Universitetet i Stavanger

En kvalitativ studie om cybertruslers påvirkning av organisasjonsstrukturer i norsk vann- og avløpssektor.

Master i Samfunnssikkerhet

Lene Kristin Vatland

Våren 2023

DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i Samfunnssikkerhet	Vår, 2023 Åpen / ~~Konfidensiell~~
Forfatter: Lene Kristin Vatland	
Fagansvarlig ved UiS: Ole Andreas H. Engen Veileder: Kristin Sørung Scharffscher	
Tittel på oppgaven: En kvalitativ studie om cybertruslers påvirkning av organisasjonsstrukturer i norsk vann- og avløpssektor. Engelsk tittel: A Qualitative Study on the Impact of Cyber-threats on Organizational Structures in the Norwegian Water and Wastewater sector.	
Studiepoeng: 30	
Emneord: Cybertrusler, Vann- og avløpssektor, cyberangrep, organisasjonsstruktur, systemteori, sikkerhetskultur, sikkerhet, IKT-sikkerhet, cybersikkerhet, NAT, HRO	Sidetall: 64 + vedlegg/annet:81 Stavanger, *15. juni 2023*

Forord

Denne oppgaven markerer slutten på min tid som masterstudent ved Universitetet i Stavanger, samt at en 9 år lang epoke som student er over. Masterstudiet i samfunnssikkerhet har gitt meg uvurderlige erfaringer og kunnskap jeg vil verdsette stort og ta med meg videre både som person og inn i arbeidslivet.

En spesiell takk rettes mot alle mine informanter som tok seg tid til å stille til intervju i en hektisk arbeidshverdag, og for interesse og engasjement rundt temaet. Det har gitt dybde og informasjon som har vært sentrale bidrag til oppgaven. Oppgaven ville ikke vært den samme uten deres innsikt, erfaringer og kunnskap.

En stor takk rettes også til min veileder Kristin Sørung Scharffscher – takk for at du har hatt troen på både meg og på oppgaven, og for at du har vist omtanke og støtte i veiledningsarbeidet i det som har vært et særdeles tøft halvår. Dine innspill og våre samtaler har gitt meg selvtillit og motivasjon til å både gjennomføre og fullføre oppgaven.

I tillegg vil jeg takke mine nære og kjære for all støtte og motivasjon. Takk til mine foreldre og bonusforeldre for gjennomlesning, gode ord, nødvendige avbrekk og kjærlighet. Takk til min bror for humor, oppmuntring, faglige innspill og for endelig korrekturlesning av oppgaven.

Tusen takk til min samboer Runar for at du har vært der for meg, og gjort det du kan for å gjøre masterskrivingen mulig for meg, spesielt i perioder hvor jeg selv ikke hadde troen. Takk for at du er du!

Sist, men ikke minst, ønsker jeg å takke «Gjengen», mine medstudenter og gode venner på masterstudiet. Dere har gjort selv de mest krevende eksamensperioder, prosjektoppgaver og sosiale sammenkomster til noe jeg vil se tilbake på med enorm glede og takknemlighet.

Stavanger, 15. juni 2023

Lene Kristin Vatland

Sammendrag

Trusselbildet er i dynamisk og konstant endring som et resultat av blant annet teknologisk utvikling, digitalisering og sikkerhetspolitiske tilstander.

I denne masteroppgaven undersøkes det hvordan cybertrusler har påvirket organisasjonsstrukturer i vann- og avløpssektoren i Norge over en periode på 10 år. Vann- og avløpssektoren er ansvarlig for drift av kritisk infrastruktur og forvalter livsviktige samfunnsfunksjoner. I kjølvannet av pandemi og konflikt i Europa, har trendene i cyberdomenet rettet blikket mot kritisk infrastruktur som aktuelle angrepsmål, da det blant annet bidrar til svekkelse av andre styresmakter og gir grobunn for påvirkning i statlige beslutningsprosesser. Internasjonale angrep mot vannverk, gjør at også Norge sperrer øynene opp for at det også kan skje i norsk sektor.

For å besvare problemformuleringer, er det benyttet et kvalitativt forskningsdesign i form av dokumentstudier og intervju. Dokumentstudiene omfavner sentrale nasjonale sikkerhetsaktørers trusselvurderinger og risikobilder, samt forskningsrapporter fra VA-bransjen. Informantene i intervjuene er et utvalg nøkkelpersoner fra kommuner og underleverandører av IKT-tjenester til VA-sektoren.

De empiriske funnene viser til flere organisatoriske endringer i strukturer som følge av økt forekomst av cybertrusler. Trusselbildet er med tiden blitt mer nyansert mot kritisk infrastruktur, noe som gir nye krav og retningslinjer for sektoren. Ved å se de organisatoriske endringene i lys av pentagonmodellen og systemteoretiske perspektiver, vises cybertruslenes påvirkningskrefter både i de ulike delene av organisasjoner, så vel som organisasjoner som helhet.

De viktigste funnene konkluderer med strukturelle endringer i form av økt fokus på opparbeidelse av digital sikkerhetskultur, fokus på målrettet risikostyring, økt behov for og økt grad av interaksjon mellom aktører i bransjen, samt satsning på ny teknologi og digitalisering av prosess-systemer.

Innholdsfortegnelse

Tabeller

Figurer

Forkortelser

PST – Politiets Sikkerhetstjeneste

NSM – Nasjonal Sikkerhetsmyndighet

NPM – New Public Management

BUM – Bestiller-Utfører-Modellen

CERT/CSIRT – Computer Emergency Response Team

HRO – High Reliability Organizations (Høypålitelige organisasjoner)

NAT – Normal Accidents Theory

IKT – Informasjons- og kommunikasjonsteknologi (brukes sidestilt med begrepet cyber)

VA-sektor/VA-bransje – Vann- og avløpssektoren/Vann- og avløpsbransjen

APT – Advanced Persistent Threats (avanserte vedvarende trusler)

GNF – Grunnleggende Nasjonale Funksjoner

SCADA – Supervisory Control and Data Acquisition

NCSC – Nasjonalt cybersikkerhetssenter

ROS-analyse – Risiko- og sårbarhetsanalyse

1. Innledning

1.1 Bakgrunn for temavalg

Den 5. februar 2021 ble et vannverk i Oldsmar, USA, rammet av et angrep fra en ukjent trusselaktør. Denne ukjente aktøren innarbeidet seg tilgang til vannverkets digitale system og justerte ved hjelp av fjernstyring på blandingsforholdet av NaOH[1] i vannet fra 100ppm til hele 11100ppm. Dette angrepet kunne fått enorme konsekvenser, men fikk på grunn av tidlig reaksjon hos operatører til stede, sikkerhetstiltak og en liten dose flaks avverget situasjonen (Ulsrud, 2021). Lignende angrep mot kritiske samfunnsfunksjoner og infrastrukturer rapporteres mer og mer globalt i takt med digitalisering og teknologisk utvikling, og har skapt nye sårbarheter og utfordringer med stort konsekvenspotensiale. Etter cyberangrepet i Østre Toten[2], og hackerangrepet på vannverket i Drammen[3], har flere aktører fått øynene opp for at cybertrusler og cyberangrep også kan ramme stort i norske virksomheter.

Norsk Vann har ved flere anledninger de siste årene ytret et behov for oppgradering og investeringsbehov i norsk vann- og avløpssektor. Dette innebærer opparbeidelse og utforming av nye infrastrukturer, som skal sikre blant annet rent drikkevann og bærekraftige avløpsløsninger som skal skåne naturen. Samtidig betyr utarbeidelsen av en slik infrastruktur også at tidligere lukkede fysiske prosesser og komponenter blir digitalisert – og derfor også mer sårbart. Digitaliseringsprosessen av vann- og avløpssektoren vil utvilsomt føre til sikrere og mer stabil drift, ved at digitale løsninger tilbyr bedre oversikt og mer nøyaktige analyser internt i organisasjonene. Digitalisering vil derimot samtidig kunne gi andre typer utfordringer som kan gi store konsekvenser både for mennesker og system. Både utilsiktede hendelser som teknisk svikt og menneskelige feil kan oppstå, men også aktører med ondsinnede tilsiktede hensikter vil enklere kunne få tilgang til infrastruktur som tidligere har vært helt utilgjengelig for utenforstående.

---

[1] NaOH er den kjemiske formelen for natriumhydroksyd (også kalt kaustisk soda eller lut). I høy konsentrasjon er det et basisk stoff som kan virke etsende, og brukes ofte i sammenheng med såpeproduksjon, avløpsrens – og til å lute fisk. I vannverk kan NaOH benyttes for å alkalisere vannet, altså å justere PH-verdi. https://kurs.norskvann.no/mod/glossary/print.php?id=676&mode=letter&hook=N&sortkey&sortorder&offset=0&pagelimit=0

[2] Østre Toten kommune ble i 2021 angrepet av et hackerangrep hvor data ble lastet opp og alle backuper slettet. Hentet fra: https://www.telenor.no/om/digital-sikkerhet/2021/angrep-pa-ostretoten.jsp

[3] Drammen kommunes vannverk ble i 2021 forsøkt angrepet av Russiske hackere. Hentet fra: https://www.dagbladet.no/nyheter/russere-angrep-vannsystemet-i-drammen/76507484

Digitalisering er en viktig del av samfunnets utvikling, og nødvendig for at teknologisk og sosial utvikling skal finne sted i dagens komplekse og globaliserte verden. Til tross for dette, er digitaliseringsprosessen svært omfattende og krevende arbeid hvor organisasjoner og virksomheter med lange verdikjeder og flere aktører kan møte nye utfordringer. Særlig oppstår utfordringer ved mangel på ressurser, kompetanse eller tilstrekkelig søkelys på mest mulig hensiktsmessig sikkerhetsstyring i forbindelse med cybersikkerhet. Vann- og avløpssektoren i Norge er en sektor med en sammensatt verdikjede, hvor kommunale og interkommunale vann- og avløpsverk, konsulentselskaper, entreprenør- og teknologibedrifter og håndverkere har et utstrakt behov for tett samhandling. Stor variasjon i størrelse, lange verdikjeder og ulik utforming organisatorisk hos de ulike aktørene, har derfor gjort det interessant å undersøke hvordan cybertrusler det siste tiåret har utviklet seg i sektoren, og hvilke organisatoriske endringer disse på generelt grunnlag har medført.

1.2 Problemstilling

Bakgrunnen for temavalg for denne oppgaven har resultert i en problemstilling som undersøker i hvilken grad cybertrusler har påvirket sektoren organisatorisk. Følgende problemstilling er derfor utformet:

«Hvordan har cybertrusler påvirket organisasjonsstrukturen i vann- og avløpssektoren de siste 10 årene?»

Problemstillingen har som mål å belyse om det er gjort bevisste og konkrete endringer i organisasjonsstrukturer i VA-sektoren som følge av et dynamisk og stadig skiftende trusselbilde det siste tiåret.

I tillegg er det utarbeidet noen forskningsspørsmål som bidrar til å belyse og besvare problemstillingen. Med mål om å få en oversikt over hvilke cybertrusler som har påvirket organisasjonsstrukturer i VA-sektoren, er det i et tidsperspektiv hensiktsmessig å se hvordan truslene har utviklet eller endret seg. Ved å undersøke disse eventuelle endringene, kan det bidra til å belyse spesifikke utfordringer som kan kreve organisatoriske endringer for korrekt og målrettet håndtering. Første forskningsspørsmål er derfor formulert på følgende måte:

Forskningsspørsmål 1: Hvordan har digitale trusler utviklet seg i vann- og avløpssektoren de siste 10 årene?

Sentralt i oppgaven er de organisatoriske elementene som et resultat av endringer i trusselbildet over en tiårsperiode. Jeg har i denne oppgaven valgt å benytte blant annet pentagonmodellen (Schiefloe, 2021) for å undersøke hvordan indre og ytre omgivelser endres og påvirker interaksjoner mellom ulike deler av organisasjoner, og hvordan disse overordnet har hatt innvirkning på organisatoriske endringer i strukturer. For å kunne belyse problemstillingen, så jeg det derfor som naturlig å undersøke de ulike delene av organisasjonene fra et helhetlig perspektiv med hensyn på cybersikkerhet og hvordan de er blitt påvirket, da sektoren er kompleks og ofte tett koplet. Andre forskningsspørsmål er derfor formulert på følgende måte:

Forskningsspørsmål 2: På hvilken måte har interne og eksterne organisatoriske faktorer hatt betydning for organisasjonsstrukturer som følge av et dynamisk trusselbilde?

Problemstillingen alene kan generere ulike innfallsvinkler. Forskningsspørsmålene har bidratt til å kunne avgrense oppgaven, i tillegg til å være retningsgivende for datainnsamlingen.

1.3 Avgrensninger for oppgaven

Cybersikkerhet i organisasjoner er et omfattende og utstrakt tema, med flere ulike innfallsvinkler og fokusområder. I denne oppgaven blir det tatt utgangspunkt i organisasjoner og virksomheter i VA-sektoren som kritisk infrastruktur, og derfor som et sårbart mål for cybertrusler og cyberangrep. Større angrep i denne sektoren kan medføre potensielt katastrofale følger for livsviktige funksjoner som samfunnet er helt avhengig av. VA-sektoren i Norge er under en omfattende oppgraderings- og digitaliseringsprosess, og det eksisterer store forskjeller på vann- og avløpsvirksomheter hva gjelder størrelsesorden, organisasjonsstrukturer, prosesser og fokusområder. Fordi disse forskjellene eksisterer, vil det også naturligvis være ulikheter i hvordan utfordringer i cyberdomenet oppfattes, og hvordan organisasjoner og virksomheter er strukturert og organisert med hensyn på disse. Likevel er cybertrusler mot kritiske infrastrukturer satt mer og mer i søkelys hos de store norske sikkerhetsaktørene, noe som har gitt oppdaterte lovverk, krav og anbefalinger mot sektorer som arbeider med kritisk infrastruktur. Denne oppgaven vil derfor ta for seg hvordan ulike aktører i VA-sektoren oppfatter og opplever cybersikkerhetsproblematikken, og hvordan disse har påvirket egen og

andre organisasjoner i sektoren. Oppgaven vil derfor ikke ta for seg cyberangrep og cybertrusler i et rent teknisk aspekt, men heller mot den generelle forståelsen av cybertrusler og hvordan de har påvirket organisasjoner i sektoren i sin helhet. På denne måten vil oppgaven ikke ha som mål i seg selv å gjøre konkrete sammenligninger av virksomheter og organisasjoner i sektoren, men heller å belyse fellestrekk for utviklingen av organisasjoner og forståelsen av cybersikkerhet og cybertrusler i denne sammenheng.

Ettersom det i denne oppgaven handler om sikkerhet i kritisk infrastruktur, er det også begrensninger i hva jeg som student i forskerrollen får innsyn i hos aktører i sektoren. Dette er hensyntatt i utviklingen i av problemformuleringer og forskningsspørsmål, men skaper også avgrensninger for hvor dypt man kan undersøke denne problematikken. Oppgaven vil derfor sikte mot å avdekke endringer og forståelser på tvers av sektoren på et mer generelt grunnlag. Med dette er ønsket at oppgaven skal kunne bidra til et økt søkelys på viktigheten av cybersikkerhets-relaterte utfordringer i VA-sektoren som helhet, og hvordan organisasjoner blir påvirket strukturelt av disse.

1.4 Oppgavens struktur

Denne oppgaven består av totalt 7 hovedkapitler. I kapittel 1 vil tema, problemstilling og forskningsspørsmål først introduseres, etterfulgt av avgrensning og oppgavens struktur. I kapittel 2 vil oppgavens kontekst og rammeverket for studien presenteres. Dette kapittelet gjør også kort rede for digitaliseringsprosessen som nå finner sted i norsk vann- og avløpssektor, samt lovverk og krav i relasjon til sektoren. Kapittel 3 er oppgavens teorikapittel. Her blir relevante teorier redegjort for, som vil bli brukt som grunnlag for analyse og drøfting senere i oppgaven. Tidligere forskning blir også omtalt i dette kapittelet. Kapittel 4 forklarer den metodiske tilnærmingen som er brukt, samt beskrivelser og begrunnelser for valg som er tatt underveis i forskningsprosessen. Kapittel 5 beskriver empiri, og det blir fremlagt funn fra både intervjuer og dokumentstudier. Funnene fra kapittel 5 blir så analysert og drøftet i kapittel 6. Kapittel 7 vil avslutningsvis svare på oppgavens problemstilling gjennom funn og drøfting, etterfulgt av egne refleksjoner samt forslag til videre forskning.

2. Kontekst

Vann- og avløpssektoren i Norge er en kritisk infrastruktur som gir samfunnskritiske tjenester. (DSB, 2016). Sektoren har et tverrsektorielt nedslagsfelt dersom sektoren skulle blitt satt ut av spill. Blant annet er kritiske infrastrukturer og samfunnsfunksjoner som eksempelvis helsetjenester og matforsyning tett knyttet opp mot VA-sektoren. Den omfattende digitaliserings- og oppgraderingsprosessen i norsk vann- og avløpssektor medfører utvilsomt en mer effektiv og bærekraftig drift, men skaper også nye og mer komplekse utfordringer med tanke på hva cyberdomenet bringer med seg av risiko. VA-sektoren er som innledningsvis nevnt en stor og kompleks sektor med et mangfold av aktører. Jeg vil i dette kapittelet derfor redegjøre kort for digitaliseringsprosessen i sektoren, samt dens aktører, reguleringer, og lovfestede krav med hensyn på å kontekstualisere oppgavens rammer.

2.1 Digitalisering og oppgradering i VA-sektoren

Vann- og avløp er av Regjeringen (2022) i samarbeid med Direktorat for samfunnssikkerhet og beredskap (DSB) i en revidert oversikt definert som en kritisk samfunnsfunksjon, og krever dermed sikker og forsvarlig drift, i tillegg til tettere oppfølging i oppgraderings- og digitaliseringsarbeidet. I forbindelse med digitalisering av denne sektoren, innebærer forsvarlig drift også at det menneskelige aspektet er ivaretatt og fulgt opp. Sikkerhetstiltak som god sikkerhetskultur, hensiktsmessig sikkerhetsstyring og risiko- og sårbarhetsanalyser er barrierer som kan motvirke effekten og konsekvensene et angrep på systemet vil kunne medføre. Ettersom vann- og avløpssektoren er en kritisk samfunnsfunksjon som ved et eventuelt ondsinnet angrep kan sette samfunnet ut av spill i lengre perioder, er det særdeles viktig å undersøke hvordan digitalisering av sektoren gjøres på en trygg og forsvarlig måte som ivaretar samfunnsinteresser. Samtidig er det hensiktsmessig å se på hvilke utfordringer den teknologiske og digitale utviklingen har gitt av type trusler, og hvordan disse utspiller seg i møte med kritiske infrastrukturer og deres organisasjonsstruktur.

Ugarelli, Raspati, Selseth, Jaatun, Røstum, Rishovd & Furuberg (2021) skriver i tidsskriftet VANN, *Cyber-sikkerhet i VA-sektoren og bidraget fra STOP-IT-prosjektet,* om viktigheten av å øke cyber-fysisk sikkerhetsbevissthet, kompetanse og teknologi i virksomheter som driver med forvaltning av vann. Dette behovet har fremtrådt i kjølvannet av den raske teknologiske og digitale utviklingen vi har sett de siste årene, og som fortsatt er dagsaktuelt. Ugarelli, et al.

(2021) påpeker at COVID-19-pandemien gjorde sårbarheter mer synlige, og åpnet opp for fjernstyring og avstandsbaserte løsninger, noe som igjen førte til økninger i risikoen for nettbaserte angrep. I etterkant av pandemien er det generelt økt brukt av avstandsbaserte løsninger i flere aspekter av virksomheters praksis, og et større akseptgrunnlag for brukere å benytte slike løsninger også i dag. STOP-IT-prosjektet (Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats) har hatt som mål å være et midlertidig organ for virksomheter for støtte, beredskap, kunnskap- og kompetanseheving for vann- og avløpssektoren som innehaver av kritisk infrastruktur og samfunnsfunksjoner. Prosjektet har vært en stor bidragsyter til bevisstgjøringen av cybersikkerhetsproblematikk i sektoren. Ugarelli, et al., (2021) forklarer at sektoren allerede er kompleks, og at det er behov for en omstrukturering og utarbeidelse av ny infrastruktur, noe som også understrekes av Norsk Vann (2022). Samtidig som det trengs nye investeringer og oppgraderinger av digitale løsninger, er det også verdt å nevne fysiske aspekter som utdaterte rør, vanntap og generelt globalt press i form av eksempelvis befolkningsvekst. Dette understreker viktigheten av at sektoren utarbeider en god digital infrastruktur parallelt med den fysiske infrastrukturen.

Som et resultat av et økt behov for digitalisering og oppgradering av vann- og avløpsnettet, blir derfor cybertrusler og cyberangrep et nytt aspekt som må tas hensyn til i arbeidet. Hvordan denne problematikken påvirker allerede eksisterende organisatoriske strukturer, praksiser og måter å tenke på, vil være bunnet i nasjonale og globale trusselbilder, teknologisk utvikling, stadig oppdaterte krav og endring i marked. Organisatorisk sett har norsk vannbransje en variert tilnærming til drift og vedlikehold av virksomhetene, og historisk sett har det vært preget av ulike former for styring basert på New Public Management (NPM) og Bestiller-Utfører-modeller (BUM).

2.2 Aktører

I norsk VA-sektor er det et stort mangfold av aktører, systemer og myndighetsorganer som er involvert. Organiseringen og ansvarsfordelingen av sektoren er preget av å være fragmentert og fordelt over et stort antall aktører, noe som gjør sektoren som helhet uoversiktlig. I dette delkapitlet vil jeg redegjøre for de mest sentrale aktørene for sektoren i korte trekk i kontekst av oppgavens avgrensninger.

Kommuner og fylkeskommuner

Fylkeskommunen har det øvre ansvaret for å utøve myndighet i forbindelse med beredskapslovgivningen, samt øvrig ressursfordeling og planlegging av tiltak i vannforsyning i kommunene. Kommunene fungerer på sin side som vannverkseiere og lokal planmyndighet. Som vannverkseiere er kommunene ansvarlig for å forvalte og overholde krav fra drikkevannsforskriften. Det er opp til kommunene selv å sørge for en mest mulig hensiktsmessig organisering av vann- og avløpstjenestene de forvalter. Med andre ord er det opp til kommunene selv om tjenester utkontrakteres, føres internt, eller om de velger å inngå i interkommunale samarbeid. Som følge av dette er det store forskjeller innad i sektoren når det kommer til forvaltning og drift. Kommunene må forholde seg til ulike lovfestede krav. Overordnet nasjonalt ansvar ligger imidlertid hos Helse- og omsorgsdepartementet (Norsk Vann, 2023).

