: https://nsm.no/om-oss/dette-er-nsm/

NSM. (2012). *Rapport om sikkerhetstilstanden 2011.* Nasjonal sikkerhetsmyndighet. Hentet Januar 7, 2023 fra https://nsm.no/getfile.php/133753-1592918149/NSM/Filer/Dokumenter/Rapporter/rst_2011.pdf

NSM. (2022a, Februar 11). *Pressemelding: Vi trenger årvåkne ledere*. Hentet Mars 1, 2023 fra https://nsm.no/aktuelt/pressemelding-vi-trenger-arvakne-ledere

NSM. (2022b). *Risiko.* Hentet Mars 1, 2023 fra https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

NSM. (2023). *Sikkerhetsfaglig råd - Et motstandsdyktig Norge.* Hentet November 22, 2023 fra https://nsm.no/getfile.php/1312994-1683615611/NSM/Filer/Dokumenter/Rapporter/Sikkerhetsfaglig%20r%C3%A5d%20-%20Et%20motstandsdyktig%20Norge.pdf

NTB. (2021, Desember 28). *Amedia utsatt for et alvorlig dataangrep*. Hentet Mars 7, 2023 fra https://kommunikasjon.ntb.no/pressemelding/amedia-utsatt-for-et-alvorlig-dataangrep?publisherId=11014241&releaseId=17923402

NVE. (2022). *Risikostyring av IKT-sikkerhet i leverandørkjeder.* Hentet August 8, 2023 fra https://publikasjoner.nve.no/eksternrapport/2022/eksternrapport2022_17.pdf

NVE. (2023, Juni 8). *Kraftforsyningsberedskap og KBO*. Hentet August 8, 2023 fra https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/

Olje- og energidepartementet. (2020). *Instruks for økonomi- og virksomhetsstyring i Norges vassdrags- og energidirektorat.* Hentet Juli 26, 2023 fra https://www.regjeringen.no/contentassets/267dd4d3be4342ca8f34e96325a7ad84/instruks-for-okonomi--og-virksomhetsstyring-i-nve.pdf

Pollitt, C., & Bouckaert, G. (2017). Problems and responses: A process model of public management reform. I *Public management reform: a comparative analysis-into the age of austerity.* United Kingdom: Oxford University Press.

PST. (2011, Februar 1). *Trusselvurdering 2011*. Hentet Januar 7, 2023 fra https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2011/

PST. (2019). *Trusselvurdering 2019.* Politiets sikkerhetstjeneste. Hentet Desember 7, 2022 fra https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

PST. (2020a, Desember 8). *Datainnbruddet mot Stortinget er ferdig etterforsket*. Hentet Mars 7, 2023 fra https://pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

PST. (2020b). *Nasjonal trusselvurdering 2020.* Politiets sikkerhetstjeneste. Hentet Desember 7, 2022 fra

https://www.pst.no/globalassets/artikler/utgivelser/2020/pst_trusselvurdering_2020.pdf

PST. (u.d.). *Dette gjør vi*. Hentet Mars 16, 2023 fra https://www.pst.no/alle-artikler/artikler/dette-gjor-vi/

PwC. (2020). *Etatsstyring i praksis.* Hentet Mars 6, 2023 fra https://dfo.no/sites/default/files/fagomr%C3%A5der/Rapporter/2021/Etatsstyring-i-praksis-en-komparativ-studie.pdf

Regjeringen.no. (2021, Juli 20). *Drikkevann*. Hentet August 8, 2023 fra https://www.regjeringen.no/no/tema/helse-og-omsorg/folkehelse/innsikt/ernaring-og-mattrygghet/mattrygghet-og-drikkevann/id448370/

Riksrevisjonen. (2023). *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor.* Hentet November 21, 2023 fra https://www.riksrevisjonen.no/globalassets/rapporter/NO-2022-2023/myndighetenes-samordning-av-arbeidet-med-digital-sikkerhet-i-sivil-sektor.pdf

Røiseland, A., & Vabo, S. (2016). *Styring og samstyring - governance på norsk.* Bergen: Fagbokforlaget.

Samfunnssikkerhetsinstruksen. (2017). Instruks for departmentenes arbeid med samfunnssikkerhet. *FOR-2017-09-01-1349*. Lovdata. Hentet Mars 3, 2023 fra https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349

Schjetne, S. (2023, Mai 25). Kripos mener å ha oppklart løsepenge-angrepet mot Hydro. *E24*. Hentet November 28, 2023 fra https://e24.no/naeringsliv/i/EQ5m6K/kripos-mener-aa-ha-oppklart-loesepenge-angrepet-mot-hydro

Sikt. (2023, Juni 21). Statsråder 2010-2023. Hentet fra https://filesender.sikt.no/?s=download&token=e4e4ff4d-1af6-47d4-b693-3fc2c949467d

