DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

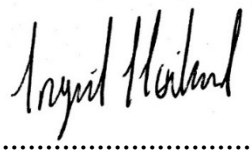
Studieprogram/spesialisering:

Master i samfunnssikkerhet

Vårsemesteret, 2022

Åpen / ~~Konfidensiell~~

Forfatter: Ingrid Høiland



.....
(signatur forfatter)

Fagansvarlig: Ole Andreas Hegland Engen

Veileder(e): Henrik Bjelland

Tittel på masteroppgaven:
Samvirkestrategi i cyber-beredskap:
En studie av operasjonalisering av samvirke i beredskapsøvelsen Cyber22.

Engelsk tittel:
Collaborative strategy in cyber preparedness:
A study of the operationalization of collaboration in the emergency exercise Cyber22.

Studiepoeng: 30

Emneord:
Beredskap, fullskalaøvelse, samvirke, cybertrusler, systemtenkning, cyber-resiliens, risiko og sårbarhet, samfunnssikkerhet, konseptualisering, betalingssystem og finanssektor

Sidetall: 98/112

+ vedlegg/annet: 14/112

Stavanger, 15.juni 2022
dato/år

Samvirkestrategi i cyber-beredskap

En studie av operasjonalisering av samvirke i beredskapsøvelsen Cyber22

Ingrid Høiland

Masterstudium i samfunnssikkerhet

Våren 2022

Universitetet i Stavanger

Det teknisk-naturvitenskapelige fakultet

Institutt for industriell økonomi, risikostyring og planlegging

Sammendrag

Kompleksitet og gjensidige avhengigheter i cyberdomenet utgjør sårbarheter i samfunnskritiske funksjoner, som finansiell infrastruktur og betalingssystemer. Dette har ført til et krav og økt fokus på samarbeid på tvers av virksomheter. Cybertrusselen kan ikke håndteres alene, men krever samvirke. Dette generer et behov og en forståelse for hvordan samvirke kan intensiveres og styrkes.

I lys av dette undersøkes det i denne masteroppgaven hvordan samvirke operasjonaliseres i planlegging og gjennomføring av beredskapsøvelsen Cyber22 i finanssektoren. Konseptualisering av samvirke, altså hvordan samvirke anvendes og tolkes er fremstilt som følge av analysen av resultatene. Det er dokumentstudier, intervju- og observasjonsdata som bidrar til å nå oppgavens målsetting. Målet med oppgaven er å rette fokus på en økt samvirkestrategi for å styrke cyber-beredskapen.

I oppgaven har det blitt forsket frem ulike aspekter som utgjør samvirke. Oppgaven har synliggjort at et godt samvirke forutsetter at de ulike aspektene aktivt anvendes og vurderes av organisasjoner. Evaluering av samvirke fra en tidligere beredskapsøvelse førte til bevisstgjøring i arbeidet med intensivering av samvirke. Funn tilsier at fullskala beredskapsøvelser er en god måte å evaluere både det interne samvirke i organisasjonene, og det eksterne samvirket på tvers av sektoren. I øvelsen Cyber22 ble det gjort et strategisk valg om å fokusere på mestring, fremfor å teste deltakernes evner til improvisasjon. Planlegging av øvelsen har vært vel så viktig som gjennomføringen. Det er i planleggingen grunnlaget for samvirke i øvelsen er lagt. Det anvendes systemteoretisk analyse for å undersøke hvordan nivåene i finanssystemet interagerer i et felles system. Dette for å kunne forstå hva som oppleves som god praksis for samvirke.

Teori om cyber-resiliens har blitt brukt gjennomgående for å analysere og drøfte datamaterialet. Teorien erfares som nyttig og sammenfaller med funnene. Samtidig åpnes det også opp for diskusjon om hvordan testing av samvirke i øvelser kan bidra til en styrket cyber-beredskap. Oppgaven konkluderer med at forhåndsetablering av relasjoner og involvering av eksterne deltakere er essensielle faktorer for å oppnå et tilstrekkelig samvirke både i en øvelse og under en reell hendelse. Den visuelle samvirkeanalysen bidrar til å synliggjøre relasjonene mellom deltakerne i øvelsen som bidrar til å styrke en felles mental modell.

Forord

Denne oppgaven har gitt meg muligheten til å undersøke nærmere, og å smelte sammen temaet samvirke i krise- og beredskapsarbeid med temaet cybersikkerhet. Det har vært en intens kunnskapsreise som jeg vet vil gjøre meg enda mer rustet til møte med komplekse sikkerhetsutfordringer i fremtiden.

Først og fremst vil jeg rette en stor takk til Norges Bank, og de menneskene som står bak beredskapsøvelsen Cyber22. Dere har gitt meg en unik mulighet til å lære og forstå sikkerhetsarbeidet fra innsiden av organisasjonen – og dessuten, uten dere hadde heller ikke denne oppgaven blitt realisert. Jeg vil også si tusen takk til informantene som har stilt opp på intervju. Deres kunnskap, tanker og erfaringer er selve fundamentet i oppgaven.

Jeg vil også takke min veileder Henrik Bjelland, Førsteamanuensis II ved Universitetet i Stavanger. Ditt kunnskapsbidrag, gode innspill og konstruktive tilbakemeldinger har bidratt til at jeg sitter igjen med et produkt jeg kan være stolt av.

Sist, men ikke minst, tusen takk til min samboer, familie og venner som har støttet meg og vist meg tålmodighet.

Ingrid Høiland
Stavanger, 15.juni 2022

Innhold

Tabell- og figuroversikt:

Forkortelser:

BFI	Beredskapsutvalget for finansiell infrastruktur
CERT	Computer Emergency Response Team
DFS	Department of Financial Services
DORA	Digital Operational Resilience Act
DSB	Direktoratet for samfunnssikkerhet og beredskap
ENISA	European Union Agency for Network and Information Security
FIN	Finansdepartementet
HRO	High Reliablility Organizations (Høy pålitelige organisasjoner)
IKT	Informasjons og kommunikasjonsteknologi
LOM	Liquidity Optimization Mechanism
Meld. St	Melding til Stortinget
NB	Norges Bank
NBO	Norges Bank oppgjørssystem
NCSC	Nasjonalt cybersikkerhetssenter
NFCERT	Nordic Financial Computer Emergency Response Team
NOU	Norsk offentlig utredning
NSM	Nasjonal sikkerhetsmyndighet
Prop.	Proposisjoner
PST	Politiets sikkerhetstjeneste
RTM	Real Time Mechanism
TIBER	Threat Intelligence-based Ethical Red Teaming
VDI	Varslingssystemet for digital infrastruktur

1. Introduksjon

«Plans are worthless, but planning is everything.»
- Dwight D. Eisenhower (1957)

13. desember 2020 ble det amerikanske programleverandør-selskapet Solarwinds utsatt for et svært omfattende dataangrep. Angrepet rammet 18 000 organisasjoner verden rundt (Lysne, 2020; NSM, 2022, s. 21). Angrepet rammet også i underkant av 100 bedrifter i New Yorks finansindustri (DFS, 2021). Solarwinds-angrepet er per dags dato det mest fremtredende og utbredte «Software supply chain»[1]-angrepet. Cyberangrepet synliggjør en ekspanderende sårbarhet i Informasjons- og kommunikasjonsteknologi-strukturen (IKT). Den gjensidige avhengigheten mellom organisasjoner gjør at ett enkeltstående angrep kan føre til katastrofale konsekvenser – både for avanserte statlige etater og private virksomheter (DFS, 2021, s. 2). Den gjensidige avhengigheten mellom sektorer og organisasjoner understreker et behov for samhandling på tvers av ansvarsområdene når det gjelder krisehåndtering og beredskapsarbeid (Meld. st. 29, 2011-2012, s. 9). Erfaringer fra tidligere cyberhendelser illustrerer også et ytterligere behov for samhandling mellom aktører i beredskapsarbeidet.

Samvirkeprinsippet ble formelt introdusert i forbindelse med organiseringen av redningstjenesten på 1950-1960-tallet. I 1953 ble Redningsutvalget oppnevnt, og samvirkeprinsippet ble dermed et ankerfeste i inkluderingen av både offentlige og private (frivillige) institusjoner som redningsinnsats på land og sjø. Grunnlaget for samvirke i beredskap og krisehåndtering bunnet i et behov for bedre koordinering av redningsinnsatsen, samt mangel på samarbeid med felles ledelse. Leder for utvalget, Politimester Simon Østmoe, viste til sine erfaringer fra krigsårene. Behovet for samvirke ble tydelig illustrert under Nazi-Tysklands okkupasjon av Norge under 2.verdenskrig. En landskrise som krevde samhandling og samhold på tvers av grenser (Aasland & Braut, 2018, s. 181). Likevel ble ikke samvirkeprinsippet innført som et av hovedprinsippene innen beredskapsarbeid og krisehåndtering før etter 22. juli 2011. Den overlastede røde gummibåten med politiressurser på Tyrifjorden ble et tydelig bilde på ressursene som ikke fant hverandre, og selve symbolet på det manglende samvirke under håndteringen av 22. juli-terroren (NOU 2012: 14, s. 134).

[1] «Software supply chain», også kalt tredjepartsangrep, er et cyberangrep der man infiltrerer et system gjennom en ekstern leverandør som gir angriperen tilgang til systemene og dataene til tredjeparten.

I den nasjonale strategien for digital sikkerhet (Departementene, 2019) hevdes det at teknologien vil endres de kommende årene. Det beskrives at vi vil få digitale tjenester vi knapt kan forestille oss. Selv om digitaliseringen bidrar til effektivisering, kommer den også med nye utfordringer. Den raske utviklingen fører til at det er utfordrende å forutse risikobildet (Departementene, 2019, s. 6). Cyberangrep beskrives i flere trusselrapporter som en sentral del av trusselbildet, der det er et forhøyet aktivitetsnivå mot norske virksomheter og institusjoner. Samvirkeprinsippet trekkes frem som helt sentralt når departement og virksomheter skal operasjonalisere sikkerhetsloven i møte med cybertrusler (NSM, 2021, s. 5; NSM, 2018). I den nyeste trusselrapporten til Nasjonale sikkerhetsmyndigheter (NSM) beskrives et taktskifte i cyberaktivitet. Fra 2019 til 2021 ser NSM en tredobling i antall alvorlige cyberhendelser. Med dagens spente sikkerhetssituasjon i Europa forventes det at cyberhendelser blir enda mer fremtredende de kommende årene (NSM, 2022, s. 8-9).