Mattilsynet

Mattilsynet fungerer som en tilsynsmyndighet for vannverk og vannforsyning i kommunene, både på lokalt, regionalt og nasjonalt nivå. Som tilsynsmyndighet bidrar Mattilsynet med veiledninger og anbefalinger med hensyn på kravene fra blant annet drikkevannsforskriften.

Norsk Vann

Den nasjonale interesseorganisasjonen for vannbransjen er Norsk Vann. Organisasjonen eies av ulike sentrale aktører i sektoren, og har som mål å bidra til trygg forvaltning av rent drikkevann, og bidra til en bærekraftig utvikling av vannbransjen. Norsk Vann er med på å sikre kompetanseheving, kommunikasjon og samhandling mellom organisasjoner og virksomheter, og har vært en stor bidragsyter i bevisstgjøringen av cybersikkerhet og cybertrusler i VA-sektoren. På bakgrunn av en oppstykket, fragmentert ansvarsfordeling hvor vann- og avløpsvirksomheter er regulert gjennom mange lover og forskrifter, har Norsk Vann gått i bresjen for muligheter for å innføre sektorlovgivning spesifikt mot VA-bransjen, og mot å utvikle en egen vanntjenestelov. Det uttrykkes både sterke ønsker og behov for at en statlig myndighet skal ha ansvar for å ivareta et helhetlig samlet regelverk som omfavner alle deler av VA-sektoren.

Kommune-CSIRT og KraftCERT

Nasjonalt senter for informasjonssikkerhet i kommunesektoren (Kommune-CSIRT) er et nasjonalt organ for kommuner og fylkeskommuner, og fungerer som et ressurssenter for rådgivning og støtte for kommunal sektor i forbindelse med digitale utfordringer og trusler,

sårbarheter i det digitale systemer og andre cyberhendelser. Sammen med KraftCERT, som er et sektor-cyberresponsmiljø for kraftsektoren, har Kommune-CSIRT poengtert viktigheten av å opparbeide et robust digitalt system også i vann- og avløpssektoren, samt digital kompetanseheving. Særlig er dette satt i søkelys etter hendelsen i vannverket i Oldsmar. I etterkant av denne hendelsen har Kommune-CSIRT og KraftCERT i samarbeid med Norsk Vann gjort vurderinger og observasjoner tilknyttet norske vannverk, da slike angrep sannsynligvis også vil kunne ramme norske vannvirksomheter (Ulsrud, 2021).

NSM

Nasjonal Sikkerhetsmyndighet (NSM) er Norges direktorat for forebyggende nasjonalt sikkerhetsarbeid. Ansvarsområdet til NSM omfatter objekter, systemer, informasjon og infrastruktur som er av nasjonal betydning, og er en sentral aktør i arbeidet med IKT-relaterte sikkerhetsutfordringer (Nasjonal Sikkerhetsmyndighet, u.å.). På bakgrunn av dette har NSM utviklet et rammeverk med tiltak og prinsipper for å beskytte informasjonssystemer mot uønskede inntrengere. NSM beskriver disse som grunnprinsipper for IKT-sikkerhet og beskrives gjennom fire kategorier: 1. Identifisering og kartlegging, 2. Beskyttelse og opprettholdelse, 3. Oppdagelse og 4. Håndtering og gjenoppretting (Nasjonal Sikkerhetsmyndighet, 2020, s. 6).

Nasjonalt cybersikkerhetssenter (NCSC) ble også etablert i 2018 som en del av NSM. NCSC bidrar til å beskytte blant annet grunnleggende nasjonale funksjoner mot cyberangrep (Nasjonal Sikkerhetsmyndighet, u.å.). Senteret er en plattform for ulike aktører i ulike nasjonale virksomheters samarbeid om å oppdage, håndtere og analysere hendelser i cyberdomenet.

2.3 Lovverk, krav og reguleringer for VA-sektoren og for cybersikkerhet

Som følge av at vannforsyning og avløpshåndtering er atskilt når det gjelder tilsynsmyndigheter, ansvarsområder og lovverk, har sektoren som helhet et stort antall gjeldende krav, lovverk og forskrifter å forholde seg til. Med hensyn på oppgavens avgrensning, vil jeg beskrive de viktigste og mest sentrale lovverkene for VA-sektoren som helhet, samt for nasjonal sikkerhet og digital sikkerhet.

Vass- og avløpsanlegglova

Lov om kommunal vass- og avløpsanlegg (Vass- og avløpsanlegglova) beskriver eier-forholdene i vann- og avløpsanlegg, og sier at nye anlegg skal være eid av kommunene, og at

kommunenes skal drifte anleggene basert på selvkostprinsippet[4]. Klima- og miljødepartementet er ansvarlig myndighet for loven.

Drikkevannsforskriften

Forskrift om vannforsyning og drikkevann (Drikkevannsforskriften) handler om de forhold som har innvirkning på drikkevann, og er underlagt Helse- og omsorgsdepartementet. Formålet med forskriften er å beskytte menneskers helse ved å stille krav om sikker levering av tilstrekkelige mengder helsemessig trygt drikkevann som er klart og uten fremtredende lukt, smak og farge (Drikkevannsforskriften, 2016, §1). Forskriften inneholder også krav om forebyggende sikring, kompetanse og beredskap. Disse kravene innebærer at vannverkseiere er pliktet til å besitte tilstrekkelig kompetanse, at det blir gjort beskyttelsestiltak og planlegging av beredskap og fysisk og digital sikring av sine systemer.

Forurensningsloven

Lov om vern mot forurensninger og om avfall (Forurensningsloven) har som formål å verne det ytre miljø mot forurensning og å redusere eksisterende forurensning, å redusere mengden avfall og å fremm en bedre behandling av avfall (Forurensningsloven, 1983, §1). Lovens kapittel 4 omhandler avløpsanlegg, og de sikringstiltak som kreves for å sikre forsvarlig drift av avløpshåndteringen. Det er Klima- og miljødepartementet som er ansvarlig departement.

Sikkerhetsloven

Lov om nasjonal sikkerhet (Sikkerhetsloven) omfatter nasjonale sikkerhetstiltak. Lovens formål er å bidra til;

a) å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser
b) å forebygge, avdekke og motvirke sikkerhetstruende virksomhet
c) at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn. (Sikkerhetsloven, 2018, §1-1).

Sikkerhetslovens §1-3 beskriver også her at loven gjelder for virksomheter som råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner. Grunnleggende nasjonale funksjoner (GNF) blir

[4] Selvkostprinsippet beskrives av Regjeringen som at inntekter fra gebyret for en tjeneste eller et produkt ikke skal overstige kostnadene ved å produsere tjenesten eller produktet, slik at kommunene ikke får et økonomisk overskudd ved ytelsen av lovpålagte tjenester (Kommunal- og moderniseringsdepartementet, 2021, s. 5).

videre definert som «tjenester, produksjon og andre former for virksomhet som er av slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser» (Sikkerhetsloven, 2018, §1-5). Vann- og avløpssektoren er innehaver av kritisk infrastruktur og defineres av Helse- og omsorgsdepartementet som en grunnleggende nasjonal funksjon, og omfavnes derfor også av Sikkerhetsloven. Gjennomgående i loven er lovfestede krav om sikkerhetstiltak i digital forstand.

Sivilbeskyttelsesloven

Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (Sivilbeskyttelsesloven) har som formål å «beskytte liv, helse, miljø, materielle verdier og kritisk infrastruktur ved bruk av ikke-militær makt når riket er i krig, når krig truer, når rikets selvstendighet eller sikkerhet er i fare, og ved uønskede hendelser i fredstid» (Sivilbeskyttelsesloven, 2010, §1). Sivilbeskyttelseslovens Kapittel V, §§14-15 beskriver kommunenes beredskapsplikt. Herunder krav om gjennomføring av risiko- og sårbarhetsanalyser og utarbeidelse av oppdaterte beredskapsplaner for uønskede hendelser.

3. Teoretisk rammeverk

En omfattende digitaliseringsprosess i infrastrukturer, teknologiske nyvinninger, globalisering og utvikling i samfunnet påvirker trusselbildet for organisasjoner på tvers av fagfelt og ansvarsområder. I en tid hvor vi i økende grad lener oss på teknologiske og digitale løsninger og komponenter, skaper dette også svært sammensatte og ofte komplekse virksomheter og organisasjoner, hvor utfordringer med cybertrusler og cyberangrep raskt kan oppstå og gjøre stor skade på samfunnsverdier. Dette kapittelet vil gjøre rede for teorier som beskriver slike utfordringer, og hvordan de kan undersøkes.

3.1 Normal Accident Theory (NAT)

Charles Perrow har i sin bok *Normal Accidents: Living with High-Risk Technologies* (1984) studert høyteknologiske systemer, og diskuterer fenomenet «normale ulykker» i slike komplekse, sammensatte systemer. I følge Perrow oppstår normale ulykker som et resultat av de komplekse samspillene mellom forskjellige komponenter i et system, hvor det kan foreligge latente usikkerheter og risikoer som til slutt vil føre til en uunngåelig ulykke eller uønsket hendelse. Disse ulykkene og uønskede hendelsene er ikke forårsaket av en enkelt feil eller enkeltpersoners handlinger, men snarere som et resultat av uforutsette samspill og interaksjoner mellom de ulike delene av systemet (Perrow, 1984). Perrow skiller mellom ulykker og hendelser i et system ved å dele systemet inn i henholdsvis fire komponenter; del, enhet, subsystem og system (Engen, et. al., 2021; Perrow, 1984). I disse komponentkategoriene finner vi menneskelige aktører, organisasjonsstrukturer og ulike former for teknologi, både mekaniske, analoge og digitale. Deler og enheter som er utsatt for skade eller risiko kan medføre såkalte *hendelser*, mens skader på subsystem og system vil medføre det Perrow klassifiserer som *ulykker* (Perrow, 1984). På bakgrunn av disse fire hovedkomponentene, skiller han også mellom det han kaller komponentfeilulykker og systemulykker (Engen, et al., 2021; Perrow, 1984). Differensieringen på ulykkene er basert på i hvilken grad feilene er koplet sammen, og om de er forutsett, forståelige eller forventet at skjer. Komponentfeilulykker viser således til ulykker hvor en eller flere feil skyldes koplinger som er koplet på forventede måter, det vil si at feil i komponenter forplanter seg i forventede sekvenser eller i kjente mønster. Systemulykker beskriver på den andre siden ulykker som skyldes ikke-forventede koplinger mellom feil i enheter eller systemer som er vanskelig å forutse. Systemulykker er forholdsvis

kompliserte, og krever utstrakt grad av forståelse og innsikt i de tett koplete og komplekse systemene for å kunne avverge eller unngå slike ulykker (Engen, et al., 2021).

Perrow (1984) poengterer videre at komplekse systemer gjerne har store mengder komponenter, og en nærhet mellom deler og enheter som kan danne uforutsette interaksjoner, som vil kunne føre til svikt i små ledd som forplanter seg i systemet og lager katastrofale følger. Lineære systemer har på den andre siden færre komponenter, tydeligere og mer løse, atskilte koplinger, som vil føre til høyere grad av gjennomsiktighet. Denne gjennomsiktigheten vil kunne påvirke systemets og virksomhetens grad av suksess i å avverge en påbegynt hendelse eller for feilen å forplante seg i totalsystemet. Hvordan systemet er koplet og egenskaper ved ulike interaksjoner sier noe om systemets grad av kompleksitet. Perrow skiller her mellom koplinger som er tette og koplinger som er løse, og mellom komplekse og lineære interaksjoner. Dersom systemet er løst koplet og har lineære interaksjoner, er sannsynligheten for store systemulykker betydelig redusert. Her vil komponentfeil være lettere å oppdage, og vil ikke kunne forårsake forplantninger i hele systemet. Derimot vil et system med tette koplinger og komplekse interaksjoner, hvor svikten eller feilen er vanskelig og tidskrevende å lokalisere, og som kan forplante seg upåaktet hen i systemet, kunne medføre store systemulykker i mye større grad.

Charles Perrows teori om normale ulykker er sentrert rundt høyteknologiske systemer med høy risiko slik som atomkraftverk, flytransport og avansert storindustri. Norsk VA-bransje kan på bakgrunn av kombinasjonen av sammensatte fysiske og digitale systemer, også omtales som et slikt høyteknologisk system med mange komponenter. Perrows teorier hevder også at komponentene i et slikt system ikke bare kan forårsake ulykker på grunn av systemfeil eller teknologiske komponenter, men også at menneskene i systemet, organisasjonsformer og ledelsesstrukturer kan være utslagsgivende for store systemulykker. Med dette til grunn, vil ikke redundante løsninger alene være tilstrekkelig for å unngå ulykker, men heller et større samspill mellom de ulike delene av organisasjonen (Perrow, 1984). Til tross for at normale ulykker-teorien ble utviklet på 1980-tallet, er teorien også overførbar til dagens situasjon, nærmere 40 år senere.

3.2 High Reliability Organizations (HRO)

High Reliability Organizations, eller høypålitelige organisasjoner (HRO), er organisasjoner som innehar høy teknisk kompetanse, utøver høy ytelse og kontinuerlig kontroll, er

tilpasningsdyktige og arbeider for pålitelighetskultur (Engen, et al., 2021, s. 171). Disse organisasjonene, til tross for ofte høy kompleksitet, har ofte svært få til ingen store ulykker eller hendelser. Til tross for upålitelige komponenter og høy grad av kompleksitet, tar HRO med andre ord utgangspunkt i at systemer likevel kan være pålitelige og at ulykker kan avverges og forebygges (Aven, et al., 2004). Høypålitelige organisasjoner har spesifikke karakteristikker som ofte er gjentakende hos de organisasjonene som er mest vellykket i form av få eller ingen ulykker. Weick & Sutcliffe (2015, s. 7-14) har identifisert særlig fem punkter som utpeker seg som avgjørende for en pålitelig organisasjon, under det de omtaler som «mindful organizing»;

1. «*Preoccupation with failure»*

Det å være opptatt av å oppdage og rapportere feil er en sentral del av en HRO. Dette innebærer i følge Weick & Sutcliffe (2015, s. 46) at man også er klar over at uventede ting kan skje, og at man stadig ser etter små feil som potensielt kan være symptomer på større feil og problemer i systemet. Samtidig er det sentralt at man anerkjenner at kunnskap og kompetanse ikke er uten svakheter og mangler, og desto viktigere er det å også kunne forutse eventuelle feil og identifisere feil man ikke ønsker å gjøre i en prosess. Med andre ord handler det om å være på kontinuerlig jakt etter feil, villighet til å stadig justere på bakgrunn av disse, og ikke minst å rapportere disse slik at de blir tatt tak i tidsnok.

2. «*Reluctance to simplify»*

Motvilje mot å forenkle problemer er et annet viktig poeng i høypålitelige organisasjoner. Forenkling av problemer kan innebære å generalisere og kategorisere feil basert på tidligere erfaringer, kjente mønstre eller antakelser, noe som kan føre til at viktige detaljer kan oversees, noe som igjen vil føre til økt sannsynlighet for en dårligere og mer upålitelig ytelse i systemet (Weick & Sutcliffe, 2015, s. 64). Ved å motstå å falle i fellen av å generalisere og forenkle problemer, kan viktige detaljer tidlig oppdages og potensielt avverge større ulykker.

3. *«Sensitivity to Operations»*

Med sensitivitet mener Weick & Sutcliffe (2015) at man benytter seg av de to foregående prinsippene – i praksis. Ved å være bevisst over mulige feil, selv i situasjoner som likner tidligere erfaringer eller i kjente sekvenser og mønster, kan man reagere i selve handlingsrommet av en situasjon eller hendelse. Med andre ord betyr dette å være seg bevisst i en situasjon, og sensitivitet til pågående operasjoner, på tross av systemets oppbygning, intensjoner og planlegging omkring operasjoner og hendelser.

4. *«Commitment to Resilience»*

Weick & Sutcliffe (2015, s. 94-95) poengterer at HROer ikke defineres som fullstendig feilfrie, men at feilene som oppstår ikke nødvendigvis setter hele systemet ute av spill. Dette handler om systemets resiliens. Resiliens er definert på flere måter i samfunnssikkerhetsfagene. Hollnagel, Wood & Leveson (2006, s. 4) beskriver resiliens i enkleste forstand som systemets evne til å forutse og tilpasse seg uventede hendelser og feil i systemets komponenter. I forbindelse med organisasjoners pålitelighet, defineres resiliens av Weick & Sutcliffe blant annet som (fritt oversatt): «Et resilient system er i stand til å effektivt tilpasse sine funksjoner før, under eller etter endringer og forstyrrelse, slik at det kan fortsette å yte som nødvendig etter avbrudd eller større uhell og i nærvær av kontinuerlige stressfaktorer» (Weick & Sutcliffe, 2015, s. 96). I komplekse systemer kan dette være utfordrende, men krever at hele systemet er bygget opp for å kunne motstå eventuelle hendelser.

5. *«Deference to Expertise»*

Siste prinsipp i Weick & Sutcliffes (2015) karakterisering av en høypålitelig organisasjon, handler om å ha respekt og tillit til ekspertise. Med dette mener de at fremfor å ha et rigid og stivt hierarki, hvor beslutningstakere oftest sitter på toppen av pyramiden, så vil problemene som oppstår danne sitt eget hierarki på grunnlag av hvilken kompetanse som behøves. Dette tillater en beslutningsmigrasjon ved uforutsette og akutte hendelser som søker problemløsning hos de mest kompetente menneskene i systemet, for en mest mulig effektiv håndtering (Weick & Sutcliffe, 2015, s. 115). På denne måten vil ikke beslutningstaking i HRO bestemt være sentralisert, men gir rom for at de riktige aktørene får tillit og mulighet til å yte best handlekraft i møte med konflikter og systemfeil.

Weick & Sutcliffes fem punkter som inngår i det de kaller «mindful organizing», kan med dette omtales som årvåkenhet og bevissthet omkring beslutning, handling og planlegging i mål om å forhindre at store hendelser skal kunne finne sted. Teorien om HRO utfordrer dermed Perrows teorier om normale ulykker, ved påstanden om at samtidig sentralisert og desentralisert styring er mulig. Høy grad av strukturell kompleksitet i organisering og ledelsesroller ble dokumentert som effektive for unngåelse av ulykker, fordi rutiner, sikkerhetstiltak og kompetanse var godt regulert og kommunisert på tvers av hierarkisk rollefordeling (Engen, et al., 2021). Ledelsesstrukturer viser seg i HRO å være fleksible i situasjoner som behøver ekstra oppmerksomhet og kompetanse, og er med på å opprettholde høy pålitelighet i organisasjoner.

En forutsetning for at dette fungerer i høypålitelige systemer og organisasjoner er også at det eksisterer en kultur for å rapportere, informasjonsdeling og kompetanseheving. James Reason (1997) peker på ulike forutsetninger som må være til stede i en organisasjon for at en sikkerhetskultur som fremmer disse elementene kan oppnås. Spesielt fire forutsetninger og komponenter utgjør det Reason (1997, s. 195) omtaler som informerende kultur. Den informerende kulturen innebærer at den er rapporterende, fleksibel, rettferdig og lærende. Dersom den informerende kulturen i en organisasjon er til stede og fungerende, danner det implisitt en felles diskurs for sikkerhet, og en samkjørt risiko- og sikkerhetsforståelse hvor systemet blir mer resilient.

Leveson (2011) hevder på sin side at organisasjoner med høy pålitelighet slett ikke er ensbetydende med absolutt trygghet og sikkerhet. I komplekse systemer kan nemlig også ulykker oppstå i interaksjoner mellom fullstendig fungerende komponenter, og ikke bare som et resultat av komponentfeil eller systemiske hendelser (Leveson, 2011). En viktig markering mellom sikkerhet og pålitelighet som forskjellige systemegenskaper er lagt til grunn for dette resonnementet. Et system kan på bakgrunn av dette tankesettet være usikkert men samtidig pålitelig, på lik linje som at et system kan være upålitelig og samtidig sikkert (Leveson, 2011). Dette perspektivet gjør seg gjeldende i forbindelse med cybertrusler i cyberfysiske systemer slik som i VA-sektoren på grunn av de ulike systemene som benyttes i sektoren.

3.3 Organisasjon og systemteori

I alle former for sosiale sammenhenger finner vi dannelser av organisasjoner, dog med ulike strukturer, mål og arbeidsfordelinger. Strukturen i organisasjoner henger sammen med de formelle målsetninger organisasjonen har fastsatt. Mintzberg (1979, s. 2) definerer organisasjonsstrukturer som «*... the sum total of the ways in which it divides its labor into distinct tasks and then achieves coordination among them*». En fordeling i arbeidsformer og koordinering av disse skjer på bakgrunn av ulike faktorer. Kast og Rosenzweig (1973) velger å beskrive en organisasjon som et system, med utgangspunkt i de sektorielle subsystemene som både kan deles inn i teknologiske, strukturelle, strategiske og kulturelle systemer som koordineres av et øvre styringssystem. Hvordan en organisasjon er strukturert er altså basert på dens virke, funksjoner og omgivelser.