SSØ. (2006). *Mål- og resultatstyring i staten . En veileder i resultatmåling.* SSØ. Hentet August 8, 2023 fra https://www.regjeringen.no/globalassets/upload/kd/vedlegg/fagerbergutvalget/veileder_resultatmaaling.pdf

Statistisk sentralbyrå. (2022, September 19). *Bruk av IKT i husholdningene*. Hentet Februar 28, 2023 fra https://www.ssb.no/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/bruk-av-ikt-i-husholdningene

Stolt-Nielsen, H., & Lysberg, M. (2021, Oktober 29). Dataangrepet kostet Hydro 800 millioner kroner. Nå er det kriminelle nettverket avdekket. *Aftenposten*. Hentet Mars 3, 2023 fra https://www.aftenposten.no/norge/i/47WR3o/dataangrepet-kostet-hydro-800-millioner-kroner-naa-er-det-kriminelle-nettverket-avdekket

Stortingsmelding [St.meld.] nr. 9 (2022-2023). (u.d.). *Nasjonal kontroll og digital motstandskraft.* Justis- og beredskapsdepartementet. Hentet Mars 15, 2023 fra https://www.regjeringen.no/contentassets/d256b455415c4cae8a710f62cc97d4f9/no/pdfs/stm202220230009000dddpdfs.pdf

Thurén, T. (2009). *Vitenskapsteori for nybegynnere* (2.. utg.). Gyldendal akademisk.

Østby, G., & Kowalski, S. J. (2022). *Hendelseshåndtering ved cyberangrepet mot Østre Toten kommune.* NTNU. Hentet Mars 7, 2023 fra https://www.ototen.no/_f/p1/idbd37a14-f91f-41e5-9fa2-14977f2a7977/v-10-ostre-toten.pdf

Figurliste

Tabelliste

Vedlegg

1. Analyserte trusselvurderinger inkludert utgiver, dokumenttittel, publiseringsdato og antall sider
2. Analyserte tildelingsbrev inkludert avsender/mottaker, brevtittel, referansekode, brevdato, og antall sider

Vedlegg 1:

Analyserte trusselvurderinger inkludert utgiver, dokumenttittel, publiseringsdato og antall sider.

Dok.nr	Utgiver	Dokumenttittel	Dato[8]	Antall sider[9]
1.	PST	Trusselvurdering 2011	01.02.2011	-
2.	PST	Trusselvurdering 2012	06.02.2012	-
3.	PST	Åpen trusselvurdering 2013	09.04.2013	-
4.	PST	Åpen trusselvurdering 2014	04.04.2014	-
5.	PST	Åpen trusselvurdering 2015	04.02.2015	-
6.	PST	Trusselvurdering 2016	09.02.2016	23
7.	PST	Trusselvurdering 2017	10.10.2017	23
8.	PST	Nasjonal trusselvurdering 2018	30.01.2018	-
9.	PST	Nasjonal trusselvurdering 2019	15.02.2019	-
10.	PST	Nasjonal trusselvurdering 2020	04.02.2020	-
11.	PST	Nasjonal trusselvurdering 2021	08.02.2021	-
12.	PST	Nasjonal trusselvurdering 2022	i.d.	30
13.	PST	Nasjonal trusselvurdering 2023	i.d.	46

[8] Publiseringsdato på nettside, evt. dato oppgitt som redaksjonsslutt i rapport. Forkortelsen «i.d.» (ingen dato) benyttes der dato ikke foreligger lett tilgjengelig verken i rapport eller på nettside.

[9] Der antall sider ikke er oppgitt er det fordi rapporten kommer frem som egen nettside hvor man blar seg nedover (uten sidetall).

14.	NSM	Rapport om sikkerhetstilstanden 2011	Juni 2012	17
15.	NSM	Rapport om sikkerhetstilstanden 2012	i.d.	20
16.	NSM	Sikkerhetstilstanden 2014	i.d.	12
17.	NSM	RISIKO 2015	i.d.	12
18.	NSM	RISIKO 2016 - Kan sikkerhet styres?	i.d.	-
19.	NSM	RISIKO 2017 - Risiko og sårbarheter i en ny tid	i.d.	44
20.	NSM	RISIKO 2018 - Verdifulle individer, verdifulle virksomheter og verdifull infrastruktur	i.d.	32
21.	NSM	RISIKO 2019 - Krafttak for et sikrere Norge	i.d.	34
22.	NSM	RISIKO 2020	20.05.2020	44
23.	NSM	RISIKO 2021 - helhetlig sikring mot sammensatte trusler	i.d.	48
24.	NSM	RISIKO 2022 - Økt risiko krever økt årvåkenhet	i.d.	40
25.	NSM	RISIKO 2023 - Økt uforutsigbarhet krever høyere beredskap	i.d.	40
26.	E-tjenesten	FOKUS 2011	i.d.	32
27.	E-tjenesten	FOKUS 2012	20.02.2012	15
28.	E-tjenesten	FOKUS 2013	07.02.2013	25
29.	E-tjenesten	FOKUS 2014	20.01.2014	32
30.	E-tjenesten	FOKUS 2015	01.02.2015	45
31.	E-tjenesten	FOKUS 2016	10.02.2016	88
32.	E-tjenesten	FOKUS 2017	20.01.2017	45