Finanssektoren er bygget på en IKT-struktur, som med sin komplekse verdikjede, er utsatt for både tilsiktete og utilsiktede handlinger. I NSMs risikorapport (2022) vises det til at statlige trusselaktører er en stor risiko i det digitale trusselbildet (NSM, 2022; PST, 2022). Analysene av Solarwind-angrepet og angrepet på Stortinget høsten 2020 viser at det er kjente statlige trusselaktører som står bak angrepene (DFS, 2021, s. 2: NSM, 2021). Statlige trusselaktører er å anse som profesjonelle aktører, med stor kapasitet og omfattende ressurser til rådighet. Konsekvensene av cyberangrep kan knyttes til store økonomiske tap, som kan være kritiske både for enkeltpersoner og organisasjoner, nasjonalt og internasjonalt. For å kunne møte disse utfordringene er det viktig at sektoren har etablert en god beredskap. En sentral del av beredskapsarbeidet er å drive med relevant trening og å øve på scenarioer som kan inntreffe. Øvelser er nødvendige for å bli bedre til både å forebygge og å håndtere alvorlige og sjeldne hendelser (NOU 2015: 13, s. 182-183). Det er ikke bare en forutsetning for god krisehåndtering, men også nødvendig for å evaluere beredskapen som er etablert i organisasjonen (Engen et al., 2016; NOU 2015: 13, s. 136).

1.1 Cyber22

Cyber22 er en fullskala beredskapsøvelse som har vært hovedgjenstand for analyse i denne oppgaven. Norges Bank (NB) har initiert og ledet planlegging og gjennomføring av øvelsen. Det gis en mer utdypende beskrivelse av Cyber22 i delkapittel 3.5.

1.2 Problemstilling og forskningsspørsmål

Formålet med denne studien er å få økt kunnskap om betydningen av samvirke i planprosessen og gjennomføringen av en beredskapsøvelse i finanssektoren. Studien fokuserer på den interne planleggingsprosessen i forkant av øvelsen Cyber22. Ved å fordype seg i en konkret øvelse kan en få verdifull innsikt i hvilke mulige utfordringer og styrker som ligger til grunn for et godt samvirke. Problemstillingen er følgende:

> ***På hvilken måte operasjonaliseres samvirke i planprosess og gjennomføring av beredskapsøvelsen Cyber22, og hvilken innsikt gir dette i samvirke som strategi for cyber-beredskap?***

Med utgangspunkt i denne problemstillingen er det utarbeidet tre forskningsspørsmål som, på hver sin måte, vil være veiledende i besvarelse av problemstillingen. Første forskningsspørsmål skal gi oppgaven dybde, fortolkning av samvirke som konsept, og hvordan konseptet kan sees i sammenheng med beredskapsøvelsen Cyber22.

Hva er samvirke?

Videre er det andre forskningsspørsmålet utarbeidet for å kunne si noe om hvilken betydning samvirke har for å oppnå god cybersikkerhet i finanssektoren. Ved å undersøke nærmere betydningen av samvirke vil en kunne finne konkrete tiltak som kan bidra til å styrke samvirke i sektoren. Dette vil kunne si noe om hvordan og hvilke ressurser sektoren skal prioritere når det kommer til samhandling og koordinering.

Hvorfor er samvirke viktig for å oppnå god cybersikkerhet i finanssektoren?

Det tredje forskningsspørsmålet er utarbeidet for å undersøke samvirke i beredskapsøvelsen Cyber22. Det vil derfor være hensiktsmessig å kartlegge i hvilken grad samvirke oppnås. Dette vil belyse hvordan kommende beredskapsøvelser skal dimensjoneres, og eventuelt sette inn nye tiltak for å bedre samvirke.

I hvilken grad oppnås samvirke i planlegging og gjennomføring av Cyber22?

Avgrensning

Finanssektoren er en stor og omfattende sektor som inkluderer en betydelig mengde aktører. Som følge av at oppgaven undersøker én enkelt øvelse vil det være en naturlig avgrensning i empirien som samles inn. Empirien vil basere seg på dybdeintervju av øvingsledelse og personer som gjennomfører øvelsen Cyber22 på operasjonelt og strategisk nivå i regi av Norges Bank (NB). Oppgaven er avgrenset til å studere tilsiktede handlinger. Dette har sin bakgrunn i scenarioet i beredskapsøvelsen Cyber22. Cyberdomenet og cybersikkerhet er svært omfattende og komplekst. Konseptene innebærer flere tekniske komponenter og systemer, og av den grunn er det viktig å poengtere at denne oppgaven ikke tar for seg det tekniske aspektet ved cybersikkerhet. Studien er avgrenset til å ta for seg håndteringen av cyberangrep på strategisk og operasjonelt nivå, og søker å forstå organisatoriske forhold og menneskelige faktorer. Studiet er også avgrenset ved å se på konseptet og prinsippet samvirke i konteksten av håndtering av cyberangrep i finanssektoren. Herunder hvordan samvirkeprinsippet operasjonaliseres i praksis.

1.3 Faglig relevans

Tradisjonelt har prinsippet for samvirke vært av stor betydning for krisehåndtering og beredskapsarbeid. Samvirkeprinsippet er et nasjonalt beredskapsprinsipp, som krever at relevante aktører får til et best mulig samvirke i arbeidet med forebygging, beredskap og krisehåndtering. Samvirke har også fått et større fokus når det gjelder identifisering og iverksetting av tiltak mot sammensatte trusler (NSM, 2021, s. 19). I denne oppgaven forstås sammensatte trusler som:

> ... statlige eller ikke-statlige aktørers trusler om, eller bruk av, en kombinasjon av ulike virkemidler for å utnytte sårbarheter, skape uro og oppnå bestemte politiske eller strategiske mål (Phillips, & Austad, 2021, s. 4).

Cyberangrep kan være av en slik karakter som kan omfattes i en kontekst av sammensatte trusler. Det er nyttig å undersøke nærmere hvilken betydning samvirke har for det forebyggende sikkerhetsarbeidet i møte med slike trusler. I sikkerhetsloven lovfestes ansvarsprinsippet ved at det med hjemmel i lov utarbeides forskrifter om ulike myndigheters og virksomheters ansvarsområder. Samtidig fastslår også loven at det er behov for samvirke mellom de ulike aktørene. Begrunnelsen for dette er behovet for å se forebyggende nasjonal sikkerhet i sammenheng, slik at den tverrsektoriell kompetanse kan nyttiggjøres. På den måte søker loven å balansere de to prinsippene (NOU 2018: 14, s. 34). Denne studien undersøker

betydningen av samvirkeprinsippet, og hvordan samvirke operasjonaliseres i forkant og i håndtering av en cyberhendelse.

1.4 Tidligere forskning

I dette avsnittet presenteres et utvalg av tidligere cybersikkerhetsforskning som er relevant for problemstillingen. I lys av tidligere hendelser relatert til cyberdomenets sårbarheter har det de siste årene oppstått et økt behov for samfunnsteoretisk forskning omkring temaet. I tidsskriftet *«The journal of cybersecurity»* vektlegges nødvendigheten av vitenskapelige bidrag fra en rekke disipliner for å forstå de varierte aspektene med cybersikkerhet (Oxford Academic, 2022). Forskningen som presenteres i denne oppgaven er hentet fra dette tidsskriftet i den hensikt å hente ut oppdatert forskning målrettet mot cybersikkerhet. Dette tidsskriftet er valgt fordi det er krav om at artiklene som publiseres skal treffe et bredt spekter av fagfelt, også innenfor samfunnsvitenskapelig emner. Artiklene undersøker ulike aspekter av cybersikkerhet, og bygger på komponenter som er i samsvar med hverandre. Temaer som samhandling og forståelse av cybersikkerhet er gjennomgående, som også underbygger betraktninger om motstandsdyktighet i cyberdomenet også kalt cyber-resiliens.

Atkins og Lawson (2021) har gjennom sin publikasjon *«Cooperation amidst competition: Cybersecurity partnership in the US financial services sector»* utført en dybdeanalyse av hvordan cybersikkerhetssamarbeidet har utviklet seg i en kritisk infrastruktursektor, inkludert en undersøkelse av barrierene for videre samarbeid. Artikkelen baserer seg på en rekke offentlige dokumenter som vitenskapelige artikler, nyhetsartikler og myndighetsdokumenter, samt flere titalls dybdeintervjuer av aktører involvert i samarbeidet om cybersikkerhet mellom næringsliv og myndigheter i finanssektoren i USA (Atkins & Lawson, 2021, s. 2). Ut ifra funnene fremtrer relasjonen mellom finansdepartementet og de viktigste finansinstitusjonene er sterke og gjensidige i sammenligning med andre sektorer.

For å få til et fungerende samarbeid kreves det at myndighetene tar ansvar for deres del av arbeidet er dimensjonert til oppgavene som skal gjøres. Tillit er en suksessfaktor for et godt samarbeid, og for å bygge tillit kreves det en god organisering som er spesielt viktig for operasjonelle relasjoner. Et annet viktig funn er den delte bevisstheten i finansnæringen når en står ovenfor nasjonalstatstrusler. Dette begrunnes med at statsdrevne cyberoperasjoner mot en enkelt virksomhet ofte er en del av en større kampanje. Det kreves at hver enkelt virksomhet samler og analyserer informasjon som indikerer en kampanje, for deretter å koordinere en

sektoromfattende respons. En slik nødvendighet understreker verdien ved å etablere varige sanntidsforbindelser på tvers av virksomheter og myndigheter på operasjonelt nivå i sektoren (Atkins & Lawson, 2021, s. 8).