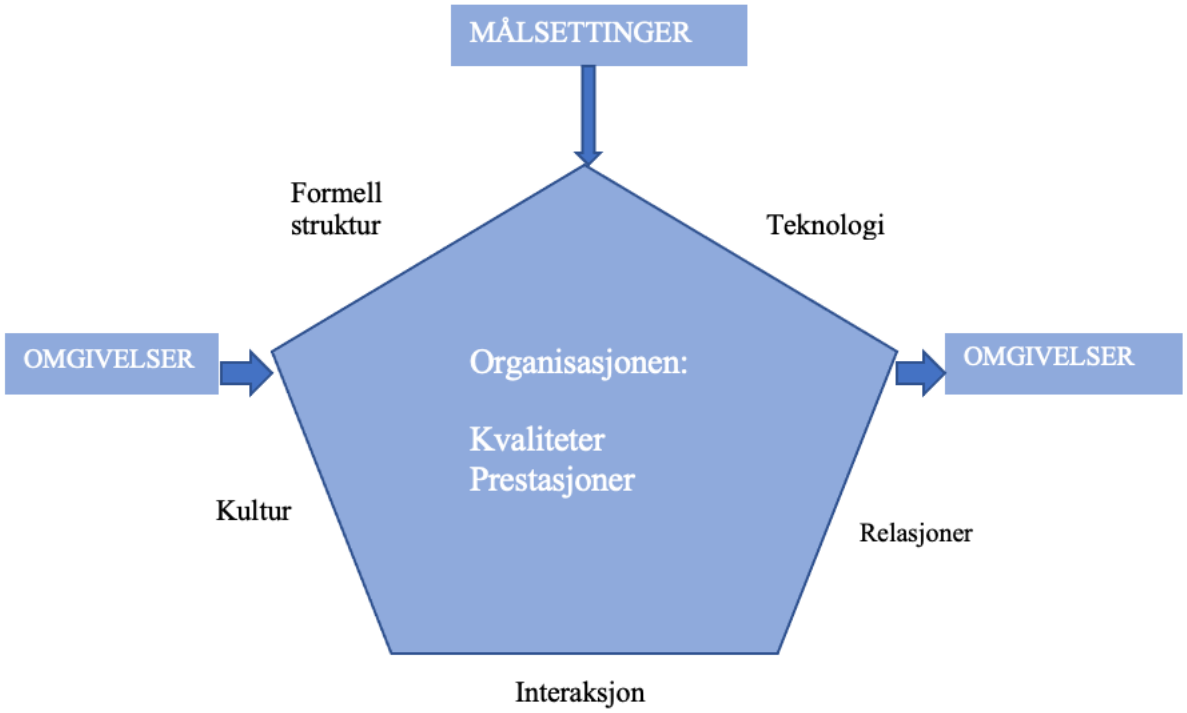
I forbindelse med organisasjonsteori, kan systemteori beskrives som en tilnærming som betrakter organisasjoner som komplekse systemer. Disse systemene består av ulike komponenter, subsystemer og styringsstrukturer som samhandler både internt og eksternt (Schiefloe, 2021). Fremfor å studere og analysere de enkelte delene av en organisasjon, viser systemteori derimot til et helhetlig perspektiv, og en helhetlig vurdering av en organisasjons problemstillinger. Schiefloe (2021) poengterer at man i systemteori derfor anser organisasjoner som sammensatt av mange deler som påvirker hverandre og delene er gjerne gjensidig avhengig av hverandre. I likhet med Schiefloe (2021), hevder også Bijker, Hughes & Pinch (2012). at et teknologisk system består av mange komponenter i samhandling. Komponentene er ifølge Bijker, et. al., (2012) sosialt konstruerte, fysiske eller ikke-fysiske, og refererer til eksempelvis datamaskiner, transformatorer og maskineri, men også regelverk, organisasjonsstrukturer, kultur og normer. Alle komponentene, store og små, interagerer, påvirker hverandre og er gjensidig avhengig av hverandre mot det som er systemets felles målsetning (Bijker, et. al., 2012, s. 45). Dersom det forekommer endringer i en komponent, vil det ha større eller mindre ringvirkninger for én eller flere andre komponenter i systemet. Dette skaper dynamiske endringer i systemet og herunder organisasjoner, som er viktig å anerkjenne.

NAT og HRO er to ulike perspektiver innen systemteori, og som illustrerer systemteoriens tankesett; organisasjoner er ofte komplekse systemer med mange komponenter i løse og tette koplinger og interaksjoner. Endringer i en del av systemet eller organisasjonen vil kunne medføre konsekvenser for hele systemet umiddelbart, men også ved at de kan utvikle seg og gi konsekvenser på sikt.

3.4 Pentagon-modellen

Pentagonmodellen er ikke en teori i seg selv, men er mer i retning av et analytisk hjelpemiddel for å forstå organisatoriske endringer. Jeg velger likevel å forklare modellen i teorikapitlet, fordi det trekker linjer organisatorisk sett både til NAT, HRO og til generell systemteori, som danner det teoretiske grunnlaget for denne oppgaven. Pentagonmodellen bidrar også til å se organisasjoner som en helhet, og hvordan de ulike delene av en organisasjon spiller inn på hverandre med indre og ytre påvirkninger og påkjenninger. Ettersom denne oppgaven etterstreber å belyse eventuelle strukturelle endringer på grunn av utfordringer fra cyberdomenet, er pentagonmodellen en visualisering av VA-sektorens systematiske komponenter i samspill.

Interne og eksterne forhold har begge stor innvirkning på en organisasjon og dens virke. Schiefloe (2021, s. 94) presiserer at organisasjoner er åpne systemer som blir påvirket av og samhandler med eksterne forhold, altså sine ytre omgivelser, på teknologisk, politisk, økonomisk og kulturelt vis, og manifesteres eksempelvis gjennom politiske vedtak, sikkerhetspolitiske situasjoner, og økonomi. De interne forholdene kan imidlertid beskrives som en organisasjons egne egenskaper. Interne forhold, eller de indre omgivelsene, skilles igjen mellom formelle og uformelle faktorer (Schiefloe, 2021). De interne og eksterne forholdene kan omtales som organisatoriske rammer og gir organisasjonen mål og retning. Disse rammene kan grupperes under fellesbetegnelsene formell struktur og teknologi, kultur, interaksjon og relasjoner som betegnet i Figur 1.



Figur 1: Pentagonmodellen med presentasjon av hovedfaktorer i en organisasjonsanalyse. Basert på modell i Schiefloe (2021, s. 96).

Formelle faktorer kan grovt deles inn i to hovedkategorier, og utgjør den øverste delen av pentagonmodellen (se figur 1). Disse kategoriene er den *formelle strukturen* og organisasjonens *teknologi.* Den formelle strukturen beskriver elementer ved en organisasjon som er mer eller mindre fastsatt, slik som organisasjonskart, vedtak og reglement og kontrollsystemer. Her

inngår også systemer for rapportering og fastsatte prosedyrer for virksomheten. Teknologi på sin side omfatter blant annet materiell infrastruktur og digitale IKT-systemer, hvor driftskontrollsystemer, utstyr og anleggs tekniske tilstand dokumenteres (Schiefloe, 2021).

Uformelle faktorer ved en organisasjon kan på sin side deles inn i tre hovedkategorier. Disse kategoriene utgjøres av *relasjoner, kulturer og interaksjoner* i organisasjonen. De sosiale relasjonene beskriver gjerne de mer uformelle strukturene i virksomheter som dannes av de sosiale relasjonene og tilknytninger mellom de ansatte, men også av interne og eksterne gruppedannelser og sosiale nettverk. Her er det vesentlig å se på nettverksdannelser og bruk av disse på tvers av fagmiljø, og forholdet mellom personell med systemansvar og utføreransvar. Kulturen i en organisasjon betegner blant annet normer, verdier, holdninger og formell kompetanse. Hvorvidt det foreligger en sikkerhetskultur eller hvor god eller dårlig den er, henger sammen med disse punktene. Den siste hovedgruppen, interaksjoner, handler om hvordan mennesker (og system) interagerer og samhandler, og særlig hvordan ledelse og styring fungerer i praksis.

De fem elementene som beskrevet over er i konstant samspill og virker inn på hverandre. Sammen utgjør de organisasjonens struktur – i dette tilfellet basert på det ytre elementet cybertrusler sin påvirkning. Dette perspektivet bidrar til å søke en balanse mellom de nødvendige formelle faktorene og de uformelle faktorene. Prosedyrer, nytt lovverk, teknologisk utvikling og IKT-systemer påvirker også de uformelle faktorene – og motsatt igjen. I HRO trekker eksempelvis Weick & Sutcliffe (2015) frem aspektet ved å være opptatt av å oppdage feil og å hele tiden være på jakt etter *mulige* feil og sårbarheter i et system. Dette skjer i de uformelle delene av en organisasjon, og helt nødvendig for å kunne gjøre nødvendige oppdateringer på systemer, ROS-analyser og risikovurderinger som en del av den formelle delen. Fra et systemteoretisk perspektiv er organisasjonen som helhet viktig for å forstå hvordan samspillet mellom de ulike delene fungerer og fører til strukturelle endringer og ytelse, noe pentagonmodellen bidrar til å belyse.

3.5 Begrepsavklaringer

New Public Management (NPM) og Bestiller-Utfører-modellen (BUM)

I forbindelse med et økt søkelys på samfunnssikkerhet og beslutningsprosesser i sikkerhetsstyring, er det i nyere tid kommet flere myndighetskrav om å redusere sårbarheter så vel som å effektivisere styring og drift av viktige samfunnsfunksjoner (Engen, et al., 2021). Dette har kommet i lys av at offentlige aktører i større grad har privatisert viktige samfunnsfunksjoner etter at offentlig sektor fikk kritikk for å være for byråkratisk og regelstyrt. Blant annet har VA-sektoren siden 80-tallet gjennomgått privatiseringer og endringer i strukturer etter New Public Management (NPM) (Engen, et al., 2021, s. 426). Dette medførte en styringsmodell som i større grad ble markedsorientert, gjennom å styrke kompetanse, effektivisering og målstyring horisontalt og vertikalt i virksomheter (Lægreid & Christensen, 2007, s. 17). Bestiller-Utfører-modellen er basert på NPM, og søker å skille mellom rådgivningsrollen og profesjonsrollen ved å dele byråkratiet i en etterspørselsside med bestillere og en tilbudsside med utførere. Dette ble gjort for å etterligne det private markedet og for å simulere konkurranse. I utgangspunktet ble modellen innført i helse- og omsorgstjenestene i kommunen, men er også benyttet i varierende grad av andre sektorer.

Ulike former for digitale angrep

Det vil i denne oppgaven beskrives ulike former for cyberangrep og -trusler. De mest fremtredende angrepsformene som betegnes i dokumentene fra dokumentanalysen blir beskrevet i Tabell 1. Beskrivelsene av angrepsformene er hentet fra NSM sin rapport Helhetlig IKT-risikobilde 2017 (Nasjonal sikkerhetsmyndighet, 2017, s. 53-56).

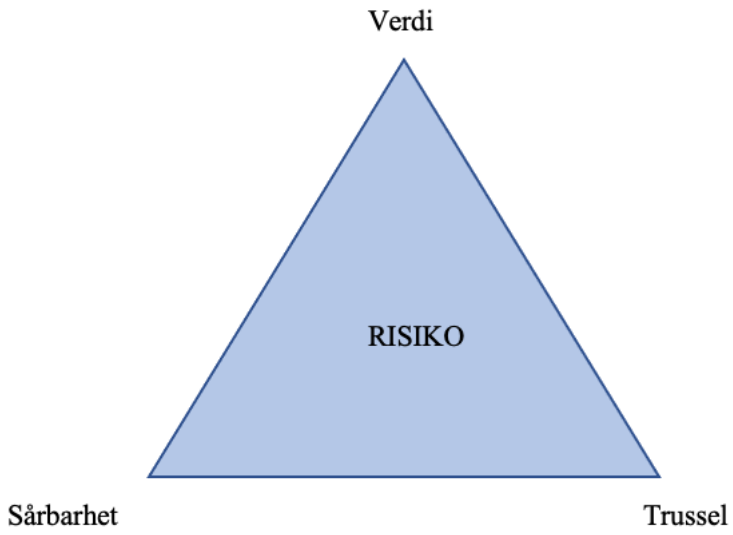
Angrepsmetode	Beskrivelse
DDoS/Tjenestenektangrep	Et internettangrep som overbelaster en server ved at stor trafikk rettes mot serveren. Hensikten er å hindre normal tilgang for ordinære brukere.
Phishing	Det å gi seg ut for å være en annen og be en person om opplysninger for å kunne plante skadevare. Personens tillit til den originale avsenderen blir forsøkt utnyttet.
Spearphishing	Skadevare levert via målrettet e-post, gjerne mot spesifikke målpersoner.
APT	Vedvarende og målrettet angrep på systemer med formål å etablere bakdører, plante og spre skadevare og hente ut fortrolig informasjon. Angriperen er gjerne ressurssterk, bruker avansert skadevare og opererer langsiktig. Også betegnelse på aktøren bak et slikt angrep.
Ransomware/løspengevirus	Skadelig programvare som krypterer systemer for så å økonomisk utpresse eieren av systemet.
Malware/skadevare	Skadelig programvare (fra engelsk malicious software).
Påvirkningsoperasjoner	Tilsynelatende usynlige operasjoner som spres misinformasjon i mål om å påvirke virkelighetsbilde og oppfatning til målet.
Kryptering	Koding av informasjon slik at den blir uleselig for uvedkommende.
Hybride trusler	Systematisk og synkronisert bruk av flere virkemidler iverksatt med formål om å påvirke en motpart og oppnå strategiske målsettinger. Den sammensatte virkemiddelbruken finner sted i en sikkerhetspolitisk kontekst og har vesentlig skadepotensial for den som rammes.
Bakdør	Skadevare som gir angriper uautorisert adgang og mulighet til å kontrollere systemer.

Tabell 1: Beskrivelse av digitale angrepsmetoder

Risiko og trefaktormodellen

Risikobegrepet blir brukt i mange sammenhenger, både fra et samfunnssikkerhetsmessig ståsted, men også i dagligtalen. Njå et al. (2020, s. 46) definerer risiko som «... et uttrykk for konsekvens/utfall av uønskede hendelser og usikkerhet assosiert med hendelser og utfall».

Risiko kan også betegnes som noe som kan eller kunne skjedd, og hvordan hendelser påvirker samfunnet, samt hvordan våre handlinger kan påvirke forløpet til en hendelse (Engen, et al., 2021, s. 93). For å kunne måle og stedfeste risiko, er det vanlig å benytte risikoanalyser. I risikoanalysene blir det oftest brukt en modell som baserer seg på analyser av verdier, sårbarhet og trusler. Disse inngår i det man kaller trefaktormodellen som vist i Figur 2 (Engen, et al., 2021).



Figur 2. Trefaktormodellen (Njå, et al., 2020, s. 259).

Njå, et al., (2020, s. 258) beskriver verdier som et begrep knyttet til en virksomhet, systemet eller den samfunnskritiske funksjonen som undersøkes. Slike verdier kan eksempelvis være en virksomhets omdømme, økonomi, liv og helse og informasjon (ibid). I VA-sektoren kan slike verdier være servere, kunnskap og kompetanse, vannverksbygg og avløpsverk og ikke minst vann som grunnleggende nasjonal funksjon. Trusselbegrepet omfatter de farene virksomheten er omgitt av. Trusler kan være alt fra spionasje og sabotasje, terrorisme, cyberangrep eller vandalisme (Njå, et al., 2020). Sårbarhet beskrives generelt av Njå, et al. (2020, s. 258) som virksomhetens eller systemets evne til å motstå truslene. Sårbarheten måles altså på i hvilken grad en trusselaktør kan utføre sine handlinger uten å bli stanset.

Robusthet

Robusthet er et begrep som blir omtalt i denne oppgaven for å beskrive systemer og organisasjoner. Begrepet kan ifølge Aven & Thekdi (2022) forstås som den evnen et system eller en virksomhet har til å tåle påkjenninger som kommer utenfra.

Digitalisering

Digitalisering er et mye brukt begrep i dagens samfunn. I forbindelse med digitalisering av offentlig sektor, er det imidlertid hensiktsmessig å konkretisere hva som menes med begrepet. I utgangspunktet handler digitalisering om å benytte digital teknologi til å fornye, forenkle og forbedre (Regjeringen, 2014). Hensikten med digitalisering er i hovedsak å skape løsninger for nye forbedrede tjenester, effektivisering, tilgjengelighet og pålitelighet. Regjeringen (2014) definerer digitalisering som;

> «I utgangspunktet er digitalisering en samlebetegnelse for overgangen fra analoge, mekaniske og papirbaserte løsninger, prosesser og systemer, til elektroniske og digitale løsninger. Begrepet digitalisering rommer derfor også etablering av nye IT-systemer som opprettholder rutiner som utføres manuelt, selv om noen av de største besparelsene ved digitalisering ofte kommer når rutiner ikke bare blir digitale, men også kan automatiseres. Slik begrepet blir brukt i dag, omfatter det dessuten også oppgradering av gamle og utdaterte løsninger, selv om gamle IT-systemer strengt tatt allerede er digitale». (Regjeringen, 2014).

I mange tilfeller medfører digitalisering et stort omstillingsarbeid. Regjeringen (2014) påpeker også at digitalisering forstått som å introdusere ny teknologi inn i en organisasjon, kan bidra til forenkling av komplekse regelverk, effektivisering av prosesser og fornying av utgått forvaltningspraksis.

3.6 Tidligere forskning og rapporter

I forarbeidet med denne masteroppgaven, ble det også gjort søk etter tidligere forskning på temaet. I forbindelse med cybersikkerhet i VA-bransjen i Norge, er det gjort kun et fåtall prosjekter som er offentliggjort i nyere tid, det vil si de siste 5 årene.

CISS-prosjektet

I regi av Norges forskningsråd, ble det i perioden 2007-2010 utført et prosjekt av SAMRISK (Program for Samfunnssikkerhet) og SINTEF hvor det ble undersøkt hvordan restrukturering av vannbransjen gir konsekvenser for samfunnssikkerhet. Critical Infrastructures, Public Sector Reorganisation and Societal Safety (CISS) er fellesbetegnelsen på dette prosjektet som tar for seg tre sektorer som håndterer kritisk infrastruktur, vann- og avløp, strøm og telekom. Det blir her gjort rede for hvordan nye organisasjonsformer gir konsekvenser for sikkerheten i kritisk

infrastruktur, og tar utgangspunkt i organisasjonsformer basert på New Public Management (NPM) i form av Bestiller-Utfører-modeller (BUM).

Norsk Vann

Norsk Vann er som nevnt i kapittel 2 den nasjonale interesseorganisasjonen for norsk VA-bransje. I samarbeid med viktige aktører i bransjen, forskningsinstitutter og kommuner utarbeider Norsk Vann veiledninger og rapporter for å styrke aktørenes kunnskapsgrunnlag og kompetansebygging. Mange av veiledningene og rapportene viser til tekniske og driftstekniske problemstillinger og løsninger, mens kun et fåtall omtaler cybersikkerhet i VA-sektoren spesifikt mot restruktureringer i organisasjoner. Et utvalg av disse er benyttet i dokumentanalysen, og omtaler sikkerhet og sårbarhet i driftskontrollsystemer, tiltak for å styrke sikkerhetskultur, og råd om strukturering av organisasjoner med tanke på å øke digital sikkerhetsbevissthet.

De nasjonale sikkerhetsaktørene

De største norske sikkerhetsaktørene utgir hvert år en trusselvurdering og situasjonsbilder i forbindelse med sikkerhet og IKT-sikkerhet. Årlige rapporter og trusselvurderinger fra Etterretningstjenesten, Politiets Sikkerhetstjeneste og Nasjonal Sikkerhetsmyndighet danner grunnlaget for mye av forståelsen for de digitale truslene vi står overfor, og er brukt som utgangspunkt for en del av dokumentanalysen i denne oppgaven.

4. Forskningsmetode

I dette kapittelet vil jeg beskrive og redegjøre for valg av forskningsmetode og beslutninger underveis i forskningsprosessen i mål om å belyse oppgavens problemformuleringer. Valg av metode, beskrivelse av innsamling og bearbeiding av data vil bli gjort rede for, etterfulgt av beskrivelser av kvalitetskriterier. Til slutt vil jeg belyse mine refleksjoner rundt metodens styrker og svakheter.

4.1 Metodisk tilnærming

4.1.1 Valg av forskningsdesign

I arbeidet med å velge ut et forskningsdesign, er det flere avveininger som skal tas med i betraktning på bakgrunn av tema, problemformulering og hva som gir representative data for oppgaven. Ulike strategier for å besvare forskningsspørsmål krever ulike sett av prosedyrer (Blaikie & Priest, 2019, s. 21). Jeg har i denne oppgaven valgt å benytte intervjuer og dokumentanalyse for å besvare problemformulering og forskningsspørsmål. Da det ikke foreligger overvekt av forskning eller tilgang til informasjon omkring tematikken, så jeg det som nødvendig å søke til nøkkelpersoner for innhenting av datamateriale, samtidig som data fra dokumentanalysen skulle danne et grunnlag for videre datainnsamling. Jeg har i stor grad latt datainnsamlingen legge føringer for forskningsprosessen og oppgaven, som igjen har påvirket utvalg av teorier, noe som sammenfaller med en abduktiv tilnærming.

Et abduktivt forskningsdesign plasserer seg i landskapet mellom induksjon og deduksjon, og søker å forstå et gitt fenomen, fremfor å produsere generaliserbare data som gjelder for alle tilsvarende tilfeller (Blaikie & Priest, 2019). Det er flere måter å forstå den abduktive forskningsstrategien. Danermark, Ekström & Karlsson (2019, s. 110), beskriver på sin side at abduksjon gjennom rekontekstualisering vil sette fenomenet i en ny kontekst, og gjerne hvor søkelyset er lagt på elementer som tidligere ikke er undersøkt. Videre hevder de at man på denne måten kan forstå fenomenet på en ny måte, som vil kunne føre til nye meninger og oppdagelser. Kovács & Spens (2005) understreker på lik linje at slike oppdagelser kan avsløre relasjoner og andre koblinger som ligger til grunn for fenomenet, som gjør at man kan forstå resultatene fra et nytt perspektiv. Ved å benytte elementer fra pentagonmodellen i analysen av hvordan cybertrusler har bidratt til strukturelle endringer, kan Danermark, et al. sin forståelse av abduktiv tilnærming hevdes å være nærmest denne oppgavens utforming.

4.1.2 Kvalitativ forskningsmetode

Med mål om å få en bredere forståelse og innsikt i temaet jeg har valgt å undersøke, har jeg i denne oppgaven valgt å benytte kvalitativ forskningsmetode. Aase & Fossaskåret (2014, s. 11) presiserer at kvalitative metoder går mer i dybden av et gitt fenomen, og viser til kvalitative data som tekst, lyd eller bilde, noe denne oppgaven også har til hensikt. Med bakgrunn i problemformulering og forskningsspørsmål, så jeg det derfor som hensiktsmessig å gjøre datainnsamlingen kvalitativt. Kvalitativ metode er fleksibelt i mye større grad enn kvantitativ metode, noe som gjør at faser i forskningsprosessen går parallelt og overlapper hverandre og skaper rom for tilpasninger jeg har ansett som nødvendig (Halvorsen, 2008, s. 131). Kombinasjonen av intervjuer og søk etter informasjon i dokumenter har skapt god innsikt for meg i forskerrollen, og gitt en dypere forståelse for de utfordringer, endringer og prosesser som organisasjonene i VA-sektoren står overfor. I startfasen av studien hadde jeg gjort egne refleksjoner rundt valg av mulige teorier, og brukte tid på å undersøke flere passende teoretiske perspektiver på temaet. Samtidig som teori på den ene siden ikke dannet utgangspunktet for oppgaven i sin helhet fra start, påvirket det likevel retning for problemformuleringer og empiri, på lik linje som at empiri påvirket sluttresultatet av utvalgt teori.

4.2 Forskningsprosess og progresjon

I Tabell 2 er forskningsprosessen og oppgavens progresjon beskrevet. Prosessen er preget av å være dynamisk, men også av vanskeligheter med å få nok informanter i henhold til det som i første omgang ble skissert. I retrospekt undervurderte jeg tidsaspekter ved forskningsprosessen. På grunn av en tidkrevende prosess med oppretting av kontakt og avtale av tidspunkt med informanter, førte det til at forskningsprosessen i sin helhet ble omrokert i henhold til eget tidsskjema. Dette har tidvis skapt utfordringer med tanke på planlegging, innhenting av egen definisjon av tilfredsstillende datamengder, og for arbeidet med fullføring av teorikapittel og empiri/drøfting. Ettersom arbeidet med denne oppgaven er utført med en abduktiv forskningsstrategi, har jeg i større grad latt empirien styre retningen for oppgaven, noe som førte til at blant annet teorikapittelet ikke ble ferdigstilt før relativt sent i skriveprosessen. Dette hadde også mindre ringvirkninger for tidsplan på tvers av oppgavens øvrige kapitler. Samtidig har den abduktive strategien gitt rom for å arbeide nettopp på tvers av kapitlene, og således ikke ført til direkte stans i skriveprosessen som følge av endringer i tidsplaner.