33.	E-tjenesten	FOKUS 2018	01.02.2018	42
34.	E-tjenesten	FOKUS 2019	21.01.2019	53
35.	E-tjenesten	FOKUS 2020	23.01.2020	65
36.	E-tjenesten	FOKUS 2021	26.01.2021	53
37.	E-tjenesten	FOKUS 2022	27.01.2022	38
38.	E-tjenesten	FOKUS 2023	27.01.2023	39

Vedlegg 2:

Analyserte tildelingsbrev inkludert avsender/mottaker, brevtittel, referansekode, brevdato og antall sider.

Dok.nr	Fra - Til[10]	Brevtittel	Referanse-kode	Dato[11]	Antall sider
1.	HOD-FHI	Endelig tildeling av bevilgning for 2011 – Nasjonalt folkehelseinstitutt	HODFHI-11	20.01.2011	16
2.	HOD-FHI	Statsbudsjettet 2012 – endelig tildeling av bevilgning – Nasjonalt folkehelseinstitutt	HODFHI-12	06.01.2012	16
3.	HOD-FHI	Statsbudsjettet 2013 – endelig tildelingsbrev – Nasjonalt folkehelseinstitutt	HODFHI-13	18.02.2013	15
4.	HOD-FHI	Statsbudsjettet 2014 – Kap. 710 Nasjonalt folkehelseinstitutt – tildeling av bevilgning	HODFHI-14	31.01.2014	15
5.	HOD-FHI	Statsbudsjettet 2015 – Kap. 710 Nasjonalt folkehelseinstitutt – endelig tildelingsbrev	HODFHI-15	29.01.2015	11
6.	HOD-FHI	Statsbudsjettet 2016 – Kap. 710 Folkehelseinstituttet – tildelingsbrev nr 1	HODFHI-16	17.12.2015	18
7.	HOD-FHI	Statsbudsjettet 2017 - kap. 710 Folkehelseinstituttet - tildelingsbrev nr. 1	HODFHI-17	12.01.2017	14

[10] Forkortelser i parentes bak virksomhetsnavn: Helse- og omsorgsdepartementet (HOD), Folkehelseinstituttet (FHI), Olje- og energidepartementet (OED) og Norges vassdrags- og energidirektorat (NVE).

[11] Brevdato. Forkortelsen «i.d.» (ingen dato) benyttes der det ikke fremgår nøyaktig brevdato av verken brev eller nettside.

8.	HOD-FHI	Statsbudsjettet 2018 kap. 745 Folkehelseinstituttet – tildelingsbrev nr 1	HODFHI-18	20.12.2017	12
9.	HOD-FHI	Statsbudsjettet 2019 kap. 745 - tildelingsbrev (nr 1)	HODFHI-19	21.12.2018	15
10.	HOD-FHI	Statsbudsjettet 2020 - kap. 745 Folkehelseinstituttet - tildelingsbrev	HODFHI-20	14.01.2020	13
11.	HOD-FHI	Statsbudsjettet 2021 – kap. 745 Folkehelseinstituttet – tildelinger på fagkapitler, spesielle oppdrag mv.	HODFHI-21	21.04.2021	14
12.	HOD-FHI	Statsbudsjettet 2022 - Folkehelseinstituttet - tildelingsbrev 2022	HODFHI-22	09.05.2022	14
13.	HOD-FHI	Statsbudsjettet 2023 kap. 745 Folkehelseinstituttet – tildeling på fagkapittel, fullmakter og spesielle oppdrag	HODFHI-23	11.04.2023	15
14.	OED-NVE	Statsbudsjettet 2011. Tildelingsbrev til Norges vassdrags- og energidirektorat	OEDNVE-11	i.d.	21
15.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat 2012	OEDNVE-12	i.d.	19
16.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat 2013	OEDNVE-13	i.d.	16
17.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat 2014	OEDNVE-14	i.d.	14
18.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat 2015	OEDNVE-15	i.d.	15
19.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat 2016	OEDNVE-16	i.d.	14
20.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat for 2017	OEDNVE-17	i.d.	15
21.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat for 2018	OEDNVE-18	i.d.	15
22.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat for 2019	OEDNVE-19	i.d.	17
23.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat for 2020	OEDNVE-20	i.d.	14

24.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat for 2021	OEDNVE-21	i.d.	14
25.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat for 2022	OEDNVE-22	08.02.2022	15
26.	OED-NVE	Tildelingsbrev til Norges vassdrags- og energidirektorat for 2023	OEDNVE-23	27.01.2023	17