Avslutningsvis konkluderes det med at interaksjonen mellom næringsliv og myndigheter i alle sektorer må kunne tilpasses i en dynamisk kontekst. Forskerne peker på cybertrusler og sårbarheters kontinuerlige utvikling i alle sektorer, men at endringshastigheten i trusler varierer fra sektor til sektor. Tradisjonelle reguleringsprosesser blir dermed utilstrekkelige og mindre effektive i noen sektorer. På den andre siden kan reguleringsmekanismer være nyttige i sektorer der utviklingen av nye infrastrukturteknologier skjer i et langsommere tempo. Til slutt understreker artikkelen den økende betydningen av tverrsektorielt samarbeid. Dette kan eksemplifiseres med selv når den finansielle sektoren har analysert sin interne cyberrisiko, har dens mottakelighet for potensielle feil i elektronisk kommunikasjon eller kraftforsyningen kunne økt i større grad. Dette viser at det stadig og tydeligere haster å håndtere tverrsektortrusler. Det kreves direkte kommunikasjon mellom foretak som er viktige for systemer fra ulike bransjer, men også en organisering fra myndighetens side som muliggjør dette samarbeidet (Atkins & Lawson, 2021, s. 9).

I artikkelen til Kavak et al., (2021) presenteres en oversikt over cybersikkerhet med fordypning i tre ulike temaer: (1) En oversikt over cybersikkerhetsdomenet, (2) Et sammendrag av modell-simuleringsforskning for cybersikkerhet og (3) Forslag videre til hvordan modell-simulering kan forsterke innsatsen for cybersikkerhet (Kavak et al., 2021, s. 1). Avslutningsvis diskuterer forfatterne ulike forslag for å utvikle tilnærminger for å etablere datainnsamling og tilgang til informasjonsmodeller. Forslagene innebærer å bruke kjente sosiale teorier for å konstruere nye sosiale teoretiske modeller spesifikt rettet mot cyberdomenet. Deriblant foreslås en kombinasjon av generell systemteori og kompleks ledelsesteori. Det konkluderes med at simulering bør få en større rolle, men det kreves mer forskning på dette området (Tisdal, 2015; Von, 1956; Uhl-Bien, 2007; Kavak et al., 2021, s. 9 & 10).

I Duponts (2019) artikkel *«The cyber-resilience of financial institutions: significance and applicability»* undersøker han betydningen av cyber-resiliens og hvordan cyber-resiliens kan fremmes i den finansielle sektoren i Canada. Han identifiserer fem organisatoriske dimensjoner for resiliens: *dynamisk*, *nettverksbasert*, *praktiserende*, *tilpasningsdyktige* og *omstridte* (se 4.5.1 for en beskrivelse). Dimensjonen *omstridt* fremstår gjerne ikke som helt selvforklarende, og i denne sammenheng dreier dette seg om dilemmaet mellom kost-nytte i en organisasjon.

Økning av motstandsdyktigheten i en organisasjon har en kostnad, som kan oppleves uforholdsmessig i forhold til risikoen. Den er omstridt fordi kost-nytte innen sikkerhetsarbeidet ofte er en grobunn for debatt. De fem dimensjonene kan også oversettes til tiltak og praktiske aktiviteter som kreves for å håndtere og forstå et bredt spekter av utfordringer i enhver organisasjon. Videre ble det undersøkt to tilnærminger som brukes på sektornivå for å øke cyber-resiliens i finansinstitusjoner. (1) En markedsføringstilnærming som er fremmet av konsulent- og sikkerhetsvirksomheter: Disse tilbyr ekspertise og en rekke verktøy som er bred, men, ifølge forfatteren, har manglende konsistens. (2) En standardisert tilnærming: En slik standard kan måles, testes og blir ofte beskrevet som «oppskriften på virkeligheten». I cybersikkerhersdomenet er det to fremtredende standarder som inkluderer tiltak som er kompatible med cyber-resilienstilnærmingen: «The International Organization for Standardization's 27000-series of information security standards» og «The National Institute of Standards and Technology's Cybersecurity Framework». Utfordringen med denne tilnærmingen er at cyberkrisers uforutsigbarhet og tendens til å overraske vil kunne forsvinne. Samtidig er det et behov for å utvikle generaliserte ressurser og kapasiteter som er tilpasningsdyktige og utholdende (Duponts, 2019, s. 1, 10, 11 & 14).

Weick & Sutcliffe (2015) har i sitt arbeid med "High reliablility organizations» (HROs) analysert hvordan tekniske og standardiserte organisasjoner, som flyselskap eller atomanlegg, oppnår resiliens. I denne teorien viser det seg at det ikke er lange lister over tekniske kontroller eller formelle prosedyrer som alene gjør dem flinke på å håndtere uventede og uønskede hendelser. Istedenfor handler det om kulturelle funksjoner som forfatterne definerer som «mindful organizing». Dette inkluderer prinsippene: Opptatt av å oppdage og rapportere feil, nekter å forenkle, fokus på drift og operasjonssensitivitet, forplikter seg til resiliens og respekt for ekspertise. Dette er delte normer og verdier som fremmer resiliens gjennom kontinuerlig kommunikasjon og korrigering i møte med ukjente risikoer (Weick & Sutcliffe, 2015; Duponts, 2019; Kristensen, 2016).

1.5 Oppgavens struktur

Denne oppgaven er bygget opp av syv kapitler: innledning, metode, kontekst, teori, empiri, drøfting og konklusjon. Helt til slutt kommer referanser og vedlagte dokumenter.

I kapittel 1 gis det en introduksjon som beskriver tema for studien. Deretter presenteres problemstillingen og forskningsspørsmål, samt faglig relevans og en gjennomgang av et utvalg av tidligere forskning.

Kapittel 2 beskriver forskningsmetoden som er anvendt i denne studien. Det vil gis begrunnelse for metode og valg som er tatt gjennom hele forskningsprosessen, samt kritiske betraktninger og refleksjon rundt valg av metode og gjennomføring av studien. Dette kapittelet kommer tidlig i oppgaven fordi det i teorien også presenteres en del data hentet fra dokumentstudiet.

I Kapittel 3 presenteres kontekst og bakgrunn for casestudien. I dette kapittelet blir den sentrale aktøren, Norges Bank (NB), presentert. Det gis også en forenklet systembeskrivelse av det finansielle systemet, en oppsummering av relevant rammeverk og hva cybersikkerhet i finanssektoren er omfattet av. Det gis også en beskrivelse av beredskapsøvelsen, Cyber22.

Kapittel 4 redegjør for det teoretiske grunnlaget som anvendes for å belyse tematikk og problemstilling. Teorien vil også anvendes i drøftelsen av problemstillingen og de tre forskningsspørsmålene.

I kapittel 5 presenteres resultatene og analysen av dokumentstudier, intervju og observasjonsdata. Resultatene presenteres under tilhørende tema som følge av analysen. Hvert tema kan sees i sammenheng med hvert av de tre forskningsspørsmålene.

Kapittel 6 omfatter drøfting av empiri og funn sammen med det teoretiske rammeverket.

Avslutningsvis vil det i kapittel 7 presenteres en konklusjon og avslutning som skal gi svar på problemstillingen. Det vil også gis forslag til videre forskning.

2. Forskningsmetode

I følgende kapittel redegjøres det for hvilke forskningsmetoder som ble anvendt for å belyse problemstillingen. Det vil også gis en vurdering for de valg som er tatt, samt gjennomgående diskutere styrker og svakheter med metoden. Ved å få innsikt i forskningens organisering gis det anledning for leseren selv til å gi en vurdering av studien.

2.1 Forskningsdesign og fremgangsmåte

Forskningsdesignet representerer den logiske planen og legger rammen for hvordan forskningen er utført. Planen innebærer valg og beskrivelse av strategi, systematikk og struktur. Forskningsdesignet legger grunnlaget for prosessen og binder sammen problemstilling, empiriske data og forskningskonklusjonen. Forskningsdesignet er selve rammeverket for hvordan akkurat denne studien gjennomføres (Blaikie & Priest, s. 33; Johannessen et al., 2016, s. 280). I Tabell 1 gis det en detaljert oversikt over den praktiske fremgangsmåten for prosjektet.

Tabell 1: Fremgangsmåten for prosjektet

Tidsperiode	Hva som ble gjort	Hensikt	Nytte
Januar	Planskisse. Problemstilling, struktur og moderere metodevalg. Dokumentsøk Dokumentinnsamling og dokumentstudier i forbindelse med kapittel 3: Kontekst og kapittel 4: Teori. Møte med informanter. Kartlegging av informanter.	En plan for det videre arbeid. Fastsette problemstillingen og få oversikt over litteratur og forskning innenfor tema cyber, finansnæringen og samvirke. Etablere kontakt og definere et samarbeid med informanter.	En konkret plan som lempelig gjør det videre arbeidet. Etablere et godt samarbeid for *casen* i studien. På bakgrunn av usikkerhet om funn kunne utgjøre potensielle sårbarheter, ble en konkretisering om av hva som skulle undersøkes, som førte til noen endringer i utvalget.
Februar	Intervjuguide Teori og metode. Intervju av nøkkelinformanter.	Utarbeide og moderere intervjuguide for intervju av nøkkelinformanter.	Revisjon av intervjuguiden førte til mer bredde i datagrunnlaget.
Mars	Intervju av nøkkelinformant. Teori og metode. Dokumentinnsamling og dokumentstudier i forbindelse med kapittel 5 empiri. Databehandling og datareduksjon av de kvalitative intervjuene av nøkkelinformantene.	Beskrivelse av teori som anses som relevant og gi en beskrivelse av metoden til leseren.	