Når	Hva ble utført	Formål	Oppnådd resultat
Des	Innlevering av masterskisse, med valg av tema og førsteutkast av problemformulering og forskningsspørsmål. Her ble det også utarbeidet en foreløpig fremdriftsplan for prosjektet.	Å få tidlig tilbakemelding på foreslått tema, kunne gjøre endringer før endelig masterskisse blir utgangspunkt for oppgaven. Tildeling av veileder på bakgrunn av temavalg.	Levert masterskisse, og fikk tid til å jobbe med konstruktive tilbakemeldinger på oppgaveskissen.
Jan	Innledende arbeid. Laget en grov oversikt over oppgaveinndeling, metodevalg og avgrensning av oppgave. Presisering av problemformulering. Første periode av prosjektet var preget av dypdykk i flere ulike teorier og aktuelle dokumenter for dokumentanalyse.	Være tidlig ute med en god plan, oversikt og foreløpig fremdrift, slik at eventuelle utfordringer kan møtes på best mulig måte. Få bedre innsikt og forståelse for emnet ved å studere relevante teorier og rapporter. Skape bredere forståelse og bedre grunnlag for kontekst. Presisering av problemformulering fører til mer presist og relevant utgangspunkt for teori og videre arbeid med datainnsamling.	Hadde klare tanker om hvor jeg ville med oppgaven, men synes det innledningsvis var utfordrende å vite veien dit. Ble klokere ved å lese meg opp på relevante teorier og rapporter, samt i samtale med veileder på første møte. Fikk større motivasjon og tro på egen gjennomføringsevne. Utforming av tydeligere problemformulering, men noe vage forskningsspørsmål.
Feb	Arbeidet med innledning, kontekst og teorikapittel. Begynte med dokumentanalyse, og gjennomgikk aktuelle dokumenter for å skape grunnlag for besvarelse på problemformulering, men også i tankeprosessen mot utforming av intervjuguide.	Sørge for en logisk og spennende inngang til temaet, samt å knytte teorier på best mulig måte mot innhenting av empiriske data. Dokumentanalysen skaper delvis grunnlaget for innhentet empiri. I tillegg legger dokumentanalysen føringer for utforming av intervjuguide.	Brukte mye tid på lesing av teori, og oppstart av teorikapittel, i mål om å finne mest mulig relevant teori for oppgaven. Arbeidet med aktuelle dokumenter i dokumentanalyse. Fikk ikke ferdigstilt innen egendefinert tidsramme, da arbeidet var mer tidkrevende og komplekst enn først antatt.

Mar	Kontaktet aktuelle kandidater for intervju. Endring i problemformulering og forskningsspørsmål. Startet på metodekapittel.	Finne kandidater til intervju. Hensikten her var å intervjue ulike nøkkelpersoner i ulike deler av VA-sektoren for å få innsikt i sektoren som helhet. Være ute tidsnok for å sørge for å ha empiri på plass tidlig, slik at det blir nok tid til analyse og drøfting av resultater. Starte metodekapittel, og beskrive prosessen underveis når den foregår, i mål om å gi en korrekt gjengivelse av prosessen i sin helhet.	Opprettet kontakt med flere kandidater for intervju. Ble videresendt i flere tilfeller til «riktige» kontakter i tilfeller der noen var mer aktuelle for studien. Det var også flere jeg kontaktet som ikke responderte. Dette resulterte i en tidkrevende og utfordrende prosess, men fikk avtalt noen intervjuer. Fikk begynt på metodekapittel som et grunnlag før datainnsamling. Dette gjorde det enklere å supplere underveis som jeg fikk innhentet dataene. I forstadiet av utarbeidelsen av intervjuguide, ble forskningsspørsmålene omformulert da de var mange, og litt upresise.
Apr	Laget intervjuguide, samtykkeskjema og holdt kontakt med aktuelle informanter på e-post. Avtalte tidspunkt for intervjuer. Nok en gang endring i forskningsspørsmål, da jeg opplevde at de var utydelige og upresise med tanke på hovedproblemstilling. Gjennomføring av tre intervjuer. Transkribering av intervjuer, i hensikt å ha samtalen friskt i minnet, samt for å kunne gjøre justeringer og forbedringer på intervjuguide.	Utarbeide intervjuguide i tråd med problemformulering og forskningsspørsmål. Få en presis og mest mulig riktig problemstilling og forskningsspørsmål i henhold til valg av retning og foreløpige teorier. Gjennomføre intervjuer i god tid for videre analyse og bearbeiding i oppgaven. Planlegging av empirikapittel for mest mulig effektiv kategorisering og notatføring av innhentede data.	Utarbeidet en intervjuguide som ble revidert mange ganger. Etter å ha fastslått endelig problemformulering og forskningsspørsmål, ble det lettere å formulere spørsmål som på best måte ville gi svar på det jeg undersøkte. Intervjuguiden ble også endret underveis, på bakgrunn av informasjon som fremgikk av intervjuer. På denne måten fikk temaene jeg undersøkte, og informasjon jeg innhentet bli brukt hos alle informanter. Gjennomføring av tre intervjuer, transkribering av disse. Ett av intervjuobjektene valgte imidlertid å trekke seg fra

	Planla gjennomføring av empirikapittel på bakgrunn av metodevalg og resultater fra foreløpige intervjuer.		studien kort tid etter intervjuet fant sted. Dette førte til fullstendig sletting av all informasjon gitt fra vedkommende. Ettersom responsen fra de kandidatene jeg kontaktet i mars ikke var som ønsket, tok jeg fatt på en ny runde. Her fikk jeg kontakt med to kandidater som jeg fikk avtale intervjuer med – dog litt senere enn tiltenkt i egen tidsramme.
Mai	Gjennomføring av to intervjuer – transkribering av disse. Arbeidet med ferdigstillelse av teorikapittel. Intervjuene pekte i retninger som gjorde det naturlig å endre noen delkapitler, og implementere nye perspektiver og teorier. Skrev videre på alle kapitler, og hovedsakelig arbeidet med empirikapittelet mot slutten av måneden. Begynnende arbeid med drøfting og konklusjon parallelt.	Fullføre datainnsamling i form av intervju og dokumentanalyse. Undersøke sammenfallende og avvikende resultater fra de to metodene basert på innhentede data. Skape grunnlag for videre analyse og drøfting. Ferdigstille deler av oppgaven som ikke var fullført.	Etter noen utsettelser og videre dialog med aktuelle kandidater fikk jeg omsider intervjuet mine siste informanter. Undervurderte kraftig hvor lang tid det ville ta å få kontakt med kandidater og avtale intervjuer i det som også er travle arbeidsdager for informantene. Samtidig ga intervjuene verdifull innsikt i min studie, og jeg fikk likevel mange gode svar på mine spørsmål. Brukte mye tid på å beslutte hvordan jeg ville fremlegge empiri. Laget et oppsett med utgangspunkt i intervjuene, men fant ut at det skapte dårlig flyt. Endret derfor fullstendig på oppsett og måten jeg representerte empirien, noe som ble gjort i sluttfasen av hele forskningsprosessen. Gjorde også andre valg for oppsett i andre kapitler, i mål om å skape en rød tråd og en behagelig flyt gjennom oppgaven.

Jun	Ferdigstillelse av analyse/drøftingskapittel, samt konklusjon. Ferdigstilling av oppgaven i sin helhet ved gjennomgang av alle kapitler og oppsett. Språkvask, korrekturlesning og sjekket referanser, figurer og tabeller.	Sørge for at oppgaven fremstår ryddig, følger krav og retningslinjer, samt at det er en rød tråd gjennom oppgaven. Se at problemformulering blir besvart.	Ytterligere endringer i oppsett, samt revidering av eksisterende tekst. Korrekturlesning og språkvask. Levering av oppgaven 15. juni 2023.

Tabell 2: Beskrivelse av forskningsprosessen

4.3 Datainnsamling

Som nevnt innledningsvis i dette kapittelet, er det benyttet en abduktiv kvalitativ forskningsstrategi. Metodene som er benyttet for innhenting av empiriske data vil bli nærmere beskrevet i følgende underkapitler, samt relevant tilleggsinformasjon knyttet til disse.

4.3.1 Dokumentanalyse

Dokumentanalysen har stått for en del av datainnsamlingen for denne oppgaven. I arbeidet med å søke etter relevante dokumenter for denne oppgaven, har det vært utfordrende å finne offentlig tilgjengelig informasjon omkring organisatoriske utviklingstrekk spesifikt for VA-sektoren. Dokumentene som er benyttet i denne dokumentanalysen er derfor i stor grad basert på første forskningsspørsmål for denne oppgaven. Utvalget av dokumenter handler derfor i stor grad om nasjonale trusselvurderinger og risikobilder fra blant de viktigste sikkerhetsaktørene i Norge som Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Etterretningstjenesten. En mindre del av utvalget handler om VA-sektoren i direkte forstand, hvor fokuset i de utvalgte rapportene handler om cyber- og IKT-sikkerhet i VA-sektoren, samt noe om restrukturering i organisasjoner. Ettersom dokumentstudiet resulterte i et mindre funn på basis av forskningsspørsmål 2 for denne oppgaven, har det vært essensielt å få primærdata fra nøkkelpersoner i sektoren for å supplere med data. I tillegg har dokumentstudien fungert som grunnlagsgivende for utarbeidelse av intervjuguide og forskningsstrategi for øvrig.

Dokumentstudien i denne oppgaven baseres på 17 dokumenter i form av offentlige utredninger, nasjonale rapporter og forskningsartikler. Ettersom jeg i denne oppgaven ønsker å se på et fenomen i et tidsperspektiv, har det vært viktig å se på trusselvurderinger og risikobilder som

representerer tidsperioden det er snakk om. Etter å ha gjennomgått en del dokumenter tidlig i forskningsprosessen, så jeg det som nødvendig å gjøre en avgrensning i antall dokumenter for analysen. Fordi den aktuelle perioden går over et tiårsperspektiv, ble det tilgjengelige utvalget dokumenter plutselig svært altomfattende og mye opplevdes overflødig. Det opplevdes lite hensiktsmessig for oppgavens natur å skille mellom minimale distinksjoner i begrepsapparat og digitale utviklinger for hvert år. Fremfor å basere analysen på rapporter fra ulike aktører fra hvert eneste år, valgte jeg derfor å redusere antallet, og heller fokusere på å se etter forskjeller i tidsrommet imellom de jeg tok utgangspunkt i. Dette har også vært en strategisk beslutning på grunnlag av oppgavens avgrensninger og tidsbegrensning. Samtidig har det gitt et tydeligere og mer presist sammenligningsgrunnlag, med tanke på det helhetlige perspektivet oppgaven søker å belyse.

Av personlig preferanse ble det ikke benyttet kodingsprogram i analysen av dokumentene. Dokumentene ble derimot grundig gjennomlest, og jeg gjorde søk etter generelle trusselvurderinger og beskrivelse av trusselbilder, samt spesifikke søk etter vann- og avløpsrelatert materiale i utvalget. Innhentede data ble så dokumentert ved skriftlige bemerkninger og notatført i et regneark i Excel. Da funnene viste til ulike formuleringer, synes jeg dette fungerte godt. På denne måten fikk jeg dokumentert funnene på en oversiktlig måte, hvor jeg enkelt kunne sammenligne og behandle funnene videre i analysen. Dokumentutvalget er nærmere beskrevet i Tabell 3.

Tittel	Utgivelsesår	Utgiver
Fokus 2013	2013	Etterretningstjenesten
Fokus 2017	2017	Etterretningstjenesten
Fokus 2022	2022	Etterretningstjenesten
Cyber-sikkerhet i VA-sektoren og bidraget fra STOP-IT-prosjektet	2021	Norsk Vannforening
IKT og sikkerhet i VA-sektoren: Hva kan gå galt?	2013	Norsk Vannforening
Sikkerhet og sårbarhet i driftskontrollsystemer for VA-anlegg. Rapport 195.	2013	Norsk Vann
Sikkerhetsstyring for vannbransjen	2015	Norsk Vann
Sikring av vannforsyning mot tilsiktede uønskede hendelser. Rapport 229.	2017	Norsk Vann
Restrukturering av norsk VA-bransje og konsekvenser for samfunnssikkerhet	2010	NTNU Samfunnsforskning
IKT-sikkerhet – Et felles ansvar (Mld. St. 38: 2016-2017)	2017	Justis- og beredskapsdepartementet
Årsrapport 2013. Nasjonal sikkerhetsmyndighet er Norges ekspertorgan på informasjons- og objektsikkerhet.	2013	Nasjonal sikkerhets-myndighet (NSM)
Helhetlig IKT-risikobilde 2017	2017	Nasjonal sikkerhets-myndighet (NSM)
NSMs Grunnprinsipper for IKT-sikkerhet. Versjon 2.0.	2020	Nasjonal sikkerhets-myndighet (NSM)
Helhetlig IKT-risikobilde 2022	2022	Nasjonal sikkerhets-myndighet (NSM)
Trusselvurdering	2013	Politiets sikkerhetstjeneste (PST)
Trusselvurdering	2017	Politiets sikkerhetstjeneste (PST)
Trusselvurdering	2022	Politiets sikkerhetstjeneste (PST)

Tabell 3: Oversikt over dokumenter til dokumentanalyse

4.3.2 Informanter

Da denne oppgaven har som formål å undersøke hvordan cybertrusler har påvirket organisasjonsstrukturer i VA-sektoren, har det vært viktig å innhente informanter med relevant bakgrunn, erfaring og kunnskap om emnet. Et slikt strategisk utvalg er å foretrekke når man søker å innhente spesifikk informasjon i et begrenset utvalg (Halvorsen, 2008). Ettersom VA-sektoren er kompleks og har lange verdikjeder med flere ulike aktører, synes jeg det var relevant for min problemstilling å ha informanter fra ulike virksomheter og enheter fra sektoren. Dette for å få et helhetlig inntrykk av sektoren på tvers av involverte virksomheter og organisasjoner. Jeg sendte derfor e-post med invitasjon og informasjon om studien til kommuner av ulik geografisk størrelse, vann- og avløpsverk og underleverandører av digitale tjenester på landsbasis. Ettersom Covid-19 pandemien har initiert og oppmuntret til en utvidet bruk av nettbaserte møtetjenester som Zoom og Teams, valgte jeg å ikke ha en geografisk avgrensning i utvalg av informanter, da intervjuene ble foreslått å holdes over nett ved store avstander. Dette opplevdes uproblematisk både for meg som forsker og for informanter som i flere tilfeller uttrykte dette som sin preferanse.

I forbindelse med kontakt med kommuner, kontaktet jeg aktuelle kandidater fra de ulike kommunenes organisasjonskart, hvor ledere for vann- og avløpsavdelinger og myndighet sto oppført med kontaktinformasjon. I første omgang viste det seg utfordrende å få svar fra kommunene. Av de jeg omsider fikk respons fra, ble det uttrykt interesse og engasjement for temaet, men det ble kommunisert at mange hadde fulle timeplaner i en travel arbeidshverdag.
I tillegg til å sende ut invitasjoner til flere norske kommuner og virksomheter, hadde jeg også bekjentskap som refererte meg til spesifikke kontaktpersoner i enkelte kommuner og øvrige aktører i sektoren, som igjen refererte videre til nøkkelinformanter som kunne være aktuelle for studien. Flere av informantene ble innhentet på denne måten. Således kan majoriteten av informantene omtales som et resultat av en snøballsutvalgsmetode, og bidro til at jeg som forsker fikk innpass og omtale i et ellers lukket miljø (Halvorsen, 2008, s. 164). Jeg endte til slutt opp med å få informanter fra både kommune, underleverandør av IKT-tjenester og vannverk, som sammen representerer VA-sektoren i denne oppgaven.

Som følge av utfordringer med å få kontakt med aktuelle informanter, er utvalget mindre enn det som var oppgavens intensjon. Likevel er informantene nøkkelpersoner i sine representative organisasjoner, og har således gitt verdifullt og kunnskapsrikt innblikk i tematikken jeg med

denne oppgaven har undersøkt. Andersen (2006, s. 279) omtaler nøkkelinformanter som «en person som antas å ha særlig god oversikt over og innsikt i et spørsmål forskeren ønsker å få belyst», noe jeg også har opplevd i samtale med mine informanter. Tross et mindre utvalg, har datainnsamling derfor likevel generert relevant og belysende informasjon som i kombinasjon med dokumentanalyse har vært mulig å benytte for å besvare problemformuleringene.
Totalt ble 6 informanter intervjuet, fordelt på 5 intervjusituasjoner. Ettersom én av informantene valgte å trekke seg fra studien kort tid etter intervjusituasjonen, er denne oppgavens empiriske funn basert på 5 informanters svar fra 4 intervjusituasjoner. Informantene vil i kapitlene for empiri og drøfting bli omtalt og referert til som «Informant K1» (Kommune 1), «Informant K2-1» (Kommune 2), «Informant K2-2» (Kommune 2), «Informant IT1» (IT, underleverandør) og «Informant IT2» (IT, underleverandør). Ettersom både informanter og deres respektive virksomheter og organisasjoner anonymiseres i denne oppgaven, er informantene derfor tilegnet egne koder ved bruk av sitater. Fordi samtlige informanter er i samme sektor, ble dette en naturlig måte å distinktere informantene på.

4.3.3 Intervjuguide

I forkant av intervjuene utarbeidet jeg en intervjuguide. Ønsket var å utarbeide en oversikt over spørsmål som dekket over tema fra forskningsspørsmålene, med fokus på å ha en naturlig samtale om emnet, hvor informantene fikk prate fritt rundt spørsmålene på egne premisser. Et semistrukturert intervjudesign ble derfor valgt. Halvorsen (2008) påpeker at semistrukturerte intervjuer er preget av fleksibilitet og mulighet for justeringer underveis i intervjuprosessen. Dette samsvarer med hva jeg ønsket å oppnå med intervjuguiden. I semistrukturerte intervjuer er ikke strukturen i spørsmålene stramme, men kan heller virke som en retningslinje for veien i intervjuet (Kvale & Brinkmann, 2021). I noen av intervjusituasjonene ble spørsmålene i større grad samtaleførende og fulgt relativt tett. I andre situasjoner hadde informantene lange utdypende svar som gikk over spørsmål og tema, slik at jeg i større grad stilte oppfølgingsspørsmål der det var behov. Således fungerte den semistrukturerte intervjuguiden helt til sin hensikt.

Intervjuguiden i seg selv ble revidert ved flere anledninger. Første gang etter endelig presisering av problemstilling og forskningsspørsmål. Deretter slik at den var i tråd både med problemstilling, forskningsspørsmål og dokumentanalyse. Spørsmålene ble kategorisert på grunnlag av forskningsspørsmålene, slik at opplegget ble tematisk oversiktlig for informantene i intervjusituasjonen. I tillegg ønsket jeg å utforme en intervjuguide hvor det var rom for

forbedringer av formuleringer og åpenhet for å legge til eventuelle spørsmål underveis, noe som også viste seg å bli gjeldende. Jeg har vært åpen om formålet for studien til informantene, samt om tema og retning for oppgavens problemstilling. Ved å være transparent om dette, har informantene fått mulighet til å få tilsendt intervjuguide i forkant av intervjuet, samt gitt muligheten for å få en mer utfyllende beskrivelse av hva formålet med studien er ved interesse eller behov.

4.3.4 Intervjuprosessen

I et forskningsdesign med kvalitativ metode, er semistrukturerte intervjuer en ofte brukt metode. Dette skaper en intervjusituasjon hvor intervjuerrollen i hovedsak gir tematiske føringer for samtalen, mens informantene får fritt spillerom til å svare på spørsmål på egne premisser. Intervjuprosessen har strukket seg over en tidsperiode på i overkant av to måneder. Dette har gitt rom for å bearbeide datamaterialet fra hvert intervju uforstyrret, og dermed også gjort meg oppmerksom på uklarheter og forbedringspotensialer i kommende intervjuer. Intervjuene ble i hovedsak overholdt med én person om gangen, men i ett intervju ble to informanter intervjuet samtidig. Dette skapte en intervjusituasjon som ble mer dynamisk og samtalerettet, og ga rom for at informantene kunne diskutere seg imellom.

Alle intervjuene hadde en varighet på mellom 50 minutter og 75 minutter, og samtlige ble holdt over nettbaserte møtetjenester. Dette har gitt muligheter for å intervjue på tvers av kommunegrenser og et bredere utvalg av aktuelle virksomheter. Noen av informantene var korte og konsise i sine svar, mens andre hadde lange, utfyllende svar. Da jeg har valgt å basere intervjuene på en semistrukturert intervjuguide, hvor informantene fikk svare på egne premisser, lot jeg informantene tolke spørsmålene mine på sin måte uten at jeg avbrøt eller forstyrret underveis. Intervjuene ble også tatt opp analogt på båndopptaker etter samtykke fra informantene. Dette for å selv kunne delta aktivt i intervjusituasjonen uten å bli distrahert av egen notatføring. I tillegg til å være mer tilstedeværende i intervjusituasjonen, har opptakene også gitt mest mulig riktig transkribering i mål om å sikre en korrekt gjengivelse av sitater i oppgaven.

4.4 Kvalitetskriterier

Kvalitetskriterier er i dette delkapittelet en fellesbetegnelse for reliabilitet, validitet og generaliserbarhet. I følgende beskrivelser av disse, vil oppgavens kvalitetskriterier bli vurdert på bakgrunn av refleksjoner rundt metodevalg og utvalg av informanter.

4.4.1 Validitet

I forbindelse med validitet, undersøker man de genererte dataenes relevans til problemstilling og forskningsspørsmål (Halvorsen, 2008). Kvale & Brinkmann (2021, s. 276) forklarer videre at validitet i vid forstand kan forstås som den grad en metode undersøker det den er ment å undersøke. Dokumentanalysen har avdekket den historiske utviklingen og søkelyset på cybertrusler og cyberangrep i kommunal sektor på landsbasis, mens intervjuene har supplert med informasjon omkring forståelsen av denne utviklingen, samt hvordan de opplever endringer i strukturelle forhold i organisasjonene de jobber i. Dokumentene fra dokumentanalysen består av offentlig tilgjengelige rapporter og artikler fra anerkjente sikkerhetsaktører og organisasjoner med tilknytning til VA-sektoren. Informantene har vært nøkkelpersoner innad i sin virksomhet og har med sin kompetanse supplert, bekreftet og avkreftet spørsmål som er generert på bakgrunn av dokumentanalysen. Sammenhengen mellom dokumentanalysen og intervjuene svarer dermed på problemstillingen og dens utforming på en tilfredsstillende måte, som igjen kan argumenteres for å styrke oppgavens validitet. Samtidig er sektoren en del av den kritiske infrastrukturen i Norge, noe som legger begrensninger for innsyn i enkelte data, konkrete sikkerhetstiltak og detaljerte organisasjonskart. Dokumentanalysen er også preget av generelle trusselvurderinger for blant kommunale sektorer, og er oftest ikke spesifikt rettet mot VA-sektoren. Dette kan til en viss grad også svekke validiteten ved at dataene ikke er dyptgående nok til å kunne undersøke faktiske forhold mest mulig nøyaktig mot gitt problemstilling.

4.4.2 Reliabilitet

Reliabilitet handler om i hvilken grad dataene er troverdige og hvorvidt de kan bekreftes (Andersen, 2006). Ettersom dataene i denne oppgaven består av en kombinasjon av de kvalitative metodene dokumentanalyse og intervju, kan det argumenteres for å styrke oppgavens reliabilitet. På den andre siden tar oppgavens empiri utgangspunkt i et fåtall informanter, noe som i seg selv kan svekke reliabiliteten. Informantene innehar dog nøkkelposisjoner og besitter kunnskap og kompetanse innen sine fagfelt og organisasjoner, som kan sies å styrke reliabiliteten i deres utsagn. Muligheten jeg fikk ved å ta opptak av intervjuene, understøtter også dette. Samtidig har dokumentanalysen bidratt til en stor del av datainnsamlingen, noe som gjør at et lite utvalg av informanter kan aksepteres og rettferdiggjøres. Dokumentene som er benyttet i analysen er offentlige tilgjengelige rapporter og artikler som enten er av kritisk art, fagfellevurdert, publisert av nasjonale sikkerhetsaktører eller anerkjente forskningsinstitutter. Dette styrker også reliabiliteten for de innsamlede

dataene. Kombinasjonen av disse gir derfor oppgaven troverdighet og grunnlag for å kunne besvare oppgavens problemstilling.

4.4.3 Generaliserbarhet

Dersom en intervjusituasjon og metodenes resultater for datainnsamling kan kvalifiseres med høy grad av validitet og reliabilitet, gjenstår spørsmålet om resultatene kan overføres til andre intervjupersoner, kontekster og situasjoner (Kvale & Brinkmann, 2021, s. 289). Denne oppgaven tar som allerede nevnt utgangspunkt i et kvalitativt forskningsdesign med kombinasjon av dokumentanalyse og intervjuer. Empiri er avgrenset til å gjelde hvordan cybertrusler påvirker organisasjonsstrukturer i VA-sektoren, og legger dermed begrensninger for hvorvidt de samme resultatene kan overføres til andre organisasjoner. Det kan sies at resultatene kan overføres til andre organisasjoner i sektoren, eller til tilsvarende sektorer innen kritisk infrastruktur med høy kompleksitet. Likevel er utvalget i datainnsamlingen kun fra et fåtall informanter. Hva som fremgår av disse intervjuene, kan ikke sies å være gjeldende for enhver organisasjon i sektoren som helhet. Det vil være forskjeller på tvers av de ulike aktørene, men også ulikheter på tvers av kommunegrenser og ulike størrelsesordener på anlegg og organisasjoner. Kvale & Brinkmann (2021, s. 289) påpeker også at det kan eksistere innvendinger mot resultatenes generaliserbarhet og overførbarhet dersom det er for få intervjupersoner i utvalget. Dokumentene fra dokumentanalysen kan i større grad benyttes for å generalisere deler av resultatene. En overvekt av dokumentene er av generell art når det kommer til trusselvurderinger og beskrivelsen av det nasjonale trusselbildet. Det er forsøkt å rette søkelyset mot kritisk infrastruktur og VA-sektoren spesielt der det har eksistert konkrete observasjoner og anbefalinger. Likevel søker denne oppgaven imidlertid å gi et generelt bilde av den nåværende situasjonen, sett i lys av den historiske utviklingen som har funnet sted over en tiårsperiode. Resultatene vil derfor i større grad gi indikasjoner på trender og generelle oppfatninger, fremfor å gi universelt gjeldende resultater som er gyldig i alle virksomheter innad i sektoren.

4.5 Styrker og svakheter ved metodisk tilnærming

Utvalget av informanter er lite, noe som har ført til et redusert empirigrunnlag. Dette er en av de større svakheter med denne oppgaven. Likevel betrakter jeg de innhentede dataene fra intervjuene som en styrke, da informantene i stor grad har vært nøkkelpersoner i sitt virke. Det har også virket styrkende på oppgaven at intervjuene ble tatt opp på diktafon, da dette har sikret

korrekte gjengivelser i sitater. Det kan også diskuteres hvorvidt det er en styrke eller svakhet ved å benytte en semistrukturert utforming av intervjuguide. Utvalget av informanter var mindre enn det jeg i utgangspunktet ønsket, og de revideringer av spørsmål som er gjort fikk derfor innvirkning på intervjuspørsmålene og deres oppsett og utforming, og dermed videre i intervjuprosessen. Dette har resultert i tydeligere forståelse og svar fra noen informanter fremfor hos andre. Ved et større utvalg hadde disse endringene ikke nødvendigvis vært av nevneverdig grad. Likevel anser jeg det som en liten svakhet ved kontinuitet i empiri, og graden av generaliserbarhet reduseres også betraktelig, selv om generalisering ikke var et mål i seg selv for denne oppgaven. Samtidig anser jeg informantene som består av nøkkelpersoner i sitt virke, som relevante nok til å kunne veie opp for et mindre utvalg enn først tiltenkt.

Dokumentstudien baserer seg på offentlig tilgjengelige dokumenter omkring tema som betegner cyber- og organisasjonstema på generelle grunnlag. Dette har innvirkning på hvor dypt man kan dykke i materien og undersøke spesifikke fenomener og trender. Det er en styrke at det er benyttet offentlig anerkjente og fagfellevurderte rapporter og dokumenter for innhenting av datamateriale. Samtidig er utvalget i en dokumentstudie forskerstyrt. Med andre ord kan det eksistere enda mer relevante dokumenter for oppgaven som jeg som forsker enten ikke har tilgang til eller har funnet frem til, noe jeg ser på som en mulig svakhet ved metoden.

Kvalitativ metode ved abduksjon har gitt muligheter for å undersøke et fenomen som ikke er utbredt i allerede eksisterende forskning ved at jeg har fått arbeide med empiri og teori om hverandre. Det har vært en styrke ved metoden at jeg har benyttet to kvalitative strategier for innhenting av data, noe som skaper et bredere innblikk i det jeg med denne oppgaven har undersøkt.

5. Empiriske funn

I dette kapittelet vil de empiriske funnene fra dokumentanalyse og intervjuer bli presentert. Funnene er gjort på bakgrunn av en analyse av totalt 17 dokumenter og 4 intervjuer som beskrevet nærmere i kapittel 4. De empiriske funnene har som formål å bidra til å besvare problemstillingen:

«Hvordan har cybertrusler påvirket organisasjonsstrukturer i vann- og avløpssektoren de siste 10 årene?»

Kapittelet er strukturert med hensyn på forskningsspørsmålene som er utarbeidet i forbindelse med problemstillingen. På denne måten vil de gjøre en tematisk inndeling av de ulike funnene for en mest mulig oversiktlig presentasjon av dataene. Funn fra informanter og funn fra dokumentstudier vil være flettet sammen, i mål om å gjøre funnene oversiktlige og i sammenheng med hverandre.

5.1 FS1: Hvordan har digitale trusler utviklet seg i vann- og avløpssektoren de siste 10 årene?

Funnene fra forskningsspørsmål 1 er i hovedsak basert på dokumenter fra dokumentstudien, men viser også til informantenes forståelse av cybersikkerhetsrelaterte forståelser. Delkapitlene beskriver trusselbilde, trusselaktører og utfordringer med digital sikring på grunnlag av disse funnene.

5.1.1 Det dynamiske trusselbildet

Trusselbildet for Norge har i løpet av det siste tiåret vært i en dynamisk endring. Truslene vi har stått ovenfor har endret seg i takt med blant annet teknologisk utvikling, digitalisering, politikk og sikkerhetspolitiske situasjoner som har oppstått i det globale samfunnet. Samtidig har enkelte trusselformer vedvart, og heller vist til gradvis økende trender og skifte i fokusområder. Dette er sentrale betraktninger i trusselvurderingene i årene fra 2013-2022

Etterretningstjenesten utfører hvert år en trusselvurdering ved navn Fokus, basert på trender og hendelser i global kontekst. Sammen med Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet, utgir de årlige rapporter om nasjonale trusselvurderinger og aktuelle trusselbilder basert på året som er gått. Etterretningstjenesten (2013) skriver i sin trusselrapport

fra 2013 at sensitiv informasjon i stadig større grad oppbevares og lagres i det digitale rom, og at dette kan bli en arena som blir sentral i håndteringen av konflikter og kriser. Det digitale trusselbildet er preget av Russlands skifte i militær beredskap, hvor cyberangrep var å anse som en krigserklæring, samt omfattende etterretningsvirksomhet og innhenting av informasjon til senere sabotasjeoppdrag (Politiets sikkerhetstjeneste, 2013). Nasjonalt digitalt risikobilde er NSMs årlige rapport om digital sikkerhet. Hensikten med rapporten er å øke bevissthet og motivasjon for en forbedret sikkerhet i det digitale rom hos private og offentlige virksomheter i Norge. Nasjonal sikkerhetsmyndighet (2013) sier også at trusselbildet er preget av det digitale aspektet i større og større grad. Samtidig som at de digitale truslene øker, blir veldig mange av de digitale truslene og angrepene utført uten at de oppdages, eller oppdages lenge etter at infiltrasjonen har funnet sted (Nasjonal sikkerhetsmyndighet, 2013). Nettverksoperasjonene er målrettede og i stor grad rettet mot myndighetsorganer og teknologibedrifter. I hovedsak er trusselbildet ifølge NSM rettet mot avlytting og overvåkning av sentrale norske virksomheter som sitter på sensitiv informasjon om nasjonale interesser. Særlig i kjølvannet av Snowden-saken[5], ble Norge bevisstgjort om at slike trusler også kan ramme Norge, og at datasikkerhet må prioriteres i tiden fremover.

I 2013 er det ikke av de mest sentrale sikkerhetsaktørene spesifisert konkrete trusler mot VA-sektoren som sådan, men Etterretningstjenesten (2013) trekker frem at flere stater utvikler avanserte skadevarer som er spesielt rettet mot infrastruktur og samfunnsfunksjoner. Noen av disse skadevarene har som hensikt å skape innganger til systemer ved fremtidige interessekonflikter, i mål om å ødelegge eller forstyrre systemer og prosesser. Slike angrep omtales også som Avanserte Vedvarende Trusler (ATP). Eksempelvis ved å utføre aksjoner mot SCADA-systemer, som er driftskontrollsystemer som blir brukt i kritisk infrastruktur slik som VA-sektoren. Samtlige informanter bekrefter også at VA-sektoren i seg selv ikke i denne perioden opplevdes som et spesifikt mål for cyberangrep. Informant K2-1 og Informant K2-2 sier at mange ikke hadde begrepsapparatet på plass, og at det ikke eksisterte en standardisert sikkerhetsanbefaling på tvers av sektoren.

[5] Den amerikanske IT-teknikeren og varsleren Edward Snowden lekket i 2013 gradert informasjon om det amerikanske etterretningsprogrammet PRISM i regi av NSA. Lekkasjen avslørte hemmelige samarbeid mellom NSA og amerikanske nettselskaper som arbeidet med overvåkning av internasjonal datatrafikk. Hentet fra: https://snl.no/Edward_Snowden

I 2017 er det digitale trusselbildet blitt større og mer spredt. Etterretningsvirksomhet, sabotasje og påvirkning står i sentrum for truslene, og er ikke lenger kun avgrenset til infrastrukturer, industrivirksomhet, men er i større grad flettet inn i sosiale interaksjoner og medier (Etterretningstjenesten 2017, s. 36). Politisk spenning mellom Vesten og Russland, fører til at cyberdomenet blir benyttet som pressmiddel og som arena for nye trusler (Etterretningstjenesten, 2017). PST skriver også i sin årlige rapport at norsk kritisk infrastruktur vil være et utsatt mål for etterretningsvirksomhet i 2017, i mål om å avdekke og innhente informasjon om sårbarheter i viktige samfunnsfunksjoner (Politiets sikkerhetstjeneste, 2017). NSM legger til at lange digitale verdikjeder åpner opp for mange muligheter for sabotasje, spionasje og infiltrering av nasjonale interesseorganer (Nasjonal sikkerhetsmyndighet, 2017, s. 7). I 2017 er trendene som ved tidligere år også rettet mot høyteknologiske systemer, kritisk infrastruktur samt politiske og økonomiske mål, men nytt for dette året er økende trender i målrettede operasjoner og angrep mot norske virksomheters underleverandører (Nasjonal sikkerhetsmyndighet, 2017, s. 11).

Justis- og beredskapsdepartementet skriver i 2017 den første stortingsmeldingen om IKT-sikkerhet. Denne stortingsmeldingen kommer i etterkant av observasjoner om økt kriminell aktivitet i cyberdomenet, og at digitale trusler i større grad preger det nasjonale helhetlige trusselbildet og vurderinger av disse (Justis- og beredskapsdepartementet, 2017). Samtidig påpekes det at truslene er store også fordi det eksisterer mangler i kompetanse, menneskelig svikt eller uklare organiseringer med tanke på digital sikkerhet (Justis- og beredskapsdepartementet, 2017). Kombinasjonen av økte forekomster av digitale trusler og en for dårlig kompetanse og bevissthet hos norske virksomheter, har ført til et behov for å sette datasikkerhet på agendaen nasjonalt. Særlig i norsk kritisk infrastruktur og i politiske beslutningsprosesser presiseres det at det vil være et utstrakt behov for å sikre systemer og opparbeide kunnskap og kompetanse i virksomheter som har ansvar for disse.

Året 2022 er på mange måter spesielt. Det markerer en overgang fra en to år lang global pandemi til krig i Europa mellom Russland og Ukraina, og et overhengende usikkert sikkerhetspolitisk globalt landskap. I likhet med de siste 10 årene, er også Russland dette året sammen med Kina de største bidragsyterne til et utvidet og bredt trusselbilde, noe samtlige sikkerhetsaktører i Norge påpeker (Politiets sikkerhetstjeneste, 2022). Under pandemien ble virksomheter tvunget til å benytte digitale løsninger i mye større grad, hjemmekontorløsningen ble semipermanent og åpnet opp for fjernstyring av systemer og driftskontrollsystemer i

storskala. Ugarelli, et al. (2021), understreker blant andre at pandemien har medført et oppsving i bruk av digitale løsninger, men også medført nye sårbarheter og nye angrepsvinkler for aktører med ondsinnede hensikter. Digitalisering og høy grad av teknologisk innovasjon medfører også stadig mer komplekse verdikjeder på tvers av virksomheter og organisasjoner, noe om igjen medfører sårbarheter som er krevende å oppdage (Nasjonal sikkerhetsmyndighet, 2022, s. 6). Nasjonal sikkerhetsmyndighet skriver i sin rapport fra 2022 at trusselbildet er preget av hendelser og begivenheter som har gjort hyppige endringer i risikobildet, og de registrerer en tredobling av forekomsten av alvorlige cyberhendelser både mot offentlige og private virksomheter (Nasjonal sikkerhetsmyndighet, 2022; Politiets sikkerhetstjeneste, 2022). Kompleksiteten i virksomheter og systemer vil derfor gi problemstillinger, trusler og hendelser det er utfordrende å henge med på. Samtidig er spekteret av aktører så bredt, fra småkriminelle til organiserte statlige aktører, noe som gir et komplekst og til dels uoversiktlig risikobilde (Nasjonal sikkerhetsmyndighet, 2022, s. 15).

Informantene fra intervjuene har ganske sammenfallende oppfatninger av trusselbildet og hvordan det har endret seg gjennom det siste tiåret. Informant K1 forteller at de opplever at trusselbildet har gått fra å være noe diffust i form av å være noe som kunne ramme alle til en viss grad, til at det er mer rettet mot større nasjonale interesser og spesielt kritisk infrastruktur. I forbindelse med en rask utvikling og digitalisering innad i sektoren, sier Informant K2-1 også at trusselen derfor oppleves som større hos aktører som driver med kritisk infrastruktur enn tidligere. Videre forteller Informant K2-2 at de vet at det er gjort forsøk på angrep mot andre kommuner, og at det kan skje. Informant IT1 poengterer likevel at truslene og cyberrisikoen i sektoren ikke nødvendigvis ikke er ekstremt høy, til tross for at trusselvurderingene i større grad i nyere tid omfatter kritiske infrastrukturer som VA-bransjen;

> «VA-bransjen har forholdsvis robuste systemer. Det er ofte store fysiske systemer med høydebasseng og store rør-og ledningsverk, som i utgangspunktet er veldig trygge systemer. Men som følge av innføring av økt digitalisering, så åpner vi opp for flere og flere muligheter for angrep, gitt at vi ikke tenker på hva som kan gå galt underveis. Cyberrisikoen er ikke sånn sett veldig stor i Norge, men økende. Vi ser jo mange angrep globalt, som åpner norske øyne for at det kan skje.» (Informant IT1).

Som en del av intervjuet, ble også det også spurt om hvordan cybertrusler og cyberangrep oppfattes på bakgrunn av hva trusselvurderingene trekker frem. Informant IT1 svarer kontant; «Så lenge man ønsker å unngå de uønskede hendelsene, så er ikke skillet mellom cybertrusler og cyberangrep så viktig. Det viktigste er å beskytte seg og systemet mot farer, og lage en borg bestående av både tekniske, men også organisatoriske ting». Informant IT1 forteller videre at de tidligere har opplevd å bli utsatt for løsepengevirus, noe de opplevde både som en trussel og som et angrep. «Noen var ute etter penger, og tydeligvis var vi åpne nok for at det kunne skje» (Informant IT1). Tilsvarende påpeker Informant K1 at både cybertrusler og cyberangrep skaper de samme virkningene, og at sikkerhetsbevissthet er like viktig om et sikkerhetsbrudd finner sted eller ikke. Informant K2-1 og Informant K2-2 diskuterer seg imellom, og stiller seg spørrende til hvorvidt de er bevisst forskjellen. De blir enige om at de oppfatter cybertrusler og -angrep som to ulike scenarioer. Informant K2-2 sier;

> «Jeg tenker mer at en cybertrussel det er en overhengende trussel som alltid er der og som har økt og økt og økt de siste 10 årene og kanskje spesielt de siste 5 årene, der antall forsøk på cyberangrep har økt eksplosivt. Men cyberangrep, da tenker jeg at det er et pågående angrep som skjer her og nå».

Oppsummert kan trusselbildet sies å være dynamisk skiftende, og at truslene i økt grad har rettet seg mot kritisk infrastruktur, herunder også VA-sektoren, spesielt de siste 5 årene. Ulike cyberhendelser, digitalisering, politiske endringer og sikkerhetspolitiske tilstander virker stort, og raskt inn på digital sikkerhet også i norske virksomheter. Dette dokumenteres i de ulike trusselvurderingene, men oppleves også av samtlige informanter i økt grad.

5.1.2 Trusselaktører og motiver

I 2013 peker Etterretningstjenesten på at trusselaktørene kan være alt fra statlige etterretnings- og sikkerhetstjenester, via militære motstandere, globale næringsbedrifter, terrorist- og ekstremistgrupper til organiserte hackergrupper (Etterretningstjenesten, 2013). Som nevnt i forrige delkapittel, har disse aktørene motiver for å svekke tillit og skape forvirring til egne systemer i hensikt å påvirke politiske beslutninger og handlekraft hos statlige virksomheter. I tillegg er angrepene og truslenes formål å innhente informasjon og infiltrere systemer, slik at tilgang oppnås ved eventuelle fremtidige konflikter (Etterretningstjenesten, 2013). Dette understrekes også av NSM, som presiserer at det i både offentlige og private virksomheter i større grad skjer nettverksoperasjoner som går under radaren over lengre tid før de blir oppdaget (Nasjonal sikkerhetsmyndighet, 2013). Politiets etterretningstjeneste (2013) skriver også i sin

trusselvurdering at det i høy grad er statlige aktører som ved cyberangrep er ute etter å styrke egne interesser, enten det er teknologisk utvikling, økonomisk vinning og vekst, generell tilgang på ressurser og å innarbeide sabotasjeplaner og pressmidler hos andre stater. Jaatun, Røstum & Petersen (2013) trekker også frem at trusselaktørene både er eksterne og interne. Typiske angrep i VA-sektoren er forsøk på angrep på driftskontrollsystemer både fysisk og digitalt, innhenting av informasjon og sabotasje av kommunikasjonsformer, og at særlig fjernstyring er utsatt (Jaatun, Røstum & Petersen, 2013, s. 29).

I 2017 er trusselaktørene på lik linje som for 5 år tidligere stort sett statlige aktører og organiserte hackergrupper. NSM trekker frem at IKT-trusselbildet fremdeles farges av statlige aktører gjennom målrettet etterretning og spionasjeoperasjoner mot høyteknologi, virksomheter knyttet til kritisk infrastruktur og økonomiske og militære mål, i tillegg til at aktørene i større grad går mot underleverandører og kontraktører (Nasjonal sikkerhetsmyndighet, 2017, s.11). Globalt ble store løsepengeviruskampanjer utført av ulike grupperinger, men fikk begrensede konsekvenser i Norge på denne tiden. I tillegg er kryptering, tjenestenekt (DDoS) og spearphishing metoder som blir hyppig brukt i mål om økonomisk vinning. Spearphishing og phishing blir benyttet i virksomhetssammenheng såvel som hos private enkeltindivider for å oppnå tilgang eller som mål for økonomisk utpressing, også i Norge (Nasjonal sikkerhetsmyndighet, 2017).

I 2022 beskrives trusselaktørene som mange med ulike motiver i større og mindre grad. NSM skriver; «Aktørene som står bak cyberoperasjonene mot Norge det siste året, har brukt et bredt spekter av angrepsmetoder som rangerer fra enkle til svært avanserte. De mest avanserte metodene skreddersys til målet. De enkleste angrepene utnytter sårbarheter til å utløse et løsepengevirus eller oversvømmer nettsider med trafikk gjennom tjenestenektangrep» (Nasjonal sikkerhetsmyndighet, 2022, s. 15). PST trekker også frem at trusselaktørene bruker de ansattes hjemmeelektronikk og alternative ruter for å oppnå videre inngang i nettverk og systemer i virksomheten de jobber i (Politiets sikkerhetstjeneste, 2022). Ugarelli, et al. (2021) skriver også i sin artikkel om spesifikke cyberhendelser knyttet til vannverk i utlandet, hvor sivile enkeltpersoner har tilegnet seg tilgang til driftskontrollsystemer, og viser at trusselaktørene ikke nødvendigvis bare er større organiserte grupper.