April	Intervju av nøkkelinformant. Databehandling og datareduksjon av de kvalitative intervjuene av nøkkelinformantene. Dokumentinnsamling og dokumentstudier i forbindelse med kapittel 5 empiri. Påbegynne analyse og drøftelse.	Samle inn data knyttet til planlegging av Cyber22. Kartlegging av hvilken informasjon i datagrunnlaget som er relevant for studien. Arbeide videre med dokumentstudier.	
Mai	Observasjon av øvelse Cyber22. Avsluttende intervju av nøkkelinformanter og deltakere i øvelsen. Databehandling og datareduksjon av avsluttende intervjuene samt observasjonsdataen. Analyse og drøfting	Samle inn data: Gjennomføringen av øvelsen. Kartlegge hvilken informasjon i datagrunnlaget som er relevant.	
Juni	Ferdigstilling av oppgaven.	Gjøre dokument klar for innlevering.	

2.2 Forskningsstrategi

Det anvendes en abduktiv strategi i forskningsdesignet. Abduktiv tilnærming kan beskrives som en mellomting av induktiv og deduktiv tilnærming. Der Induktiv svarer på «hva» spørsmål og deduktiv svarer på «hvorfor» spørsmål – søker jeg ved en abduktiv strategi å svare på begge spørsmålene. På denne måten inkorporerer den abduktive tilnærmingen mening, tolkning, intensjon og motiver hos sosiale aktører (Blaikie & Priest, s. 99). Abduktiv strategi er valgt på bakgrunn av forskningsspørsmålene, samtidig som jeg ønsket en fleksibilitet i forskningstilnærmingen.). Ved en slik strategi har jeg kunnet bevege meg frem og tilbake mellom empiri og teori – der jeg gjennom en stegvis-deduktiv-induktive (SDI) prosess svarer på problemstillingen (Tjora, 2021, s. 20). Tidlig i prosessen dannet jeg meg et teoretisk grunnlag som jeg anså som relevant. Under innsamlingen av data har jeg vurdert mitt teoretiske grunnlag opp mot mine empiriske funn. Videre supplerer jeg med ny teori der jeg mente dette bidro på en bedre måte til å forklare og forstå funnene. Denne metodiske tilnærmingen begrunnes i at problemstilling og forskningsspørsmål søker å forstå meninger og motiver som leder til sosiale aktiviteter. Thagaard (2018) beskriver ved analysen av data utvikler forskeren en forståelse av den innsamlede dataen (Thagaard, 2018, s. 184). Gjennom intervju av informantene utvikler jeg en forståelse av hvordan sosiale aktører konseptualiserer de sosiale fenomenene omkring samvirke i håndtering av cyberhendelser. Dette kombineres med teori som gir meg økt forståelse, og som underbygger og utfordrer datamaterialet.

2.2.1 Ontologiske og epistemologiske antakelser

Som samfunnsforsker er det viktig å være bevisst på egne antakelser om den sosiale virkeligheten (ontologi), og hvordan jeg får kunnskap om den sosiale virkeligheten som studeres (epistemologi) (Blaikie & Priest, s. 101-102). Informantene vil også ha sin egen forståelse av virkeligheten om ulike konsepter. Forståelsen av samvirke-konseptet er et slikt eksempel. Her vil både analysen av dokumenter og litteratur være preget av mine ontologiske og epistemologiske antakelser, samtidig som dybdeintervjuene av informantene vil være basert på deres ontologiske antakelser. Gjennom en systematisk forskningsprosess har jeg tilstrebet å etablere kunnskap som kan gi en forståelse og beskrivelse av samvirke-konseptet. Gjennom en hermeneutisk tilnærming har jeg ved å undersøke og reflektere utviklet konseptet. Målet med dette har vært å generere et konsept som svarer på problemstillingen for å etablere teori som kan være nyttig. Andre studier og metoder kan føre til nyetablerte oppfatninger av konseptet. Det er derfor enda viktigere å tydeliggjøre og å begrunne mine antakelser når jeg skal drøfte forskningsspørsmål og problemstilling (Grønmo, s. 30; Blaikie & Priest, s. 129). Min *ontologi* vil også påvirke min *epistemologi,* altså hvilke vitenskapelige metoder som brukes i lys av min forståelse av den virkelige verden. Ettersom jeg har et konstruktivistisk perspektiv ønsket jeg gjennom intervjuene å forstå informantenes sosiale verden. Dermed ble kunnskapen som er etablert i oppgaven et resultat av en balanse mellom det hverdagslige samfunnsspråket og det tekniske samfunnsvitenskapelige språket (Blaikie & Priest, s. 104).

2.2.2 Casestudie og problemstilling

Casestudier kjennetegnes ved at undersøkelsen rettes mot å studere mye informasjon om få enheter eller *caser* (Thagaard, 2018, s. 51). I denne studien anvendes en holistisk tilnærming til studien, og ved å studere en «enhet» kan den betegnes som en *enkelcasestudie* (Johannessen et al., 2021, s. 209). Min «enhet» i oppgaven er øvelsen Cyber22, men mer spesifikt planleggingsgruppen for øvelsen Cyber22. Casestudie som grunnlag i forskningsmetoden har stadig blitt utfordret av forskermiljøet. Flyvbjerg (2006) påpekte fem misoppfatninger om case-studier som indikerte at teori, pålitelighet og gyldighet er usikkert (2006, s. 221). Han konkluderte likevel med at denne misoppfatningen om case-studier er misledende, og at case-studier er en tilstrekkelig metode for visse forskningsoppgaver innen samfunnsvitenskapen (2006, s. 241). Denne forskningsoppgaven tar for seg operasjonalisering av samvirke tilknyttet en konkret øvelse. Ved å studere en bestemt øvelse er casestudie en tilstrekkelig metode for å kunne svare på problemstillingen.

Denne *casen* er å anse som *paradigmatisk* ved at den søker å etablere et tankesett for det domenet som casen tar for seg (2006, s. 230). Casestudie som design samsvarer med problemstillingen, ved at den er avgrenset til en bestemt kontekst for å forstå et spesifikt fenomen. Analyseenheten som studeres er en bestemt øvelse og dette presiseres i problemstillingen: *«På hvilken måte operasjonaliseres samvirke i planprosess og gjennomføring av beredskapsøvelsen Cyber22? ... ».* Selv om problemstillingen innebærer kun ett enkelt tilfelle vil den kunne ha betydning for generell interesse, som følge av at det er et behov for en bredere forståelse omkring operasjonalisering av samvirke i krisehåndtering og beredskapsarbeidet. Jeg vil påpeke at formålet er analytisk, der jeg ønsker å gå i dybden på temaet, og at det da nødvendigvis ikke er generalisering som er hovedpoenget.

2.3 Datagenerering

2.3.1 Kvalitativ metode

I denne oppgaven ønskes det kunnskap omkring mening og prosesser som ikke lar seg tallfeste og måle kvantitativt. Ved en kvalitativ undersøkelse går jeg i dybden på tematikken for å forstå fenomenet gjennom en helhetlig fortolkning. Det er dermed benyttet kvalitativ metode for å kunne gi mye kunnskap om planleggingen og gjennomføringen av beredskapsøvelsen Cyber22, samtidig som det besvarer problemstillingen (Dalland, 2017, s. 52). De kvalitative innsamlingsmetodene som er valgt er i form av dybdeintervju, dokumentstudier og observasjonsdata. Hensikten ved å bruke ulike metoder er å generere data som utfyller hverandre. Der et dybdeintervju frembringer dyp og meningsbærende informasjon, vil et offentlig dokument gjerne mangle nyanser og dybde. Kombinasjonen av ulike datagenereringsmetoder gir dermed bredere innhold og dybde i datagrunnlaget som er med på å styrke validiteten i studien (Denzin, 2012, s. 82).

2.3.2 Kvalitative intervju

Det er gjennomført semi-strukturert dybdeintervju av informanter som er å anse som helt sentrale for å kunne besvare problemstillingen. Valget om å benytte et semi-strukturert dybdeintervju baseres på et ønske om en viss struktur under intervjuet, samtidig som det ga meg fleksibilitet i datainnhentingen og en fremhevelse av den naturlige samtalen. Dette gjorde det mulig å følge opp spørsmål som jeg ønsket å gå enda mer i dybden på. En svakhet med det semi-strukturerte intervjuet var at ikke alle informantene fikk muligheten til å svare på de eksakt samme oppfølgingsspørsmålene. På en annen side var spørsmålene så åpne at det var opp til

hver enkelt informant å vektlegge hva som var betydningsfullt innenfor hvert tema. Dette bidro til å fange opp en stor variasjon og ulike perspektiver i meningsinnholdet – som igjen ga bredde i datagrunnlaget.

Utvalg

Utvalget i denne studien er av strategisk karakter. Strategisk utvalg betyr at jeg har valgt informanter som har kvalifikasjoner som er strategiske i forhold til problemstillingen. Dette begrunnes med at jeg studerer en bestemt *case* innenfor en bestemt aktivitet i en avgrenset tidsperiode, som sammenfaller med utvalget (Tjora, 2021, s. 48). Utvalget er basert på en *snøballutvelging*, som er en form for utvelging som skjer av aktøren selv (Grønmo, 2016, s. 117). Under denne studien startet det med en kontaktperson i NB, som foreslo andre aktører gjennom *nettverkforbindelser*. Nettverksforbindelse baseres på nettverksrelasjoner i organisasjonen. Denne metoden har vært særlig nyttig da jeg som forsker har begrenset oversikt og innsikt, og det har dermed vært verdifullt å nyttiggjøre seg av aktørens egne vurderinger av hvem som kunne bidra med relevant informasjon (Grønmo, 2017, s. 117).

Det strategiske utvalget består av totalt ni informanter som befinner seg på strategisk og operasjonelt nivå i organisasjonen NB, der fire av dem er nøkkelinformanter tilhørende øvingsledelsen. Disse betegnes som *nøkkelinformanter* fordi de har en helt sentral posisjon innenfor planleggingen og gjennomføring av øvelsen Cyber22. Dette er mennesker som jobber med sikkerhet og beredskap i det daglige, og som er å anse som eksperter på dette fagfeltet. De fem andre informantene er deltakere på øvelsen og betegnes som *deltakerinformanter,* som representerer ledere og beredskapspersonalet som håndterer sikkerhetshendelsen i Cyber22. I kapittel 5 ble det ikke gjort et skille på informantene ved bruk av betegnelser som informant A, informant B også videre. Dette er et bevisst valg for å tilstrekkelig anonymisere informantene.