Informantene har ulike opplevelser av hvem som er de største trusselaktørene mot VA-sektoren. Informant IT2 forteller at de i hovedsak skiller mellom to typer trusselaktører; «...de som er til

for å ødelegge og sette ut et system, og de som ønsker å få fordeler, ikke nødvendigvis for å ødelegge, men for å sørge for å fremme egne interesser». Informant K1 sier på sin side; «Trusselaktørene kan være alt fra oss selv, at vi gjør feil som utsetter systemet vårt for risiko, til vanlige hackere og statlig organiserte hackergrupper som er ute etter å innhente sensitiv informasjon». Samtlige informanter trekker også inn den sikkerhetspolitiske situasjonen som finner sted imellom Russland og Ukraina som eksempel. Informant K2-1 forteller;

> «Jeg tenker at trusselaktørene er det samme som i andre sektorer. Det ene er rent økonomisk vinning. Det er gjerne det som har vært den største drivkraften inntil nylig, men nå etter invasjonen i Ukraina, begynner det å bli mer en sikkerhetssak, hvor de egentlig er ute etter å finne sårbarheter i samfunnet og finne muligheter til å svekke land og samfunn på. Vi driver med samfunnskritiske tjenester og du ser jo det i Ukraina og – de går jo etter infrastruktur. Både vannforsyning og strøm er noe de ønsker å slå ut. Og det er klart at det sitter onde krefter som prøver å finne ut av hvordan de kan ramme blant annet Norge. Da vil våre tjenester være blant målene» (Informant K2-1)

> «Og så har vi disse hybride truslene vi ser i Ukraina for eksempel, hvor Russland i forkant av bomber og granater har hacket systemene og infrastrukturen for å skape totalt sammenfall i samfunnet der.» (Informant IT1)

At informantene opplever et utstrakt spekter av trusselaktører, samsvarer også med hva som kommer frem av trusselvurderinger og rapporter gjort av de ulike sikkerhetsaktørene PST, NSM og Etterretningstjenesten. Informant K1 forklarer også at fordi trusselaktørene er skiftende, og også kan omfatte egen menneskelig svikt, er det utfordrende å holde tritt med hvem og hva som til enhver tid utgjør en trussel for sektoren.

5.1.3 Utfordringer med fysisk og digital sikring

NSM trekker frem i sin rapport for 2013 at kontrollsystemer for industrier og infrastrukturer er koblet til nett i høyere grad enn før. Disse kontrollsystemene består av teknologiske systemer som ikke nødvendigvis er utformet for å kunne styres og kontrolleres gjennom nettbaserte løsninger, og har historisk sett vært utviklet for å kunne fungere i lukkede datamiljøer, slik som vann- og avløpsverk har vært (Nasjonal sikkerhetsmyndighet, 2013, s. 8). Manglende bevissthet omkring mulighetene for hacking av kontrollsystemer medfører en virksomhet som er mer utsatt for digitale trusler. Ved fravikende kunnskaper om angrepsmuligheter i disse systemene,

og ikke minst om hvordan systemene fungerer, er det naturligvis vanskelig å innføre målrettede tiltak. Mulige sikkerhetsutfordringer er at virus får spre seg i disse kontrollsystemene uoppdaget og føre til større sikkerhetsbrudd.

Rapportene utgitt av Etterretningstjenesten, NSM og PST oppsummerer de viktigste og mest utpekte truslene og angrepsformene for året som er gått. En av informantene poengterer; «Det holder ikke å lese rapportene sent på året og tenke at dette må vi gjøre noe med, for nye hendelser og trender har jo skjedd i månedene etter og for hver uke, ikke sant» (Informant IT1). Flere av informantene forstår at anbefalinger og råd omkring cybersikkerhet kan omtales som ferskvare, og må behandles deretter, men at dette er utfordrende. Det krever en kontinuerlig oppdatering og oversikt over de aktuelle truslene til enhver tid. En informant forteller; «En ting er fysisk sikring av vannverkene og bygg, det får vi til. En annen er digital sikring, det krever både en robust digital infrastruktur, men også at brukerne er bevisst sine handlinger og forstår at truslene stadig endres og påvirker hvordan systemet er satt opp» (Informant K1). Samtidig uttrykkes det utfordringer med tanke på kommunikasjon, og en informant forteller;

> «Du må jo ha kompetanse på dette her. De som jobber med vannforsyning, er gode på vannforsyning. Og så er det andre i kommunen som kanskje er god på IT. Og da må plutselig de to snakke sammen. Vannforsyningen er jo regulert av Drikkevannsforskriften. Og den sier at den som er vannverkseier skal tenke på alle farer - ledningsbrudd, og sånne fysiske utfordringer, men også det digitale. Men det kan man jo ikke. Utfordringen er jo nettopp at IT-mannen kan jo ingenting om vann og avløp og motsatt. Det er det samspillet der som må på plass» (Informant IT1).

Informant K2-1 sier at sikring i stor grad handler om å ha backup-løsninger, som for eksempel servere på fysisk atskilte steder og oppbygging av parallelle reservesystemer. Informant K2-2 følger opp med at; «Det som kan være kanskje en av de største utfordringene er at ansatte åpner lenker som ikke de burde åpne. Vi har mange som ikke sitter foran pc-en til daglig og som av nysgjerrighet plutselig klikker på en lenke de ikke burde. Det kan være vanskelig å få ut til alle hvor nøye man må være egentlig på de tingene der».

Norsk Vanns rapport *Sikring av vannforsyning mot tilsiktede uønskede hendelser* fra 2017 påpeker også at den nye Drikkevannsforskriften medførte skjerpede krav til vannverkenes beredskap og forebyggende sikkerhetsarbeid (Riis & Hareide, 2017, s. 5). Fordi anleggene og systemer i hovedsak ble bygget for flere tiår siden, er det vanskelig å håndtere nye trusler og å

overholde de lovfestede kravene om forsvarlig sikring (ibid). Driftskontrollsystemene utgjør i seg selv også farer og sikkerhetsrisikoer, fordi styringssystemene kan manipuleres på flere måter (Jaatun, Røstum & Petersen, 2013, s.8). Informant K1 har tidligere vært delaktig i digitaliseringsarbeidet av eldre systemer, og bekrefter at disse utfordringene eksisterer i sektoren på nasjonal basis.

5.2 FS2: På hvilken måte har interne og eksterne organisatoriske faktorer hatt betydning for organisasjonsstrukturer som følge av et dynamisk trusselbilde?

Funnene gjort på bakgrunn av forskningsspørsmål 2 er gjort med hensyn på faktorene i pentagonmodellen, i mål om å se på endringer i de viktigste delene av organisasjoner. Delkapitlene representerer de ulike delene, og hva som er funnet i dokumenter og intervjuer.

5.2.1 Digital sikkerhetskultur og kompetanseutvikling

I samtlige dokumenter i dokumentanalysen er manglende kompetanse, bevisstgjøring og behov for kurs og opplæring et overhengende tema i hele tiårsperioden som er undersøkt. Dette bunner i en vedvarende manglende forståelse eller bevissthet for digitale systemer, egne verdier og egen sikkerhetstilstand. Nasjonal sikkerhetsmyndighet (2013, s. 8) påpeker i 2013 særlig på at flere virksomheter ikke har klart dokumentert sine sikkerhetsutfordringer eller opparbeidet gode nok målformuleringer for sikkerhetsarbeidet. NSM forteller videre i rapporten at dette ofte skyldes manglende risikobevissthet og anerkjennelse av at virksomheten kan være utsatt for cyberangrep og cybertrusler (Nasjonal sikkerhetsmyndighet, 2013, s. 8). Sikkerhetsarbeidet kommuniseres som å være et lederansvar, noe som krever bevissthet og konkret handlingsevne hos ledere i virksomheter som benytter digitale systemer, noe NSM påpeker at ikke blir prioritert raskt nok. I forbindelse med digital kompetanseheving og opplæring, registrerer NSM også svakheter i ansvarsfordelinger, klareringskompetanse og ressursbruk på IKT-sikkerhet.

Både intervjuer og dokumenter trekker frem at det skjer en vesentlig endring i 2017. NSM lanserer første utgave av sine grunnprinsipper for IKT-sikkerhet, og har blitt revidert ved flere anledninger (denne oppgaven tar imidlertid utgangspunkt i siste versjon fra 2020). Disse grunnprinsippene har til hensikt å fungere som et hjelpemiddel for virksomheter for hvordan de kan sikre sine digitale systemer, og å øke bevissthet om digital sikkerhet på tvers av virksomhetens hierarkiske rollefordelinger (Nasjonal sikkerhetsmyndighet, 2020). Prinsippene er inndelt i fire hovedkategorier som både bygger på både teknologiske og organisatoriske

tiltak. Som nevnt i kapittel 2, er disse henholdsvis 1. Identifisere og kartlegge, 2. Beskytte og opprettholde, 3. Oppdage og 4. Håndtere og gjenopprette. Samtlige informanter forteller at grunnprinsippene er i bruk i sine virksomheter, dog i ulikt omfang. Informantene fra kommune 2 forteller at grunnprinsippene inngår i nyansattkurs, og at elementer fra disse inngår i årlige minikurs hos de ansatte. «Det er veldig elementære ting, som at ikke trykk på lenker og så videre...» (Informant K2-2). På tross av at kursene blir sendt til alle ansatte, er det langt fra alle som velger å gå gjennom dem i denne tidsperioden. Informant IT1 forteller også at ledelsen hos flere virksomheter i VA-bransjen har travle arbeidsdager hvor det NSM og andre sikkerhetsaktører ikke ble prioritert, men at informasjonsflyten på tvers av avdelingene da er ekstra viktig.

Informant IT2 presiserer at sikkerhetskulturen alltid kan forbedres, men at det ikke alltid er nok. «Det er ikke alltid det går på kompetanse heller, men heller en sånn *skal bare*-mentalitet» (Informant IT2). Informant IT2 bemerker at dette gjelder både de på gulvet, men også i ledelsen. Dette understrekes i behovet for bevisstgjøring, som i samtlige dokumenter blir trukket frem som et risikoreduserende tiltak. Veilederen for sikkerhetsstyringen i VA-bransjen utgitt i 2015 presiserer at ledelsen er et viktig element i opparbeidelsen av en tilfredsstillende sikkerhetskultur. «En ledelse som skal styre sikkerhetskultur må selv erkjenne behovet for å styre disse temaene, kommunisere dette behovet til ansatte og vise ansatte at ledelsen følger egne retningslinjer i praksis» (Endander, Hauland & Fotland, 2015, s. 32).

I 2022 kommuniseres det i flere rapporter at mange virksomheter benytter seg av blant annet NSMs grunnprinsipper for IKT-sikkerhet, og at det er en økning i kompetansenivå. Det er ikke spesifisert direkte mot VA-sektoren, men innehavere og ansvarlige for kritisk infrastruktur, påpekes å måtte sikre at sårbarhetene i driftskontrollsystemer som SCADA må identifiseres. Nasjonal sikkerhetsmyndighet (2022, s. 6) påpeker også at risikoforståelse er helt avgjørende for at sikkerhetsarbeidet i virksomhetene er hensiktsmessige og forsvarlige. Etterretningstjenesten (2022) og PST (2022) trekker frem at kriser, endringer i sikkerhetspolitiske sammenhenger og digitalisering kan oppstå svært raskt og uforutsett, noe som krever årvåkenhet og økt digital kompetanse på tvers av virksomheter særlig i offentlig sektor som behandler kritisk infrastruktur. Informant K1 forteller at digitalisering til tross, så er vannbransjen fremdeles nokså konservative, og at mange av funksjonene i vannverkene er beholdt som manuelle operasjoner. Informant K2-1 forteller at de nok selv etter et tiår med

stadig økende trusler har et behov for å innføre en sikkerhetsterminologi i det daglige arbeidet for å øke bevissthet. Informant K2-2 følger opp med at;

«Jeg tenker at opplæringen og informasjonen er der. Men det er vanskelig å ha kontroll på alle når det er mange tusen ansatte i virksomheten. Spesielt i situasjoner hvor noe ser veldig tilforlatelig ut – det er fort gjort.» (Informant K2-2).

5.2.2 Samhandling og interaksjon

I 2013 uttrykkes det av NSM et behov for å styrke samordningen på IKT-sikkerhetsområdet, og å utvikle plattformer for økt digital rådføring og veiledning. Regjeringen bevilget i 2014 millionsummer til dette formålet, og NSM vil med dette være en viktig bidragsyter i arbeidet for å kunne møte det stadig mer komplekse IKT-risikobildet (Nasjonal sikkerhetsmyndighet, 2013). Læring etter hendelser viser seg å ikke være nok, da cybertruslene stadig er ett skritt foran. «Man lærer jo mest av de hendelsene som har vært, men poenget er jo å finne den hendelsen du *ikke* visste om at kunne skje» (Informant IT1).

Enander, Hauland & Fotland (2015, s. 33) påpeker at utfordringer knyttet til kommunikasjon og samhandling i mange tilfeller er koblet til målkonflikter relatert til hemmelighold. Fordi man i sikkerhetsarbeidet aktivt forsøker å skjerme sensitiv informasjon om virksomheters sårbarheter fra reelle og potensielle trusselaktører som bruker denne informasjonen til å utføre angrep og inntrengninger, går dette også på bekostning av VA-sektoren på tvers (Enander, Hauland & Fotland, 2015). Dette fører til en avstand mellom eierskap og delaktighet til gjeldende rutiner og tiltak for sikring (ibid).

I samtlige rapporter fra NSM, er behovet for digital sikkerhetshjelp nevnt. Det har fra 2015 vært opprettet en stor andel ulike CERT for virksomheter i Norge, også på tvers av sektorer og bransjer. Først i 2020 kom Kommune-CSIRT, og skulle være et hjelpeorgan for kommunene spesifikt, og som i større grad har spisskompetanse rettet mot kontrollsystemer og prosesser også i VA-sektoren (Nasjonal sikkerhetsmyndighet, 2022). I tillegg ble Felles cyberkoordineringssenter (FCKS) opprettet i 2017, som skulle fungere som en nasjonal plattform for digital hjelp (Nasjonal sikkerhetsmyndighet, 2017). I 2022 skriver NSM at også at NSMs nasjonale cybersikkerhetssenter NCSC er med på å ivareta beredskap og krisehåndteringshjelp i cyberdomenet. Tiltakene og cyberhjelpen blir mange, og samtlige

informanter opplever at det er uoversiktlig. Da mange kommuner allerede har teknisk kompetanse eller automatisk medlemskap, er det også vanskelig å navigere i hvilke man skal være en del av. Informant K1 kan fortelle at alle kommuner er automatisk med i HelseCERT, men at medlemskapet ikke gir utfyllende informasjon – spesielt ikke mot VA-sektoren. Informant IT2 forteller at det ikke er alle kommuner som heller ser medlemskap og cybersikkerhets-aktører som en viktig del av sikkerhetsarbeidet sitt enda; «Jeg tror mange tenker at dette er overflødig og ikke noe man egentlig trenger. Og i hvert fall om det koster penger. Alt er prioriteringer og ikke minst et ressursspørsmål. Særlig i kommunene hvor midlene er knappe og skal fordeles på mange andre samfunnsfunksjoner som er viktige. Det er den situasjonen vi sitter i. Og ikke minst en *det skjer nok ikke meg*-holdning» (Informant IT2)

På den andre siden mener Informant IT1 at sikkerhetsarbeidet bør inkludere medlemskap hos flere ulike cybersikkerhetsaktører for å styrke sin evne til å motstå angrep, men også i å begrense konsekvensene av et eventuelt angrep. Kommune-CSIRT blir i denne sammenheng trukket frem som en viktig aktør for VA-sektoren, men oppslutningen er forholdsvis dårlig og informanten stiller seg derfor spørrende;

> «Det er altså 60 av 356 kommuner som er medlemmer i Kommune-CSIRT. Det vil si at det er 60 kommuner som får hjelp, og omkring 300 kommuner som ikke får hjelp. Er det gode tall?» (Informant IT1)

Informant IT1 stiller også spørsmål ved hvorvidt VA-etaten har kontroll på svakheter ned i verdikjeden i rekken av tredjepartsleverandører, og at det er vel så viktig at underleverandørene er med i CERT-ordninger for å kunne sikre en helhetlig robust verdikjede.

Erfaringsdelingen på tvers av kommunene utenom de organiserte hjelpeaktørene oppleves av informantene som til dels tvetydig. Informant K2-1 er positivt innstilt til at blant annet Norsk Vannforening har satt søkelys på cybersikkerhet i sine seminarer og samlinger på årsbasis, og at det skaper rom for diskusjoner som ellers ikke hadde funnet sted. «Hendelsen i Østre Toten har vært snakket mye om innad i vannbransjen og vi har i etterkant hatt NSM inne ved flere anledninger for å holde innlegg om dette» (Informant K2-1). Informant IT2 mener på sin side at erfaringsdeling og kommunikasjon mellom organisasjonene i sektoren ikke er god nok; «...for hadde alle snakket med alle, hadde det jo strengt tatt hold at én hadde et uhell eller en hendelse og at alle andre lærte av det. Men det er nok ikke satt av nok tid til det, spesielt av de

mindre organisasjonene og kommunene» (Informant IT2). En bemerkelse gjort av en av informantene lyder;

«Hackerne deler informasjon med hverandre *hele tiden*. Det gjør ikke vi. Og det må vi!»
(Informant IT1)

5.2.3 Teknologi

Det teknologiske aspektet ved en organisasjon i VA-sektoren er sammensatt. Jaatun, Røstum & Petersen (2013) skriver at VA-systemene har gått fra å være mer eller mindre lukkede fysiske systemer, til åpnere og mer digitaliserte prosesser. Det har lenge vært benyttet driftskontrollsystemer for å styre og overvåke vannbehandlingsanlegg og avløpsrenseanlegg, og det er en viktig del i driften av denne kritiske infrastrukturen. Økt bruk av IKT-løsninger innen drift av VA-systemer har gitt teknologiske effektiviseringer og muligheter for fjernstyring, kontrollert styring og overvåkning av komponenter (Jaatun, Røstum & Petersen, 2013, s. 8). Samtidig har dette medført reduserte kostnader og en reduksjon i driftsansatte.

Driftskontrollsystemene er omgjort til integrerte løsninger, som gjør at systemene ikke lenger er selvstendige. Jaatun, Røstum & Petersen (2013) skriver at dette utsetter driftskontrollsystemene for de samme sårbarhetene som alle andre IT-systemer. Dette poengteres også av Tøndel, Jaatun & Røstum (2013, s. 265) som rapporterer om at det foreligger en målsetning om at kontrollsystemene i VA-prosessene skal være atskilt fra administrasjonssystemene og kontornettverk, men at det er vanskelig å få til dette i praksis. Behovet for fjerntilgang, statusinformasjon, oppgraderinger og vedlikehold gjør at kontrollsystemene ikke lenger kan ses på som isolerte systemer, og skaper sårbarheter som er utfordrende å løse (Tøndel, Jaatun & Røstum, 2013, s. 265).

«Utfordringen er at i løpet av disse 10 årene trekker vi inn flere og flere komponenter som blir digitale, og komponentene snakker sammen og overlapper privat og i jobbsammenheng. Da får du plutselig ekstremt mange innganger og muligheter for å trenge inn i systemer enn før.
Men så har vi også benyttet oss av skyløsninger i større grad, og det har gjort lagring og oppbevaring av disse dataene en del tryggere.» (Informant IT1)

NSM bemerker likevel at det er en positiv effekt i bruk av flere virtuelle arbeidsflater (Nasjonal sikkerhetsmyndighet, 2017). Dette begrunnes med at angrepsflatene blir redusert parallelt med

at arbeidet sentraliseres mot et samlende digitalt system, noe som øker den generelle IKT-sikkerheten (ibid). Samtidig vil IKT-sikkerheten også være samlet på færre steder, og utsette virksomheters robusthet og sårbarheter ved eventuelle angrep om ikke det er gjort backup-løsninger som kan vedlikeholde drift.

5.2.4 Organisatoriske endringer

Samtlige rapporter utgitt av Norsk Vann peker på at det er de enkelte kommunenes ansvar for å sørge for mest mulig hensiktsmessig organisering av sine tjenester da de er lovfestede eiere av vannverkene gjennom Vass- og avløpsanlegglova. Almklov, et al. (2010) bemerker at kommunene de har undersøkt i sin casestudie på bakgrunn av lovfestede krav og drift ved selvkostprinsippet, har bevegd seg mot en mer liberal tilnærming til forvaltningen. I Norge er omorganisering av offentlig sektor over tid blitt påvirket i retning av New Public Management ved bestiller-utfører-modeller og at organisasjonsstrukturer og prinsipper i større grad er inspirert av det private markedet og næringslivet. Informant K1 forteller; «Det er litt ulike måter å organisere på, avhengig av kommunenes størrelse. Det er flere som har brukt og som fremdeles bruker en bestiller-utførermodell, men i de større kommunene har det de siste årene blitt mer vanlig å drifte anleggene selv». Dette bekrefter også Informant K2-1 og Informant K2-2. «Jeg vet ikke om jeg kan uttale meg på vegne av alle, men det er en modell (BUM) som har vært veldig i tide, men som på en måte er litt på retur. Og det henger litt sammen med svingninger politisk» (Informant K2-1).

Justis- og beredskapsdepartementet (2017) presiserer at Drikkevannsforskriften ble revidert til å stille krav til forebyggende sikring av styringssystemer for vannforsyningen. Med dette kom også nye krav til at vannverkseiere og ledelsen skal sørge for at det eksisterer nødvendig kompetanse for å imøtekomme disse kravene, enten gjennom egne ressurser eller i form av tjenesteutsetting. Vannverkene bør derfor også definere hvem som har eksplisitt ansvar for sikkerhet i forbindelse med forhindring og beskyttelse mot utilsiktede og uønskede hendelser (Endander, Hauland & Fotland, 2015, s. 21). Enander, Hauland & Fotland (2015, s. 21) hevder i likhet med Justis- og beredskapsdepartementet videre at; «Hvem som fyller disse funksjonene kan variere mellom ulike VA-virksomheter, og bør vurderes ut fra organisasjonsstruktur, personlig egnethet og arbeidsoppgaver».

Organisatorisk sett er den mest betydningsfulle trenden i 2017 ifølge NSM (2017, s. 31) at virksomheter har vekst i bruk av skytjenester og tjenesteutsetting. Bruk av slike tredjepartstjenester som igjen bruker andre tredjepartsløsninger forklares som å skape en kompleks avhengighet mellom aktørkjedene på tvers av sektorer og samfunnsnivå (Nasjonal sikkerhetsmyndighet, 2017). Dette medfører en kompleksitet også i de digitale verdikjedene, og skaper problematikk i forhold til informasjonskontroll. Informant IT2 understreker at dette skyldes at flere, særlig små virksomheter i VA-sektoren, over tid har innsett at cyberproblematikken er for stort til at de selv kan ha kontroll på det. Informant IT1 forteller at en klar endring i organisasjoner i VA-sektoren er at cybersikkerhet er satt på agendaen, og at flere og flere benytter seg av CERTer og samarbeid med andre kommuner, særlig i kjølvannet av hendelsen i Østre Toten i 2021. «Cybersikkerhet er ferskvare! Man må være oppdatert på det siste, og det blir man når man snakker sammen» (Informant IT1). Informant K2-1 forteller imidlertid at det i de større kommunene ofte er inngått store interkommunale samarbeid, hvor IKT-sikkerhet oftest blir håndtert internt i IT-avdelinger og beredskapsavdelinger, men at å ha en fast CERT-ordning i all hovedsak er positivt; «Det er en spesialistfunksjon. I kommunen har vi veldig mye vi skal ha kontroll på, og vi kan ikke være eksperter på alt. Det er jo sånn sett derfor fornuftig å være en del av et sånt samarbeid uansett».

Informant K2-2 kan også beskrive at de i sin kommune i løpet av de siste 5 årene har opprettet et eget informasjonssikkerhetsråd, hvor NSMs råd om integritet, konfidensialitet og tilgjengelighet er i høysetet. «Informasjonsnivået er derfor høyere hos oss, og det hjelper å vite hva man ikke vet. IT-avdelingene pusher oss på kurs og opplæring for å øke bevisstheten vår». Informant K2-1 skyter inn at myndighetskrav og oppgraderte lovverk tvinger en organisatorisk omveltning, ved at det foreligger krav om ROS-analyser, oppdatere beredskapsplaner og implementere digital sikkerhet i sikkerhetsarbeidet. NSM skriver imidlertid at de erfarer at virksomheter likevel unnlater å rapportere alvorlige sikkerhetsbrudd og hendelser, noe som reduserer evnen til å lære av feilene man gjør (Nasjonal sikkerhetsmyndighet, 2017, s. 23).

Jaatun, Røstum & Petersen (2013) peker på at det i det organisatoriske oppsettet er viktig å ha et helhetlig beredskapskonsept, hvor det blir utført øvelser og ROS-analyser for korrekt risikostyring i virksomheter. Risikostyring kan imidlertid oppfattes som til dels abstrakt og vanskeligere enn ved erfaringsbasert læring ifølge Enander, Hauland og Fotland (2015, s. 13). I sin rapport registrerer de at det er et stort sprik mellom tilnærmingene organisasjonene har til risikobasert risikostyring. Dette kommer også frem av informantene i intervjuene, som sier at

det har skjedd store endringer med tiden etter hvert som ledelsen og organisasjonen har fått en bedre risikoforståelse og retningslinjer fra ansvarlige myndigheter.

6. Drøfting

I dette kapittelet vil jeg drøfte de empiriske funnene mot det teoretiske rammeverket for oppgaven. I likhet med kapittel 5, vil dette kapittelet også struktureres med hensyn på forskningsspørsmål 1 og 2, og drøftingen av disse vil lede opp mot svar på problemstillingen; Hvordan har cybertrusler påvirket organisasjonsstrukturen i vann- og avløpssektoren? Endelige konklusjoner fra drøftingen og svar på problemstillingen som helhet følger i kapittel 7.

6.1 FS1: Hvordan har digitale trusler utviklet seg i vann- og avløpssektoren de siste 10 årene?

Trusselbildet

Det digitale trusselbildet har ifølge empirien forandret seg dynamisk og i en rasktvoksende kurve de siste 10 årene. Funnene fra dokumentstudiet signaliserer mer spissede trusler, og trusselbildet går fra å omfatte sentrale norske virksomheter på tvers av bransjer og sektorer, til å i større grad forsøke å sette statlige interesser og kritisk infrastruktur ut av spill. Da det i dokumentstudiet ble fokusert på trusselvurderinger med et mellomrom på femårsperioder, ble disse forskjellene tydeliggjort nærmere. Angrepsmetodene er ikke bare flere, men de er hyppigere, hissigere og mer målrettet, og vitner om at cybertrusler blir en større trusselaktør for hvert år som går. Når det i tillegg råder en global uro som følge av konflikten mellom stormakten Russland og Ukraina, blir trusselbildet enda mer komplekst. PST påpeker i sin trusselvurdering for 2022 at Russland som trusselaktør går ustabilt og uforutsigbart i front i cyberdomenet. NSM registrerer også en tredobling i forekomsten av alvorlige cyberhendelser både i private og offentlige virksomheter, noe som kan tenkes å i stor grad skyldes Russlands behov for å markere seg i Vesten. At trusselbildet vender seg mot kritiske infrastrukturer i økt grad enn tidligere, er av PST, NSM og etterretningstjenesten beskrevet som hovedsakelig politisk og økonomisk motivert. Å innhente sensitiv informasjon om systemer i kritisk infrastruktur, danne bakdører og forsøk på gjentatte cyberangrep, vil kunne medføre svekket omdømme og tillit, påvirke beslutningsprosesser og skape sosial uro i stater.

Funnene fra intervjuene bekrefter funnene fra dokumentene, og informantene uttrykker en økt bevissthet om de ulike formene for cybertrusler og -aktører. Spesielt i forbindelse med konflikten mellom Russland og Ukraina, har antallet hackere, cyberkrigere og spionasje fått søkelyset mot seg, og vi hører mer om skadevarer og ulike aktører i media i større grad. I forbindelse med kritisk infrastruktur og VA-sektoren, har informantene på grunn av spissede

mål mot egen sektor også de siste par årene fått mye større innsikt i hva cyberangrep kan gjøre mot systemer. En av informantene fortalte at deres virksomhet ble utsatt for løsepengevirus, og krypterte all data. Ettersom vedkommende arbeider i en IT-virksomhetsleverandør, ble cyberresponsmiljøer og CERT trukket frem som essensielle i arbeidet med å gjenopprette systemene. Det å være medlem i organiserte cyberresponsmiljøer kan ha enorm betydning for konsekvensutfall og skadebegrensning. Informantene er seg bevisst på hvilke verdier de arbeider med, men påstår at mange er uforsiktige eller forsinket i sitt bevisstgjøringsarbeid. Et vesentlig poeng som kommer frem av empiri, er at man stadig må være oppdatert og forberedt på morgendagens trusler. Cybersikkerhet er ferskvare, og det krever ressurser å opprettholde et sikkert digitalt system, både med tanke på økonomi og kompetanse.

Digitalisering som kilde til sårbarheter

Vann- og avløpssektoren kan betraktes som et system bestående av mange systemer og systemkomponenter, og kan derfor anses som et høyteknologisk system. Systemet består av mange enheter, deler og subsystemer, og organisasjonene kan i denne sammenheng derfor betraktes som en helhet i systemteoretisk henblikk. Sektoren opererer med norsk kritisk infrastruktur, som innebærer at de forvalter verdier som i Sikkerhetsloven (2018) kategoriseres som grunnleggende nasjonale funksjoner. Kompleksiteten i sektoren øker naturligvis i stor grad, fordi kompromitteringer og bortfall av tjenestene medfører store samfunnsmessige konsekvenser. I denne sammenheng kan det trekkes linjer til Perrows (1984) teori om normale ulykker. Et komplekst system med tette koplinger og lange verdikjeder, tilsier at ulykker ikke er til å unngå. Digitale løsninger effektiviserer drift og eliminerer brudd i prosesser i større grad. Det er enklere å identifisere feil og problemer, og å opprette normaldrift raskere. Koplingene kan i lys av dette oppfattes som lineære og løst koplet. Ved eventuelle cyberangrep, kan imidlertid systemene settes ut av drift på andre premisser, og lokaliseringsarbeidet og gjenoppretting kan vise til at de samme koplingene i denne sammenheng kan oppleves som komplekse og tette.

De tette koplingene kan i VA-sammenheng kobles til samfunnets avhengighet av rent drikkevann. Et lengre avbrudd i disse funksjonene vil gi konsekvenser for enkeltindivider, men også påvirke tverrsektorielt med tanke på matforsyning og helsevesen. Et annet eksempel på tette koplinger er VA-sektorens avhengighet til kraftsektoren for å kunne drifte digitale og mekaniske prosesser og systemer. En avhengighet til IKT-systemer og driftskontrollsystemer

en annen. Sektoren i Norge har per i dag ikke hatt mange store eller alvorlige cybersikkerhetshendelser, noe som kan argumenteres for at samsvarer med en høyteknologisk og pålitelig organisasjon slik Engen, et al, og Weick & Sutcliffe beskriver. Samtidig viser flere av trusselvurderingene fra 2022 at APT er en trend i cyberangrepsmetoder, og i økt grad blant aktører som driver med kritisk infrastruktur. NSM (2017) beskriver at ATP som metode innebærer vedvarende og målrettet angrep på systemer med formål å etablere bakdører, plante og spre skadevare og hente ut fortrolig informasjon. Angriperen er gjerne ressurssterk, bruker avansert skadevare og opererer langsiktig. Ettersom sektoren er i en omfattende oppgraderingsfase med høy grad av rask digitalisering, kan det ikke dermed utelukkes at også de norske systemene er sårbare for slike infiltrasjoner. Nærhet mellom komponentene, slik som for eksempel mellom det administrative systemet og driftskontrollsystemet, kan ifølge NAT føre til tidligere ukjente interaksjoner som kan føre til svikt i funksjon eller gi inngangsvinkler for ondsinnede aktører.

Empirien tilsier også at mange av organisasjonene i VA-sektoren på mange måter arbeider med cybersikkerhet i en retning som samsvarer med enkelte prinsipper for HRO som Weick & Sutcliffe (2017) trekker frem. Informantene forteller om stadig økt grad av bevisstgjøring omkring de truslene som eksisterer, men også at det arbeides med å identifisere hva som kan gå galt eller hvilke sårbarheter deres system må kunne håndtere. Å være opptatt av dette, og samtidig opparbeide rom for trygg rapportering og hendelseshåndtering er en sentral del av HRO-tankegang. I forbindelse med fysisk og digital sikring, blir det beskrevet ulike former for fysiske barrierer inn mot vannverkene, sonedeling og backupløsninger, både i form av parallelle systemer og manuelt strømbasert utstyr. Dette vitner om en bevissthet og arbeid med å bygge resiliente løsninger som kan beskytte systemene fra fullstendig bortfall. Innhenting av ekspertkunnskap på områder hvor organisasjonen selv innser sine mangler, beviser også at mange av organisasjonene er opptatt av å sørge for best mulig håndtering og gjør systemet mye mer pålitelig. Som nevnt er HRO en beskrivelse av et komplekst system med høy integritet og et fåtall uhell og ulykker. HRO er i så måte en slags idealmodell det kan være hensiktsmessig å strekke seg etter. Organisasjonene i VA-sektoren søker som de fleste å bygge pålitelige systemer, og da er de små detaljene viktig.

6.2 FS2: På hvilken måte har interne og eksterne organisatoriske faktorer hatt betydning for organisasjonsstrukturer som følge av et dynamisk trusselbilde?

Empirien har belyst cybertruslenes hyppige utvikling de siste 10 årene. Som følge av et økt trusselbilde som er mer rettet mot kritisk infrastruktur, viser dette til diskrete, men konkrete endringer i organisasjonsstrukturer. På bakgrunn av pentagonmodellen (Schiefloe, 2021), er det mulig å identifisere hvor i de ulike delene av organisasjonen at det største endringene har funnet sted som et resultat av økt cyberfare.

Eksterne faktorer betegnes ifølge Schiefloe (2021) som det ytre miljøet. Det kan eksempelvis være cybertrusler og trusselaktører, internasjonal sikkerhetspolitikk, økonomi og politiske svingninger. De eksterne faktorene skaper mange av rammene VA-sektorens organisasjoner må forholde seg til. Empiri fra både dokumentstudiet og intervjuer belyser det politiske aspektet som i stor grad har ført organisatoriske endringer i en retning av NPM og BUM. Dette har fremmet bruk av tjenesteutsetting, og skapt lengre verdikjeder i organisasjonene. Samtidig har tjenesteutsetting av spesielt IKT-tjenester og skytjenester ført til at eksperter med spisskompetanse har

Formell struktur

For den formelle strukturen i organisasjoner i VA-sektoren, er det gjort en del større endringer som påvirker organisasjonsstrukturene på tvers av virksomhetene. Det kommer frem i NSMs vurderinger og Norsk Vanns rapporter at det spesielt de siste 5 årene har skjedd en endring i både cyberresponsmiljøer, men også i skjerpede krav fra myndigheter. Drikkevannsforskriften gjennomgikk en fornying i 2017 som presiserer at det er vannverkene selv som er ansvarlig for å sikre sine systemer både fysisk og digitalt mot tilsiktede og utilsiktede hendelser. Dette fordrer en skjerpet ledelse som må følge strengere krav og incentiver, hvor også digital sikkerhetsstyring blir en sentral del av arbeidsoppgavene. De lokale prosedyrene og rammeverkene medfører et økt behov for helhetlige ROS-analyser og en økt beredskapsstab. Samtidig peker Jaatun, Røstum & Petersen (2013) allerede i 2013 på at risikostyring, utvidet beredskapskonsept og hyppige risikoanalyser er sentralt for å opprettholde en sikker organisasjon. Dette tyder på at det tidligere har vært utydelige rammer og mål, og at behovet for målrettet risikostyring har vært tilstedeværende lenge. I praksis betyr dette å implementere trefaktormodellen inn i sikkerhetsarbeidet. Klare retningslinjer og mål for verdier, sårbarheter og trusler må implementeres og analyseres på bakgrunn av organisasjonens overordnede målsetninger og krav. Trefaktormodellen kan benyttes som et hjelpemiddel for å fastslå den

reelle risikoen organisasjoner står overfor, slik at det blir enklere å vedta lovfestede krav og reglement, gjøre endringer i organisasjonens avdelinger, og innføre nødvendig kompetansehevende tiltak. Almklov, et al. (2010) beskriver at disse prosessene også er viktig i sammenheng med behovsavdekking omkring innhenting av eksterne aktører. Dette krever på sin side at ledelsen er involvert og engasjert i det digitale sikkerhetsaspektet ved risiko- og sikkerhetsstyring.

NSM (2017) peker på at organisasjoner i større grad benytter seg av tjenesteutsetting de senere årene, spesielt med tanke på IT-kompetanse og IKT-sikkerhetsløsninger. Noen av informantene fra intervjuene hevder at dette forekommer oftere hos de små kommunene, men at også de store organisasjonene henter inn ekspertise for å holde seg oppdatert på cyberfronten. Dette kan ses i sammenheng med de skjerpede myndighetskravene, hvor ledere har sett behov for å hente inn spisskompetanse for å tilfredsstille krav og forventninger. Som et tilleggsledd i den formelle strukturen, forteller informantene om innføring av egne informasjonssikkerhetsråd. På den ene siden fører dette til økt bevissthet og målrettet kompetanseheving i organisasjonen. Samtidig kan slike interne råd påvirke nettverksbygging og utnyttelsen av etablerte cyberresponsaktører, noe som også fremgår særlig i store interkommunale samarbeid. Her er organisasjonene i samhandling, og flyter over i hverandre. Store beredskapsteam og IT-avdelinger kan dekke over det som muligens er hull i kompetanse og egnethet, spesielt i forbindelse med store cyberangrep. Ettersom det som sagt ikke per i dag har skjedd alvorlige cyberangrep i norsk VA-sektor, er dette imidlertid vanskelig å si noe om.

Teknologi

Cybertruslene har i kombinasjon med teknologisk utvikling og digitalisering også fremmet et behov for et utvidet IT-team i organisasjonene i sektoren, og et økt kompetansebehov for IKT-systemene hos aktørene i systemet. Jaatun, Røstum & Petersen (2013) presiserer at VA-systemene har gått fra å være mer eller mindre lukkede systemer som i raskt tempo er under oppgradering og digitalisering. Mange av systemene har gått fra å være manuelle og analoge prosesser til en fullstendig omveltning med nye teknologiske løsninger. Samtidig som at digitalisering medfører en rekke fordeler, skaper de også nye sårbarheter og mulige angrepsflater for ondsinnede aktører å innarbeide seg tilgang til. Informantene kommuniserer at det fremdeles i dag er utvidet bruk av sensorer og smart teknologi for effektiv styring av drift. Det gjør den helhetlige driften sømløs og tilsynelatende tryggere ved at feil i komponenter kan oppdages raskt. Informantene uttrykker at det finnes sårbarheter i systemene, men at de likevel

oppleves som robuste. Nettopp fordi det ikke har skjedd alvorlige cyberrelaterte hendelser i norsk VA-sektor, kan det argumenteres for at det kan foreligge mistolkninger og feiloppfattelser av systemets reelle tilstand.

Usikkerheter i IKT-systemer, nye koblinger mellom IT og driftskontrollsystemer, medfører også ringvirkninger til blant annet kulturen i organisasjonen. Når det ikke foreligger en felles forståelse, normer og holdninger til cybersikkerhet og digital sikkerhetskultur, vil dette kunne medføre ulik forståelse og kunnskap om systemene på tvers av virksomhetene. Det uttrykkes fra empiriske funn i dokumenter og intervjuer at det også er forskjeller blant IT, administrasjon og driftsteknikere. De arbeider med ulike nettverkssystemer, ulike kontrollsystemer og digitale infrastrukturer, noe som igjen kan tenkes å medføre menneskelig svikt. Dette er problematikk som ikke nødvendigvis kommer frem av oppgavens utforming i seg selv, men et uttalt element fra informantene.

Kultur

Alle organisasjoner har en kultur, og oftest også en sikkerhetskultur. Med cybertruslenes fremspring og utbredelse, er det også oppstått et behov for en utstrakt digital sikkerhetskultur. Fra empirien er det synlig fra trusselvurderingene og situasjonsbildene fra 2013 at digital sikkerhetskultur begynner å få mer oppmerksomhet. Samtlige dokumenter har manglende kompetanse, bevisstgjøring og behov for kurs og opplæring som overhengende tema.

Det digitale trusselbildet kan sies å ha vært et problem som i større grad påvirket et bredere nedslagsfelt privat, men rettet mot sentrale myndigheter og interesser nasjonalt. Rundt 2017 skjer det imidlertid et skifte, og cyberresponsmiljøer, NSMs grunnprinsipper for IKT-sikkerhet og bevisstgjøringskampanjer gjør sitt ultimate fremtog. Flere informanter bekrefter at tiltak er satt inn, det er økt fokus på sikkerhet på tvers av sektoren, og organisering av kurs og opplæring, men at det er vanskelig å få alle med på samme note. Digitale utfordringer fordrer de samme innstillingene som det en overordnet sikkerhetskultur vil gjøre, men synes å være vanskeligere å implementere. Det er tidkrevende og møysommelig arbeid å etablere en felles diskurs og forståelse for cybersikkerhet og IKT-kompetanse. Kunnskapsgrunnlaget, holdninger og verdier til ansatte i virksomhetene varierer, noe som også påvirker dynamikken blant de ansatte. Sett i lys av Weick & Sutcliffes fem prinsipper for «mindful organizing» i høypålitelige systemer, synes det å være en diskrepans mellom mål og praksis. Årvåkenhet og bevissthet omkring

handlinger, beslutninger og planlegging med mål om å forhindre ulykker og hendelser, krever en konstant innsats. I en sektor hvor oppgradering og digitalisering av systemer som tidligere har vært lukket for omverdenen, kan det argumenteres for at det kan være vanskelig å henge med i svingene. Men det er også nettopp derfor det er sentralt å innarbeide gode rutiner for IKT-håndtering. Reason (1997) sier at en det i en høypålitelig organisasjon er en forutsetning at de foreligger en informerende kultur. Denne kulturen skal fremme kulturer for rapportering, læring, fleksibilitet og rettferdighet.

Relasjoner

Cybertruslene har på mange måter forent organisasjoner ved å ha en felles målsetning i virksomheten. Målene fra organisasjonens ledelse er satt i tråd med gjeldende krav og bestemmelser ut fra et risikostyringsperspektiv. Samtidig medfører det også i større grad en flatere ansvarsfordeling, hvor ansatte på tvers av hierarki har et eget ansvar for å holde seg oppdatert på systemene, trusselbilder og trender i sitt arbeid. Til tross for at det i store organisasjoner ofte er mange avdelinger og mange ansatte, er dette et viktig tiltak for å styrke ansvarsbevissthet og skape tillitsbånd. Dette opplever samtlige informanter at er implementert i de fleste organisasjonene. Således er sikkerhetsarbeidet på mange måter desentralisert samtidig som det er sentralisert, noe som samsvarer med teorien om HRO. Engen, et al. (2021) peker på nettopp det at strukturell kompleksitet i organisering er effektive mål mot ulykker og hendelser, fordi rutiner og kompetanse er godt nok regulert og kommunisert på tvers av hierarkisk rollefordeling.

Interaksjoner

Funnene fra dokumentanalysen og intervjuer, peker på et økt fokus på nettverksbygging. Nettverksbygging kan tolkes som nettverk i umiddelbar omkrets, slik som nærliggende kommuner og interkommunale samarbeid, men også i VA-sektoren på tvers. I tillegg trekker særlig NSM frem cyberresponsmiljøer som et viktig støtteapparat og som en plattform for erfaringsdeling og kompetanseheving. Særlig de siste 5 årene har disse miljøene fått økt oppslutning, men ikke på langt nær nok til å sørge for at det er en jevn sikkerhetsressurs gjennom hele VA-sektoren. Informantene opplever at mange store kommuner og interkommunale samarbeid verner om egen organisasjon og utfører operasjoner, opplæring og hendelseshåndtering i stor grad på egenhånd. På den andre siden er det mange mindre

kommuner og vannverk som ikke har samme ressurser verken økonomisk eller som arbeidskraft.