Utforming av intervjuguide

Intervjuguiden setter en ramme for intervjuet og fungerer som et hjelpemiddel for å lede en gjennom intervjuet. Dalland (2017) viser til et kjennetegn ved det kvalitative intervjuet er å skape kunnskap gjennom samtale, dermed forutsetter det seg ikke å låse seg til punktvise spørsmål. I utformingen av intervjuguiden tilstrebet jeg å formulere åpne spørsmål som fremhever en samtale og bidrar til å kunne følge opp med nye spørsmål underveis. Videre måtte jeg vurdere informasjonsbehovet, og denne vurderingen er foretatt med utgangspunkt i studiens

problemstilling. På grunnlag av informasjonsbehovet har jeg spesifisert ulike temaer (Grønmo, 2017, s. 168-169). Intervjuguiden ble dermed strukturert inn i ulike temaer med tilhørende åpne spørsmål under hvert tema (se vedlegg 1).

Etter første intervju opplevde jeg at det var behov for å revidere intervjuguiden ved å supplere med nye spørsmål. Dette fordi spørsmålene jeg hadde stilt ikke var spesifikke nok for å danne et bredt kunnskapsgrunnlag. Intervjuet ble dermed et grunnlag for en datatest etter SDI metoden nevnt i 4.2 forskningsstrategi. En datatest består av spørsmål om hvorvidt de empiriske data som genereres, er relevante for spørsmålene som stilles. Eksempelvis om spørsmålene er detaljerte nok og ikke for detaljerte (Tjora, 2021, s. 286).

Gjennomføring av intervjuer

Det ble tilstrebet en uformell tilnærming for å fremme en god kommunikasjonssituasjon (Grønmo, 2016, s. 170). Jeg ønsket at informantene skulle oppleve at jeg både var fleksibel og engasjert i deres kunnskap. Det ble tidlig i prosjektet sendt ut informasjon om oppgaven. Ved avtale om intervju ble det uttrykket fleksibilitet med tanke på tid for intervju. Videre ble intervjuene foreslått å gjennomføres via Microsoft Teams. Det er både fordeler og ulemper ved å gjennomføre intervjuene digitalt. En klar ulempe ved å ikke møte informantene personlig, var at det kunne føre til at den samme kontakten ikke ble oppnådd slik den ville ved et personlig møte. Fordelene var likevel flere, da det førte med seg fleksibilitet for både informantene og forskeren i gjennomføringen av intervjuene. Informantene oppholder seg på et annet geografisk område, samtidig som det var en pågående pandemi. Dette var to avgjørende faktorer for beslutningen. Alle intervjuene ble tatt opp digitalt på en kryptert enhet. Dette muliggjorde bruk av aktiv lytting i kommunikasjonen samt at jeg kunne fokusere på oppfølgingsspørsmål underveis i samtalen. Det var også fordelaktig med tanke på å få mest mulig detaljert informasjon som senere ble transkribert til tekstdokumenter. Totalt ble det gjennomført 12 intervju. I forkant av øvelsen ble det gjennomført fire intervju med plangruppen som dannet det empiriske grunnlaget for oppgaven. De siste åtte intervjuene med øvingsledelsen og deltakere, ble gjennomført etter øvelsen, og fungerte som en oppsummering og kvalitetssikring av observasjonsdata fra øvelsen.

2.3.3 Dokumentstudier

I denne studien er det generert og analysert bakgrunnsdata fra allerede eksisterende dokumenter som gir informasjon om ulike forhold og formål som et nedtegnet på bestemte tider og steder. Det er i hovedsak tatt utgangspunkt i *generelle* offentlige dokumenter både litteratur,

forskningsdokumenter, rapporter og politiske dokumenter. Det har vært hensiktsmessig for å kunne forstå konseptene samvirke og cybersikkerhet i finanssektoren. Strukturering og innsamling av denne type data ble påbegynt innledningsvis i utforming av studien. Denne type datagenerering har vært essensiell for å kunne få en forforståelse av temaet, og bidratt til konseptualisering av viktige konsepter. I den sammenheng ble det foretatt dokumentsøk der formålet var å gå ut bredt, for å så å innskrenke søket.

Dokumentsøk

Søk tilknyttet forskningsdokumenter som beskrives i delkapittel 1.4 «Tidligere forskning», 3.4 «Cybersikkerhet i finanssektoren», 4.4 «Samvirke» og 4.5 «Resiliens» presiseres å være basert på kun et utvalg av tidligere forskning. Søk er foretatt i databasene Google Scholar og Oria på følgende ord: «Samvirke», «cybersecurity», «financial sector», «collaboration», «communication», «coordination». Dette ledet meg videre til flere artikler. Artiklene som er valgt er publisert i fagfellevurderte tidsskrifter, og utvalget baseres på en vurdering av artiklenes relevans i henhold til denne oppgaven. Andre forskere ville kanskje valgt andre artikler utfra deres vitenskapelige ståsted, noe som kan tilsi en svekket validitet. Likevel styrkes også oppgavens validitet ved at jeg gjennom en systematisk fremgangsmåte bruker en standard for å søke bredt for så å innskrenke søket. Angående offentlige dokumenter og rapporter ble det foretatt søk i søkemotoren google.no og en gjennomgang av politiske dokumenter publisert via regjerningen.no. Dokumentsøk er en datagenereringsmetode som ble brukt gjennomgående under hele studien, da det har vært hensiktsmessig som bidrag i fremstilling av teori og analysen av empirisk data. Tabell 2 viser et utvalg av de mest sentrale politiske og offentlige dokumentene som er brukt i fremstilling av empirien.

Tabell 2: Et utvalg av de mest sentrale offentlige dokumentene

Innholdstype	Tittel	Opphav	Publisert
Norske offentlige utredninger (NOU)	**2019:13** *Når krisen inntreffer*	JD	2019
	2018:14 *IKT-sikkerhet i alle ledd*	JD	2018
	2016:19 *Samhandling for sikkerhet*	FD	2016
	2015:13 *Digital Sårbarhet – sikkert samfunn*	JD	2015
	2012:14 *Rapport fra 22.juli kommisjonen.*	SMK	2012
Stortingsmeldinger (Meld. St. **NR**)	**5** *Samfunnssikkerhet i en usikker verden*	JD	2020-2021
	10 *Risiko i et trygt samfunn.*	JD	2016-2017
	29 *Samfunnssikkerhet*	JD	2011-2012

	31 *Finansmarkedsmeldingen.*	FIN	2020-2021
	38 *IKT-sikkerhet - Et felles ansvar*	JD	2016-2017
Proposisjoner	**135 L** *Lov om nasjonal sikkerhet (sikkerhetsloven*	FD	2016-2017
Rapporter, trusselvurderinger og planverk	*Risiko 2022 Økt risiko krever økt årvåkenhet.*	NSM	2022
	Risiko 2021. Helhetlig sikring mot sammensatte trusler.	NSM	2021
	Nasjonal strategi for digital sikkerhet.	Departementene	2019
	Report on Cyber Crisis Cooperation and Management.	ENISA	2014
	15 stk. rapporter fra finansmyndigheter i Norge.	FIN, NB, Finanstilsynet	2009-2022
Totalt antall dokumenter	**30** offentlig publiserte dokumenter		2009-2022

2.3.4 Deltakende observasjon

I denne studien består den deltakende observasjonen av å observere beredskapsøvelsen Cyber22. Det er valgt å bruke en åpen observasjonsform, både for å ivareta det forskningsetiske og av rent praktiske grunner. Min rolle var ikke deltakende i den grad at jeg deltok i selve øvelsen, men ved at jeg var en *interaktiv* observatør (Tjora, 2021, s. 71). Dette fordi jeg ikke ønsket å unødig forstyrre deltakerne under øvelsen. Dermed tok jeg en mer aktiv rolle i situasjoner jeg naturlig deltok i samtale med deltakere. Ved forberedelse til observasjonen har det vært hensiktsmessig å kartlegge hva jeg ønsket kunnskap om. Intervju med nøkkelinformanter og dokumentstudier dannet et utgangspunkt for tematikken som skulle studeres under observasjon. På forhånd ble det utformet et skjema der jeg kunne fylle inn interessante observasjoner innenfor forhåndsbestemte temaer på bakgrunn av analysen. Det var hensiktsmessig å note ned begreper og hendelser som ble oppfattet som uforståelige under øvelsen. Etter øvelsen ble disse undersøkt ved hjelp av oppslagsverk og som spørsmål under intervju. Konfidensialitet og ivaretakelse av personvern var en prioritert når jeg noterte ned observasjoner. Det vil si at jeg ikke noterte ned personalia som kan knyttes til bestemte personer. Jeg noterte heller ikke ned informasjon som jeg oppfattet å være konfidensiell.