En bekymring som utmerker seg uavhengig av medlemskap i cyberresponsmiljøer, er at sårbarheter, hendelser og erfaringer ikke snakkes nok om. Som en informant sier;

«Hackerne deler informasjon med hverandre *hele tiden*. Det gjør ikke vi. Og det må vi!»
(Informant IT1)

Med tanke på informasjonsdeling, er det altså noe å lære av de organiserte kriminelle – kommunikasjon og å utvikle plattformer for deling av erfaringer og viktig informasjon med hverandre. Norsk Vann har i flere år fungert som VA-bransjens interesseorgan, og hjelper til med kompetanseutvikling, men har også fungert som en samlingsarena for de ulike aktørene i VA-bransjen. Dette har gitt rom for interaksjoner mellom kommuner, underleverandører, kontraktører og andre relevante parter, noe deltakende virksomheter har hatt god nytte av. I et HRO-perspektiv er dette også svært hensiktsmessig med tanke på å opparbeide kunnskap om det man ikke allerede er klar over at man ikke vet. Ved å utveksle erfaringer og kompetanse, vil dette gi ringvirkninger på organisasjonens relasjoner seg imellom, men også fra et kulturelt perspektiv. Å opprettholde en god digital sikkerhetskultur, er forutsatt at man kjenner til sårbarheter, åpninger og trusselformer som kan oppstå også i egne systemer. Dette er imidlertid en komplisert prosess, fordi det

Oppsummerende refleksjoner

Fra et systemteoretisk perspektiv, er det tydelig at cybertrusler både påvirker enkeltdelene av organisasjoner, men også organisasjonene som helhet. Til tross for at kommuner av ulike størrelser har ulike tilnærminger til strukturoppsett i sine organisasjoner, finnes det likevel noen fellestrekk som bunner i håndtering av cybertrusler og av systemenes kompleksitet. Organisasjonsstrukturene i VA-sektoren har ifølge de empiriske funnene fra intervjuer og dokumentanalyse trekk både fra NAT og HRO. De er begge systemteoretiske perspektiver som beskriver systemenes kompleksitet. Systemenes kompleksitet, ulikheter i løse eller tette koplinger og lineære eller komplekse interaksjoner, kan synes å bunne i en fragmentering av tilsynsmyndigheter, reguleringer og lovverk, og ikke minst kompetanseforskjeller når det kommer til cybersikkerhet. Fellesnevneren for systemene, tett koplet eller ei, er at de består av mange deler som påvirker og er gjensidig avhenging av hverandre. Sett i lys av

pentagonmodellen, er arbeid med digital sikkerhetskultur både blitt løftet frem som en viktig del av organisasjonen, men samtidig også en utfordring å få alle med på. De formelle strukturene i organisasjonen er styrt av flere og mer målrettede tiltak fra myndighetssiden, noe som fører til større behov for mest mulig korrekt risikostyring. På interaksjonsdelen, handler det om endringer i kommunikasjon og innføring av cyberresponsmiljøer. Av informantene ses dette som utelukkende positivt, men igjen at det krever innsats i form av tid og penger, og blir derfor ofte nedprioritert. Sist men ikke minst, har teknologidelen av pentagonmodellen fått et løft de siste årene. Mange av prosesskomponenter, mekanismer og driftskontrollsystemer samles på samme system med mål om å sørge for både en trygg og effektiv drift. Ironisk nok er det også nettopp digitaliseringen av disse som også utgjør noen av de største digitale utfordringene og sårbarhetene for VA-sektoren.

Særlig i en tid hvor det foregår et omfattende oppgraderingsarbeid og digitalisering av kommunenes vann- og avløpsverk, er det utfordrende å klassifisere organisasjonene som fullstendig pålitelige eller sikre mot cyberangrep. Det synes passende å se organisasjonene i VA-sektoren gjennom Levesons (2011) prinsipp, om at det i høypålitelige organisasjoner kan eksistere pålitelige men usikre systemer, så vel som upålitelige men sikre systemer. På sett og vis kan Levesons (2011) utsagn sies å trekke elementer fra både NAT og HRO i beskrivelsen av høyteknologiske systemer som også passer for VA-sektoren.

7. Konklusjon

Drøftingen av de empiriske funnene har satt cybertruslene i kontekst til organisatoriske trekk og endringer i strukturer. For å kunne besvare problemstillingen «hvordan har cybertrusler påvirket organisasjonsstrukturen i vann- og avløpssektoren de siste 10 årene», har det vært hensiktsmessig å besvare forskningsspørsmålene i drøftingskapittelet. Forskningsspørsmål 1 har bidratt til å forstå hvordan cybertruslene har økt i takt med digitalisering og globale teknologiske fremskritt. I etterkant av pandemi og krig, har trusselaktører fått øynene opp for en bredere angrepsflate, med mål om statlig etterretning og sabotasje. Dette er en trend som særlig de siste årene har vist seg gjeldende, og som truer kritisk infrastruktur i Norge. Truslene mot VA-sektoren er basert på disse vurderingene, men har fått mer oppmerksomhet etter hendelser internasjonalt. Forskningsspørsmål 2 har bidratt til forståelse for hvordan de ulike delene av en organisasjon fungerer i et helhetlig samspill, og som stadig påvirker hverandre. Empiriske funn og drøftingen av disse har pekt ut spesielle utfordringer og påvirkninger cybertruslene har påført organisasjonsstrukturer i vann- og avløpsbransjen.

Oppgavens problemstilling kan besvares ved å trekke frem de viktigste funnene fra de ulike delene av en organisasjon med henblikk på pentagonmodellen. Det er først og fremst en ytre påvirkningskraft fra cybertrusler og teknologi/digitalisering som utgjør store endringer i de formelle forholdene. Disse ytre forholdene skaper endringer i lovverk, reglement og krav til målrettet risikostyring. Organisasjonens formelle struktur blir påvirket av at ansvarsfordeling og myndighet fordeles bredere på organisasjonen, samtidig som at det stilles skjerpede krav til risiko- og sårbarhetsanalyser, beredskapsteam og beredskapsøvelser og øvrig sikring. Slike endringer medfører permanente og semipermanente endringer i prosedyrer som er nødvendig for å opprettholde et sikkert system. Organisasjonenes teknologi, blir påvirket i form av stadig fornyelse av gamle IT-systemer, automatisering av manuelle prosesser, bruk av sensorstyrte prosesser, IKT-tjenester og skylagring som utgjør strukturelle endringer i form av færre driftsteknikere og flere IT-teknikere. IT-avdelingene blir større og har stor innvirkning på organisasjonen som helhet. Her skapes rammeverk for digital sikkerhetskultur, kontrollstyring og overvåkning av digitale og automatiserte prosesser lengre ned i virksomheten. Det er samtidig også her at cybertruslene får slå rot, noe som skaper en dynamikk som er vanskelig å balansere. For organisasjonens kultur, altså sikkerhetskultur, normer og holdninger, spiller cybertrusler en stor rolle. Over tiårsperioden som er undersøkt, er digital sikkerhetskultur et av de største og mest gjentatte temaene. Det kommer frem av empiriske funn at

kompetansebygging gjennom kurs, bevisstgjøring og holdningskampanjer preger hele organisasjonen i enormt stor grad i dag kontra for 10 år siden. Likevel er det over tiårsperioden et frafall i forsøkene på å bedre digital sikkerhetsforståelse, og det er utfordrende å ha kontroll på hvor mange som setter seg godt nok inn i tematikken. Sist, men ikke minst, er det et større behov for interaksjon innad og utad i organisasjonene. Spesielt i den siste femårsperioden har det vokst frem et stort antall cyberresponsmiljøer og digitale støtteapparater. Med tanke på organisasjonenes variasjon av kompetanse, grad av digitalisering, har dette vært et viktig tiltak. Noen har involvert seg, mens andre ikke. Likevel har disse støtteapparatene sørget for en plattform for VA-aktører til å snakke sammen, dele erfaringer, bekymringer og forslag til tiltak. Dette tar de igjen med seg til organisasjonen, og bidrar til nye normdannelser, forslag til teknologiske løsninger og ideer.

Cybertruslene har på bakgrunn av dette altså ikke hatt innvirkning på enkeltdeler i organisasjoner, men spiller en større eller mindre rolle i alle delene av organisasjonene, og på tvers av dem. Påvirkningene må ses i et helhetlig perspektiv, som i systemteorien. En endring i en del, vil medføre endring i en eller flere andre deler. Alle delene virker inn på hverandre. Organisasjonene i VA-strukturen kan betraktes likeledes. Uavhengig av kommunestørrelse, ressurser eller inventar, vil cybertrusler og cyberangrep kunne ha innvirkning på langt flere enn kun den angrepne organisasjonen.

7.1 Forslag til videre forskning

Denne oppgaven har undersøkt hvordan cybertrusler har påvirket organisasjonsstrukturer i norsk vann- og avløpssektor. I takt med en omfattende digitalisering av norsk offentlig sektor, og stadig presserende cybertrusler, kunne det vært interessant å se hvordan truslene påvirker organisasjonsstrukturer i VA-sektoren i større skala. Denne oppgaven viser til funn fra et fåtall kommuner og underleverandører, men det er et forslag å se på cyberproblematikken i en større kontekst. En slik undersøkelse kunne gitt en pekepinn på sektorens digitale tilstand, mål på resiliens og om det eksisterer generelle strukturendringer i organisasjonene på bakgrunn av dette. Samtidig som at VA-sektoren er en kritisk infrastruktur, kunne det også vært interessant å overføre tematikken til andre sektorer som behandler kritisk infrastruktur og samfunnsfunksjoner. Dette vil også kunne bidra til å inspirere andre virksomheter og organisasjoner til å i større grad implementere sikkerhetstiltak spesifikt rettet mot cybertrusler og cyberangrep.

8. Litteraturliste

Aase, T. H., & Fossaskåret, E. (2014). *Skapte virkeligheter. Om produksjon og tolkning av kvalitative data. 2. utg.* . Universitetsforlaget.

Almklov, P. G., Antonsen, S., Fenstad, J., Røstum, J., Sjøvold, F. & Værnes, R. (2010). *Restrukturering av norsk VA-bransje og konsekvenser for samfunnssikkerhet.* NTNU Samfunnsforskning.

Andersen, S. S. (2006). *Aktiv informantintervjuing*. Norsk Statsvitenskapelig Tidsskrift. 22(3), s. 278-298.

Aven, T., Boyesen, M., Njå, O., Olsen, K.H. & Sandve, K. (2004). *Samfunnssikkerhet*. Oslo: Universitetsforlaget.

Aven, T. & Thekdi, S. (2022). *Risk Science. An Introduction*. Routledge

Bijker, W. E., Hughes, T. P. & Pinch, T. (2012). *The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology*. London/Cambridge: The MIT Press

Blaikie, N., & Priest, J. (2019). *Designing Social Research. The Logic of Anticipation. (3rd ed.).* Malden.: Polity Press.

Danermark, B., Ekström, M., & Karlsson, J. C. (2019). *Explaining Society. Critical Realism in the Social Sciences (2nd ed.).* New York: Routhledge.

Direktoratet for samfunnssikkerhet og beredskap (DSB). (2016). *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid? Versjon 1.0*. Hentet fra: https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Drikkevannsforskriften. (2016). *Forskrift om vannforsyning og drikkevann (LOV-2016-12-22-1868)*. Lovdata. Hentet fra: https://lovdata.no/forskrift/2016-12-22-1868

Enander, L., Hauland, G. & Fotland, K. E. (2015). *Sikkerhetsstyring for vannbransjen. Rapport 213.* Norsk Vann

Engen, O. A., Gould, K. A., Kruke, B. I., Lindøe, P. H., Olsen, K. H., & Olsen, O. E. (2021). *Perspektiver på samfunnssikkerhet. 2. utg.* Oslo: Cappelen Damm Akademisk.

Etterretningstjenesten. (2013). *Fokus 2013*. Hentet fra: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus%202013.pdf/_/attachment/inline/da91de2b-44d1-45df-9a18-45daee59bb09:79de99796af76303df3195e7476c8fb650f0ced6/Fokus%202013.pdf

Etterretningstjenesten. (2017). *Fokus 2017*. Hentet fra: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus%202017.pdf/_/attachment/inline/1598e832-8978-4c14-8c02-0a19ededd8f0:0e0b2667071f959c2629358c674de5be18c31a75/Fokus%202017.pdf

Etterretningstjenesten. (2022). *Fokus 2022*. Hentet fra: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus-2022-til-web.pdf/_/attachment/inline/184ffb15-e45f-42ac-b1e0-32292cd4e390:e4014ab4d0e3bd8b2509e7974430fe121e0473ba/Fokus-2022-til-web.pdf

Forurensningsloven. (1981). *Lov om vern mot forurensninger og om avfall (LOV-1981-03-13-06)*. Lovdata. Hentet fra: https://lovdata.no/lov/1981-03-13-6

Halvorsen, K. (2008). *Å forske på samfunnet. En innføring i samfunnsvitenskapelig metode*. Oslo: Cappelen Akademisk Forlag

Hollnagel, E., Woods, D. D. & Leveson, N. G. (2006). *Resilience Engineering – Concepts and Precepts*. Ashgate Publishing Limited

Jaatun, M. G., Røstum, J. & Petersen, S. (2013). *Veiledning for sikkerhet av driftskontrollsystemer for VA-systemer. Rapport 195*. Norsk Vann

Justis- og beredskapsdepartementet. (2017). IKT-sikkerhet – Et felles ansvar. (Mld. St. 38: 2016-2017). Hentet fra: https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/?ch=1

Kast, F. E. & Rosenzweig, J. E. (1973). *Contingency Views of Organization and Management*. Chicaco: Science Research Associates

Kommunal- og moderniseringsdepartementet. (2021). *Veileder for beregning av selvkost og gebyrforskrift i byggesaker.* Hentet fra: https://www.regjeringen.no/contentassets/b915d2f464d74fa8ad22994ac934340f/no/pdfs/h-2514-b-veileder-for-beregning-av-selvkost_v2.pdf

Kovács, G. & Spens, K.M. (2005). *Abductive reasoning in logistics research*. International Journal of Physical Distribution & Logistics Management, Vol. 35 No. 2, s. 132-144.

Kvale, S. & Brinkmann, S. (2021). *Det kvalitative forskningsintervju. 3. utg*. Oslo: Gyldendal Akademisk

Leveson, N. G. (2011). *Applying systems thinking to analyze and learn from events. Safety Science*, Vol. 49 (1), s. 55-64.

Lægreid, P. & Christensen, T. (2007). *Transcending New Public Management: The Transformation of Public Sector Reforms*. London/New York: Routledge

Mintzberg, H. (1979). *The Structuring of Organizations*. Pearson.

Nasjonal Sikkerhetsmyndighet. (2013). *Nasjonal sikkerhetsmyndighet er Norges ekspertorgan for informasjons- og objektsikkerhet. Årsrapport 2013*. Hentet fra: https://nsm.no/getfile.php/133385-1591858822/NSM/Filer/Dokumenter/Rapporter/nsm-arsrapport-2013.pdf

Nasjonal Sikkerhetsmyndighet. (2017). *Helhetlig IKT-risikobilde 2017*. Hentet fra: https://nsm.no/getfile.php/133675-1592831718/NSM/Filer/Dokumenter/Rapporter/helhetlig_ikt-risikobilde_2017_orig_enkeltsider_low.pdf

Nasjonal Sikkerhetsmyndighet. (2020). *NSMs Grunnprinsipper for IKT-sikkerhet. Versjon 2.0.* Hentet fra: https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

Nasjonal Sikkerhetsmyndighet. (2022). *Nasjonalt digitalt risikobilde 2022*. Hentet fra: https://nsm.no/getfile.php/1311995-1664550278/NSM/Filer/Dokumenter/Rapporter/NDIG%202022.pdf

Nasjonal Sikkerhetsmyndighet. (u.å.). *Dette er NSM*. Hentet 30. mai 2023 fra: https://nsm.no/om-oss/dette-er-nsm/

Njå, O., Sommer, M., Rake, E. L. & Braut, G. S. (2020). *Samfunnssikkerhet. Analyse, styring og evaluering*. Oslo: Universitetsforlaget

Norsk Vann. (2023). *Vann- og avløp*. Hentet fra: https://va-finansiering.no/selvkost/vann-og-avlop/

Norsk Vann. (2021). *Investeringsbehovet i kommunalt eide vann- og avløpsanlegg fortsetter å øke*. Hentet fra Norsk Vann: https://norskvann.no/interessepolitikk/investeringsbehovet-i-vann-og-avlopsanlegg/

Perrow, C. (1984). *Normal Accidents. Living with High-risk Technologies.* New Jersey: Princeton University Press.

Politiets sikkerhetstjeneste. (2013). *Nasjonal trusselvurdering 2013*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2013/

Politiets sikkerhetstjeneste. (2017). *Nasjonal trusselvurdering 2017*. Hentet fra: https://pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2017/

Politiets sikkerhetstjeneste. (2022). *Nasjonal trusselvurdering 2022*. Hentet fra: https://www.pst.no/globalassets/ntv/2022/nasjonal-trusselvurdering-2022-pa-norsk.pdf

Reason, J. (1997) *Managing the Risks of Organizational Accidents*. New York: Ashgate Publishing.

Regjeringen. (2014). Digitalisering i offentlig sektor. Hentet fra: https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringen-i-offentlig-sektor/id2340245/

Regjeringen. (2022, 2. 3.). *Liste over kritiske samfunnsfunksjoner.* Hentet fra Samfunnssikkerhet og beredskap: https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/liste-over-kritiske-samfunnsfunksjoner/id2695609/

Riis, L. & Hareide, A. (2017). Sikring av vannforsyning mot tilsiktede uønskede hendelser. Rapport 229. Norsk Vann

Sikkerhetsloven. (2018). *Lov om nasjonal sikkerhet (LOV-2018-06-01-24).* Lovdata. Hentet fra: https://lovdata.no/lov/2018-06-01-24

Sivilbeskyttelsesloven. (2010). *Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (LOV-2010-06-25-45).* Lovdata. Hentet fra: https://lovdata.no/lov/2010-06-25-45

Schiefloe, P. M. (2021). *Organisasjonsanalyse.* Bergen: Fagbokforlaget.

Tøndel, I. A., Jaatun, M. G. & Røstum, J. (2013). *IKT og sikkerhet i VA-sektoren: Hva kan gå galt?* VANN, Vol 02, s. 265-269.

Ugarelli, R., Raspati, G., Selseth, I., Jaatun, M. G., Røstum, J., Rishovd, H., & Furuberg, K. (2021). *Cyber-sikkerhet i VA-sektoren og bidraget fra STOP-IT-prosjektet.* VANN, Vol. 03, ss. 253-261. Norsk Vannforening

Ulsrud, O. A. (2021, 2. Mars). *Angrep på vannverk i Florida*. Hentet fra: https://kommunecsirt.no/nyheter-og-artikler/angrep-på-vannverket-i-oldsmar-florida-5-februar-2021

Vass- og avløpsanleggslova. (2012). *Lov om kommunale vass- og avløpsanlegg (LOV-2012-03-16-12).* Lovdata. Hentet fra: https://lovdata.no/lov/2012-03-16-12

Weick, K. E. & Sutcliffe, K. M. (2015). *Managing the Unexpected: Sustained Performance in a Complex World*. Jossey-Bass

VEDLEGG I

Samtykkeerklæring

Bakgrunn og formål med studien:

I forbindelse med min masteroppgave i samfunnssikkerhet ved Universitetet i Stavanger, skal jeg gjennomføre flere intervjuer. Tema for oppgaven er cybersikkerhet i vannbransjen, hvor formålet med studien er å undersøke hvordan cybertrusler har påvirket organisasjonsstrukturen i vann- og avløpssektoren de siste 10 årene.

Personopplysninger:

Jeg benytter retningslinjene fra NSD som gjelder oppbevaring av sensitive opplysninger i mål om anonymitet og konfidensialitet. Det er ønskelig å gjennomføre intervju med opptak med diktafon for å sikre korrekt transkribering og gjengivelse i oppgaven. Opptaket vil bli slettet umiddelbart etter transkribering. Det vil ikke bli samlet inn personopplysninger, og informant og virksomhet vil bli anonymisert i oppgaven.

Deltakelse i studien er frivillig, og du kan når som helst trekke deg som deltaker uten å oppgi grunn. Alle oppsamlede data vil i dette tilfelle slettes umiddelbart.

Ved å signere denne erklæringen godtar du at opplysningene som har blitt oppgitt under intervju benyttes videre i oppgaven.

Signatur:

.....	.....
Lene Kristin Vatland	Respondent
Masterstudent i Samfunnssikkerhet	
Universitetet i Stavanger	

VEDLEGG II

INTERVJUGUIDE

Introduksjonsspørsmål:
Kan du først fortelle kort om din bakgrunn, og om din erfaring knyttet til IKT-sikkerhet og VA-sektoren?

Tema FS1: Cybersikkerhet/Utvikling av cybertrusler

1. Hva karakteriseres som en *cybertrussel* og et *cyberangrep* i VA-sektoren?

2. Vil du si at det er en høy cyberrisiko i VA-sektoren?

3. Kan du si noe om hva som preger trusselbildet mot VA-sektoren i 2022/2023?
   - Hvem er de utpregede trussel-aktørene og hva er deres motivasjon?
   - Blir utilsiktede hendelser kategorisert som trusler?

4. Det er blant annet av NSM og Norsk Vann uttalt ved flere anledninger de siste årene at norske vannforsyningsanlegg er for dårlig sikret og at mulighetene for cyberangrep gjennom de digitale systemene og OT-systemer er store. Hva tenker du er de største utfordringene med fysisk og digital sikring av systemene?

5. Vannbransjen i Norge utgjør en veldig sammensatt verdikjede, med behov for tett samhandling. Fordi den består av kommunale og interkommunale vann- og avløpsverk, teknologibedrifter, konsulentselskaper, entreprenører og håndtverkbedrifter, er sektoren derfor også veldig kompleks.
   - Tenker du at samhandlingen er god nok mellom av aktørene med tanke på sikkerhet? Hvorfor/hvorfor ikke?
   - Skaper denne kompleksiteten utfordringer knyttet til IKT-sikkerhet i VA-sektoren? I så fall hvilke?

6. Av hendelser og trusler som har skjedd – er det mest tilsiktede eller utilsiktede hendelser?

7. Kan du gi noen eksempler på noen konkrete endringer i trusselbildet for VA-sektoren i løpet av de siste 10 årene?

Tema FS2: Organisatoriske endringer

8. Opplever du at opparbeidelse og opprettholdelse av digital sikkerhetskultur er en prioritet i din virksomhet? Hvordan er dette organisert?

9. Fører uønskede hendelser og forandring i trusselbilde til endringer i praksis?
   - Skjer endringene i så fall hurtig nok?

10. Tenker du at digital kompetanseheving i VA-sektoren på generell basis er tilfredsstillende organisert med tanke på nåværende trusselbilde?
    - Hva kan gjøres annerledes?

11. Er deres kommune/virksomhet medlem i Kommune CSIRT/KraftCERT?
    - Hvis ja: Hvilke fordeler fører det til for dere organisatorisk sett?
    - Hvis nei: Hvorfor ikke?

12. Av 356 kommuner i Norge er kun ca 60 kommuner som er medlem i Kommune - CSIRT. Hvorfor er det slik, og hva kan konsekvensene av å ikke være medlem være?

13. Hvor utbredt er Bestiller-Utfører-modellen i norsk vannbransje i dag?

14. Hvilken effekt mener du BUM har på sikkerhetsstyring og organisasjonsstruktur på tvers av sektoren?

15. På hvilken måte påvirker tjenesteutsetting av IKT-tjenester kommunenes sårbarhet og robusthet?

16. Hvordan påvirker digitalisering, teknologisk utvikling og innovasjon robusthet i VA-sektoren?

17. På tross av vannbransjens komplekse sammensetting, vil du si at kommunikasjon og erfaringsdeling basert på tidligere hendelser eller utfordringer er transparent og tilgjengelig på tvers av etater og virksomheter?

18. Har det skjedd noen konkrete organisatoriske endringer på generell basis i VA-sektoren de siste 10 årene med tanke på cybersikkerhet?