2.4 Metode for analyse

2.4.1 Bearbeiding av data

Gjennom en strukturert metode har jeg forsøkt å unngå at analysen av empirien ikke ble påvirket av mine forutinntatte tanker. Ved å utvikle en tiltro til empirien og ved opprettholdelse av god

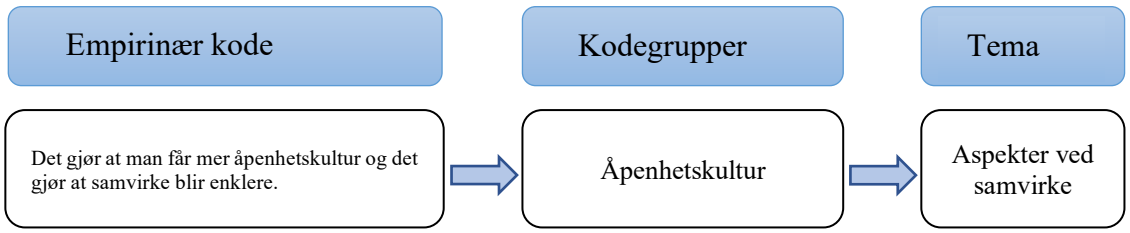
systematikk gjennomgående har jeg forsøkt å unngå premature konklusjoner. Alle intervjuene ble transkribert fra lydopptaket slik at jeg satt igjen med det som kalles *analysedata.* Transkribering er tidkrevende og detaljorientert arbeid, der det ble brukt opptil 8 timer per intervju. Transkribering ble foretatt direkte etter gjennomføring av intervju. Ved å ha intervjuet ferskt i minne kunne misforståelser forhindres for å sikre kvaliteten ved overføring fra lyd til tekst. Muntlig språk kan noen ganger fremstå uforståelig når lyd transkriberes om til skriftlig tekst. Tegnsetting var et viktig virkemiddel for å sikre et entydig språk under transkriberingen. Informanter som ønsket å kvalitetssikre intervjuet fikk tilsendt intervjudokument for gjennomlesning. Dette var svært nyttig da det i noen av intervjuene var vanskelig å tolke interne terminologier og som gjorde det mulig å rette opp i mulige misforståelser. Intervjuene som ble foretatt etter gjennomføring av øvelsen fungerte som en kvalitetssikring av observasjonsdata. De avsluttende intervjuene var i betydelig grad kortere og dermed mindre tidkrevende å transkribere. Disse intervjuene ble gjennomført kort tid før innlevering av oppgaven, og dermed ble det ikke tid til å sende dem for gjennomlesing.

2.4.2 Koding

Kodingsarbeidet ble foretatt i det kvalitative dataverktøyet NVIVO, dette fungerte godt for å forenkle prosessen ved å ekstrahere essensen i intervjuene og redusere materialets volum. Samtidig som det gjorde det lettere å systematisere empirien. Jeg holdt fast med SDI-metoden ved å fremme en ren induktiv strategi i kodingen, som også kalles en induktiv *empirinær koding*.

> En slik strategi for koding gjør det mulig å redusere påvirkningen av forventinger og teorier som enhver forsker mer eller mindre eksplisitt vil trekke inn i analysen (Tjora, 2021, s. 218).

I grounded theory kalles dette *åpen koding,* som finner sted når den abduktive metoden blir brukt (Blaikie and Priest, 2019, s. 204). I kodingen har jeg hentet ut deltakerutsagn fra intervjuene for å kunne ivareta det helt spesifikke i materialet. Jeg har vekslet mellom å kode hele avsnitt, hele og halve setninger – avhengig av informasjonen i de ulike utsagnene. For hvert intervju endte jeg opp med ca. 100 empirinære koder. Det at antall koder ble svært høyt opplevde jeg som noe utfordrende. På en annen side så kan et stort antall koder tyde på en detaljert koding der det empiriske innholdet blir godt bevart (Tjora, 2021, s. 220). I tillegg bidro dette positivt i neste trinn av kodingen. De empirinære kodene ble videre gruppert tematisk i kodegrupper som igjen ble delt inn i overordnete tema. Kodene som ble oppfattet som irrelevante ble plassert i en restgruppe. Prosessen for koding er illustrert i figur 1.



Figur 1: Illustrasjon av kodingsprosess

Ved at problemstillingen stiller spørsmålet om hvordan informantene har operasjonalisert samvirke var det nødvendig å gjøre et dypdykk i samvirke-konseptet. Følgelig ble forskningsspørsmålet «Hva er samvirke?» en del av studien. Som et produkt av kodingen, ble tema tilknyttet hvert forskningsspørsmål. Der temaet «Aspekter ved samvirke» (se avsnitt 5.1.2) er med på å svare på forskningsspørsmålet, som igjen bidrar til å besvare den øvrige problemstillingen. Dette var en gjennomgående prosess som koblet tema og forskningsspørsmål sammen.

2.4.3 Systemteoretisk analyse

I deler av analysen av empiri har jeg tatt utgangspunkt i elementene til Nancy Levesons systemtenkning, som presenteres i delkapittel 4.3 i teorikapittelet. Systemmodellen viser hvordan nivåene under og over interagerer sammen i et felles system. Dette vil gi en forståelse av hvor aktører befinner seg i systemet. I analysen vil jeg trekke frem funn som illustrerer hvordan sikkerhetsbegrensninger pålegges aktører på ulike nivåer. Dette kan gi et tydeligere bilde på hvordan kontrollfunksjonen fungerer i deler av finanssektoren. Informasjonsprosessen som omhandler hvordan kommunikasjon nedover og oppover i systemet gir grunnlag for å vurdere effekt og justeringer i sikkerhetsbegrensningene. Det er samvirke som er interessant i denne studien, og systemteori bygger nettopp på interaksjon mellom komponentene i systemet. Dermed vil analysemetoden fremme de funn som kan knyttes til teorien i oppgaven. I analysen legges det vekt på hva som oppfattes som avvik i forhold til systemtenkningen og hva som oppleves som god praksis. Dette støtter opp under et ønske om å øke *motstandsdyktighet* i et system, også kjent som *resiliens,* som også presenteres i delkapittel 4.5 i teorikapittelet.

2.5 Studiens kvalitet

Til nå har jeg redegjort for mine fremgangsmåter relatert til metode, utvalg og analyse. I dette delkapittelet vil jeg forsøke å belyse studiens kvalitet fra et helhetlig perspektiv. Ved kvalitativ forskning vurderes studiens kvalitet og troverdighet basert på begrepene relabilitet, validitet og overførbarhet (Thagaard, 2018, s. 19). Relabilitet kan beskrives som forskningens pålitelighet. Ved vurdering av reliabilitet redegjør jeg for hvordan data produseres. Dette innebærer blant annet at jeg forklarer hvordan jeg har etablert kontakt med informantene. I tillegg vil mine egenskaper og posisjon ha betydning for utvikling av data (Thagaard, 2018 s. 181 og 189). Forskningens validitet handler om gyldigheten til resultatene og hvordan vi tolker disse. Jeg må dermed være kritisk til hva jeg baserer mine tolkninger på. Thaagard (2018) beskriver at forskerens tilknytning til det miljøet som studeres påvirkes av hvordan forskeren tolker sine resultater. Jeg hadde ingen kjennskap til miljøet eller informantene i forkant av studien, og kom dermed inn som en utenforstående. Hvordan jeg posisjonerer meg i miljøet vil også påvirke mine resultater. Videre må jeg også vurdere om den forståelsen jeg utvikler innenfor denne studien også kan være relevant i andre situasjoner. Dermed hvordan tolkningen av resultatet kan gi grunnlag for en overførbarhet. Overførbarhet blir et formål ved kvalitative studier, der tolkningene fra dette studiet kan få en betydning av mer generell relevans (Thagaard, 2018, s. 194-195).

2.5.1 Relabilitet (pålitelighet)

For å styrke studiens pålitelighet har det blitt lagt vekt på å gi en konkret og detaljert beskrivelse av fremgangsmåten for utvikling av data. Ved å gjøre dette fremheves en transparent forskningsprosess som gjør at leseren kan gjøre en egenvurdering av valgt forskningsstrategi og analysemetode (Thagaard, 2018, s. 188). Videre har det vært viktig å synliggjøre det som er primærdata og det som er egne fortolkninger. Dette gjøres ved å redegjøre for et tydelig skille mellom hva om er intervjudata, informasjon fra dokumenter, noterte observasjoner og hva som er mine egne fortolkninger. Til tross for det vil jeg understreke at primærdataen vil være preget av min egen forståelse av det jeg hører og ser. I tillegg vil dokumentstudiet og hvilket faglig premiss som er lagt til grunn for analysen være preget av min egen subjektive vurdering av hvilke rammeverk oppgaven bør ha. Andre ville kanskje tatt utgangspunkt i andre kilder, og dermed er jeg kritisk til min egen pålitelighet i valg av kilder. På en annen side er metoden og analysen bygget på en faglig forankring, der jeg har fulgt forskningsetiske- og juridiske prinsipper. Primærdata hentet fra dybdeintervju er også kvalitetssikret av informantene som er med på å styrke påliteligheten til data. Det er også tatt utgangspunkt i et stort antall offentlige

dokumenter som er med på å styrke påliteligheten til datagrunnlaget ytterligere. Valg og relasjon til informantene har også innvirkning på studiens pålitelighet (Tjora, 2021, s. 264). Utvalget av informanter er redegjort for under 2.3.2. Jeg hadde ikke noe tilknytning eller personlig kjennskap til informantene. Av den grunn at oppgaven er et samarbeid mellom informant og forsker har det vært viktig å opprettholde et profesjonelt og transparent samarbeid. Det vil si at jeg har formidlet hva jeg trenger fra informantene og har hatt en jevn dialog gjennom hele forskningsprosessen.

2.5.2 Validitet (gyldighet)

Ved vurdering av forskningens gyldighet har jeg lagt vekt på å drøfte tre validitetstyper innenfor kvalitativ forskning: kompetanse, kommunikative og innholdsvaliditet. Kompetansevaliditet er et uttrykk for forskerens egne erfaringer og kunnskap for datagenerering (Grønmo, 2017, s. 254). For å styrke gyldigheten til data har det vært nødvendig å være fleksibel ved utforming og forbedring av intervjuguide. På den måten har jeg under datagenereringsprosessen vurdert validiteten til dataen for så å forbedre den. Det teoretiske rammeverket og de empiriske funn har bidratt til å styrke gyldigheten til dataene. Ved tidlig datagenerering fikk jeg kontakt med kildene som fremmet muligheten for en informasjonsinnhenting som var mest mulig relevant opp mot problemstillingen. Den kommunikative validiteten innebærer at jeg som forsker har diskutert gyldigheten av hvor godt og treffende materialet er i forbindelse med problemstilling.

En kontinuerlig diskurs om teori og empiri med veileder under forskningsprosessen har bidratt til å avdekke mulige svakheter i datamaterialet. Videre har også informantene kvalitetssikret intervjudata. På denne måten får informanten mulighet til å se om vedkommende kjenner seg igjen i sin fremstilling. I denne studien fikk også aktøren som undersøkes mulighet til å lese gjennom oppgaven, som igjen er med på å styrke gyldigheten til dataene som fremlegges. Det har ei heller ikke vært noen utfordringer knyttet til at kilden selv forsøker å ta over forskerens beskrivelse av forhold. Den tredje validitetstypen som er relevant for denne studien er innholdsvaliditet, da denne studien tar sikte på å undersøke og utvikle komplekse begreper (Grønmo, 2017, s. 257). For å styrke gyldigheten har det blitt gjort en omfattende gjennomgang av litteratur og dokumenter som beskriver begrepet *samvirke,* og en kontinuerlig vurdering om begrepet blir tilfredsstillende belyst i datamaterialet.

2.5.3 Overførbarhet

For denne studien er det særlig relevant å være bevisst på forskningens relevans og dens overførbare betydning. Det fordi det er en *enkeltcasestudie* med et utvalg primært tilhørende en organisasjon, og at det derfor er sentralt å drøfte dens betydning på generell basis. Jeg som forsker må kunne argumentere for at den forståelsen jeg kommer frem til, også kan være relevant i andre sammenhenger (Thagaard, 2018, s. 194). I denne sammenheng brukes generalisering på samme måte som overførbarhet. I denne studien er målet om generalisering todelt, ved å både fremme moderat generalisering og konseptuell generalisering. Moderat generalisering handler om at forskeren kan beskrive hvilke forhold (tid, sted og kontekst) resultatene vil være gyldig (Tjora, 2021, s. 268). I denne studien vil resultatene være gyldig under flere forhold fordi studien er av en slik karakter at nytten av den ikke er kontekstuelt betinget. Kunnskap omkring samvirke i cyberdomenet og generell krisehåndtering er fagfelt som vil kunne brukes på flere områder i samfunnet uavhengig av sektor eller område. Eksempel er funnet av den visuelle samvirkeanalysen. Den vil kunne anvendes på andre områder enn i håndtering av cyberhendelser i finanssektoren. Målet med studien har ikke vært å evaluere NBs evne til å håndtere, men å se på hvordan samvirke kan brukes som strategi i beredskapsarbeidet. Konseptuell generalisering handler om hvordan kvalitativ forskning utvikler konsepter eller teorier som vil ha relevans for andre caser enn det som blir studert (Tjora, 2021, s. 268). Operasjonaliseringen av samvirke har vært essensen i denne studien, og en videreutvikling av konseptet samvirke vil være anvendbart i andre studier.

2.6 Forskningsetiske refleksjoner

Under forskningsprosessen har det blitt foretatt refleksjoner og betraktninger omkring det forskningsetiske i studien. For å holde en høy forskningsetisk standard ble de grunnleggende kravene for forskningsetikk ivaretatt - ivaretakelse av personvernet, taushetsplikt, korrekt gjengivelse og informert samtykke (Jacobsen, 2015; Dalland, 2017). I denne prosessen ble prosjektet i en tidlig fase meldt inn til NSD (Norsk senter for forskningsdata) som følge av kravet til utlevering av personopplysninger, informert samtykke og retten til å trekke seg fra forskningsprosjektet (Tjora, 2021, s. 54). Det var også viktig å tydeliggjøre dette for informantene ved å gi utfyllende informasjon om hva deltakelsen i prosjektet innebar. Det vil være ulike etiske utfordringer med ulike datagenereringsmetoder. For eksempel under observasjon har det vært viktig å anonymisere deltakeres utsagn. Refleksjoner om hva slags etisk sans bør ligge implisitt i all forskning, uavhengig av de formelle juridiske kravene til forskningen. Generelt for alle studier vil tillit, konfidensialitet, respekt og gjensidighet prege

kontakten med deltakerne. I denne studien har jeg som forsker vært preget av at jeg skriver tekster «om dem», og det vil dermed ligge en naturlig forventing om å gi noe tilbake til «dem jeg forsker på» (Tjora, 2021, s. 53).

Høye krav stilles til samfunnsforskning, da jeg som forsker bryter inn på folks arenaer og fordi resultatene offentliggjøres. For denne studien var konfidensialitet ytterst relevant ettersom temaet som skrives om kan avdekke sårbarheter som kan ha konsekvenser for finanssektorens sikkerhet. Dette var en problemstilling som i den innledende fasen til prosjektet ble drøftet åpent med kontaktperson. Vi ble enige om at oppgaven måtte ha en overordnet tilnærming for å redusere mulighetene for å fremstille konfidensielle sårbarheter. Vi ble også enige om at kontaktperson også skulle lese gjennom oppgaven før innlevering for å forebygge at konfidensiell informasjon publiseres. Av den grunn at fortolkning er en integrert del av denne forskningsprosessen har det vært viktig å reflektere over og å redegjøre for hvordan mine egne holdninger kan påvirke valg av tema og datakilder. Felles forskningsetiske forpliktelser som redelighet i dokumentasjon, konsistens i argumentasjon, upartiskhet og åpenhet rundt usikkerhet er alle momenter som er tatt i betraktning gjennom hele prosessen (Tjora, 2021, s. 55).

3. Kontekst

3.1 Presentasjon av aktør

Finanssektoren består av både av private og offentlige aktører, og omfattes av alle finansielle tjenester som banker, finansieringsforetak, forsikringsselskap samt utøvende myndigheter som skal sikre finansiell stabilitet i sektoren. Ansvaret for å sikre finansiell stabilitet er i Norge delt mellom Finansdepartementet, Norges Bank (NB) og Finanstilsynet (DSB, 2016, s 82-83; NAOB, 2021). Denne studien gjøres i samarbeid med aktøren NB. NB er Norges sentralbank og forvaltningsorgan som har som samfunnsoppdrag å fremme finansiell stabilitet og forvalter store verdier på vegne av fellesskapet (Norges Bank, 2021a, s. 5). «*Finansiell stabilitet innebærer at det finansielle systemet er robust overfor forstyrrelser og bidrar til økonomisk utvikling»* (Norges Bank, 2021b, s. 3). Årlig publiserer NB rapporten *Finansiell stabilitet,* en vurdering om sårbarhet og risiko i det finansielle systemet. Gjennomgående fra 2017 til 2021 er cyberangrep vurdert som en stadig økende trussel og som utgjør en sårbarhet for det finansielle systemet (Norges Bank, 2021b; 2020c; 2019; 2018; 2017).Samfunnsoppdragene til NB innebærer flere ulike sentralbankoppgaver, og en forutsetning for denne forvaltningen er ivaretakelse av nasjonal beredskap og sikkerhet. NB er en tilknyttet virksomhet til Finansdepartementet (FD), som igjen er underlagt den norske stat (Finansdepartementet, 2019a). Jeg vil presisere at NB er et eget rettssubjekt og er en organisasjon som baserer seg på sterk faglig kompetanse.

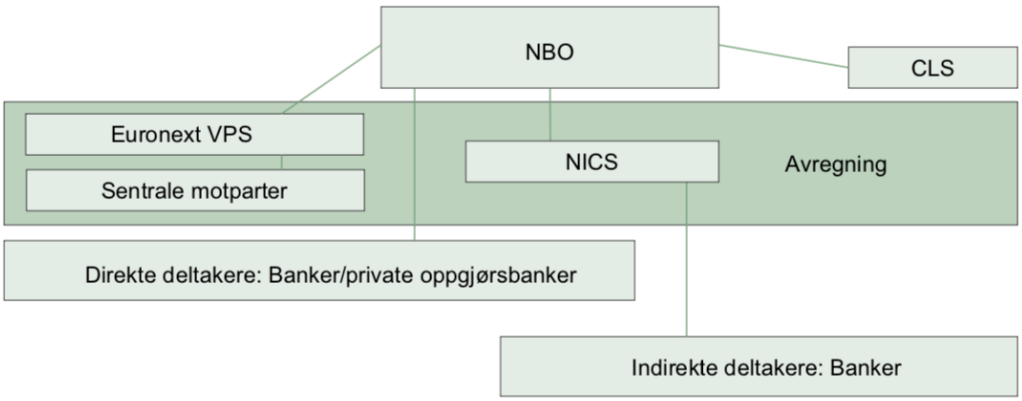
3.2 Det finansielle system (DFS)

I publikasjonene *Det norske finansielle systemet 2021* gis det en forenklet, men oversiktlig innføring i det finansielle systemet i Norge, samt hvilke oppgaver som utføres og hvordan dette utføres. Det finansielle systemet har tre hovedoppgaver: Gi personer og bedrifter muligheter til å låne og spare, gjennomføre betalinger og håndtere risiko. Det finansielle systemet kan videre deles inn i tre undergrupper: finansmarkedet, finansforetak og finansiell infrastruktur (Norges Bank, 2021, s. 8). Det er sistnevnte som vil behandles videre i denne oppgaven.

3.2.1 Finansiell infrastruktur

Den finansielle infrastrukturen består av de systemer der det gjennomføres finansielle transaksjoner mellom ulike aktører i økonomien. Det vil si alle transaksjoner som gjøres, fra vanlige betalinger med kort i butikk til transaksjoner i verdipapir- og valutamarkedet. Dette kan være infrastruktur som betalingssystemer, oppgjørssystemer for verdipapirer, verdipapirsentraler, sentrale motparter og transaksjonsregister (2021c, s. 76). Den finansielle

infrastrukturen består både av de tekniske systemene, samt avtaler og regelverk som regulerer bruken av dem. Et betalingssystem kan deles inn i to systemer: «*Systemer for betalingstjenester»*, som er det systemet som gjør det mulig for personer og foretak å betale i nettbank, bruke betalingskort og å ta ut kontanter fra sine bankkontoer. *«Interbanksystemer»,* gjør det mulig for bankene å gjøre opp betalingen seg imellom (2021c, s. 76). Det er interbanksystemer, herunder Norges Banks oppgjørssystem (NBO), som vil være relevant å redegjøre for i denne studien.



Figur 2: Det norske betalingssystem. Fra «Det norske finansielle systemet 2021,» av Norges Bank, s. 76.

Norges Banks oppgjørssystem (NBO)

NBO beskrives som selve kjernen i interbanksystemet, der NB er den øverste oppgjørsbanken i det norske betalingssystemet. Alle betalinger som blir gjort i norske kroner gjøres i siste instans opp mellom bankene i NBO. 129 banker har konto i NBO, og det inkluderer de fleste norske banker. Bankene kan delta indirekte eller direkte i de ulike oppgjørene i NBO. Indirekte vil si at en bank lar en annen bank gjennomføre oppgjøret for seg i NBO. Det er et fåtall av bankene som gjør direkte oppgjør i NBO, dvs i hovedsak de største norske bankene og norske filialer av skandinavisk bankkonsern (Norges Bank, 2021c, s. 84).

Oppgjørssystemets hovedfunksjon

Ved å bruke det internasjonale meldingssystemet SWIFT eller NBO Online får bankene tilgang til oppgjørssystem. Hver bank har en RTM-konto (Real Time Mechanism), en lånekonto og en eller flere underkontoer, også kalt LOM-kontoer (Liquidity Optimization Mechanism). SWIFT er hovedkanal for de største bankenes betalingsoppdrag til NBO. Dersom det forekommer SWIFT-baserte betalinger der banker ikke benytter SWIFT, er det etablerte

automatiserte rutiner for oppgjør og kontoinformasjon. NBO Online fungerer som en direkte kanal mellom bankene og NBO. I NBO Online kan bankene overvåke saldoene på sine kontoer, få detaljert informasjon om verdipapir de har pantsatt til fordel for NB, samt foreta spørringer og ta ut rapporter (Norges Bank, 2009).

3.2.2 Lovkrav og rammeverk

Viktige rammebetingelser for å sikre finansiell stabilitet og å drive med forebyggende beredskapsarbeid er sikkerhetsstyring ved hjelp av lovverk, forskrifter og rammeverk. Av den grunn at finanssektoren er regulert av en rekke lovkrav og rammeverk vil det følgende gis en kort oppsummering av de bestemmelser og rammeverk som anses som relevante i lys av aktør og tema for oppgaven. Se vedlegg 4 for en utfyllende og detaljert beskrivelse av lovverket.

Oppsummering av relevant lovverk

De fire hovedprinsippene i arbeidet med samfunnssikkerhet legger noen overordnede føringer på hvordan organisasjoner skal ivareta krisehåndtering og beredskapsarbeidet. I kontekst av denne studien er det samvirkeprinsippet som vil vektlegges. Det er likevel slik at i en samhandlingskontekst kan ansvarsprinsippet virke som en konkurrerende faktor. Ansvarsprinsippet skal sørge for at den organisasjonen som har ansvar for et fagområde i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og håndtering av hendelsen på området. Samvirkeprinsippet tar for seg hvordan virksomheter skal legge til rette for samvirke mellom relevante aktører i arbeidet med sikkerhet (Meld. St. 10, 2016-2017, s. 20). Prinsippene skal veies likt og ved regulering søker sikkerhetsloven søke å balansere de to prinsippene. Dette ved at sikkerhetsloven fastslår både behovet for et sentralt og tverrsektorielt samarbeid, samtidig som ansvarsprinsippet for enhver sektor lovfestes. Sikkerhetsloven regulerer tjenester og infrastruktur av samfunnskritisk betydning slik som betalingssystemer (Deloitte, 2022). Formålet med loven er å bidra til å forebygge, avdekke og motvirke sikkerhetstruende virksomhet (Sikkerhetsloven, 2019). Loven dekker dermed tilsiktede handlinger, men tar ikke for seg utilsiktede handlinger. Videre sikrer loven at NSM har ansvaret for koordineringsoppgaver som for eksempel innebærer å legge til rette for informasjonsdeling (NOU 2018: 14, s. 34).

Sentralbankloven (2019) regulerer NB sin rolle og ansvar i den finansielle infrastrukturen. Formålet med loven er å opprettholde en stabil pengeverdi, fremme stabilitet i det finansielle systemet og sikre et effektivt og sikkert betalingssystem jf. § 1-2, Sentralbankloven. I

betalingssystemloven er det hjemlet at finanssektoren har et ansvar for å dimensjonere robuste systemer, og at aktørene selv har ansvar for å ta hensyn til risiko og effektivitet ved drift av interbanksystemene (Direktoratet for samfunnssikkerhet og beredskap, 2016, s. 84). Etter betalingssystemloven (1999) har Finanstilsynet ansvar for tilsyn knyttet til de systemer for kunderettede betalingstjenester og systemer for verdipapiroppgjør, mens NB har konsesjons- og tilsynsmyndighet med interbanksystemene (Norges Bank, 2021d, s. 10). IKT-forskriften (2003) er supplerende til betalingssystemloven og er en viktig del av sikkerhetsstyringen av finanssektoren. Denne forskriften er gjeldende for alle norske finans- og bankvirksomheter i finanssektoren, samt IKT-systemer som har betydning for foretakets virksomhet. Bestemmelsen i forskriften påser at virksomheter gjennomfører risikoanalyser og fastsetter kriterier for akseptabel risiko i forbindelse med bruk av IKT-systemene jf. § 3 (IKT-forskriften, 2003). NB omfattes ikke av denne forskriften, men følger også denne forskriften i tråd med god praksis for viktige IKT-systemer (Norges Bank, 2019d, s. 8).

3.3 Cybersikkerhet i finanssektoren

I dette avsnittet vil jeg forsøke å kontekstualisere hva cybersikkerhet er i finanssektoren. Først og fremst er det hensiktsmessig å definere hva cybersikkerhet er. Det finnes utallige begreper som oppfattes synonymt med cybersikkerhet, som IKT-sikkerhet og digital sikkerhet. Innholdet i alle disse begrepene varierer og har en tendens til å gli over i hverandre (NOU 2018: 14, s. 13). Martin (2019) definerer cybersikkerhet som *«beskyttelsen av digitale systemer, dataene på dem og tjenestene de leverer mot uautorisert tilgang, skade eller misbruk» (2019, s. 218)*. I denne definisjonen legges det vekt på beskyttelsen som en evne eller virkemiddel for å hindre tilgang, skade eller misbruk av systemer, data og tjenester. Kavak et al., (2021) poengterer at det er nesten umulig å finne en konsensus i definisjonen av cybersikkerhet. Dette med bakgrunn i cybersikkerhets dynamiske form. Ved å samle sammen definisjoner fra ulike kilder har han kommet frem til at sikkerhetsmålene med cybersikkerhet er å forsvare og beskytte *cyberspace*[2] for å sikre tilgjengelighet, integritet og konfidensialitet (Kavak et al., 2021, s. 2).

Videre deler han cybersikkerhet inn i tre dimensjoner: mål, trusler og forebyggende tiltak. Følgende definerer han cybersikkerhet som *«praksisen med å beskytte mål og deres operasjoner mot trusler, gjennom en kombinasjon av forebyggende tiltak»* (Kavak et al., 2021, s. 2). Dette er også i overenstemmelse med Justis- og beredskapsdepartementet forståelse av

[2] «Cyberspace» er en betegnelse på en «verden» av sammenkoplede datasystemer og informasjonsressurser.

begrepet IKT-sikkerhet (NOU 2015: 13, s 34). Videre kan en si at cybersikkerhet omfatter en beskyttelse av alt cyberdomenet inkluderer. Eksempler på dette er datasystemer og kommunikasjonsinfrastruktur. I denne studien har jeg derfor på samme måte som departementene valgt å definere cybersikkerhet som:

> Digital sikkerhet handler om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi. Brukes synonymt med begrepene IKT-sikkerhet og cybersikkerhet (Departementene, 2019, s. 6).

Finanssektoren er heldigitalisert og er bygget på en infrastruktur som er helt avhengig av cyberdomenet, og det kan hevdes at cybersikkerhet har en signifikant betydning for sektoren. Det er dermed rimelig å påstå at alvorlige cyberangrep som rammer sektoren kan få svært negative følger. Tar vi utgangspunkt i den utvidede definisjonen av cybersikkerhet til Kavak et al., (2021) er forebyggende tiltak essensielt for å styrke cybersikkerheten. Tiltakene har han igjen delt inn i tre underkategorier: Teknologi, kunnskap og trening. Teknologi dreier seg som de verktøy, teknikker og programvarer som kan oppdage, forhindre eller stoppe cyberangrep. Det er likevel de to sist nevnte som er avgjørende for å styrke cybersikkerhet, da de fleste cyberhendelser innebærer menneskelige feil som faktor (Kavak et al., 2021, s. 4).

For at de forebyggende tiltakene skal være effektive må de ta for seg menneskelige komponenter. Organisasjonen må trene, ha kunnskap og utdanning i cybersikkerhet. Det vil si at det må være en grunnleggende forståelse av hva cybersikkerhet dreier seg om. Opplæring og trening spenner fra passordsikring, kunnskap om angrepsmetodikk og trening på hvordan sikkerhetseksperter skal kunne oppdage, håndtere og reagere på cyberangrep. Organisasjonen må også utdannes i cybersikkerhet og dette kan skje med implementering og håndhevelse av retningslinjer og prosedyrer. Interne dokumenter som beskriver beste praksis samt noen generelle retningslinjer som deles i organisasjon er nødvendige for å forbedre sikkerheten (Kavak et al., 2021, s. 4). En kombinasjon av tekniske tiltak som beskytter mål mot trusler, samt en rekke forebyggende tiltak er å anse som nødvendige for å styrke cybersikkerheten i finanssektoren.

3.4 Beredskapsøvelse Cyber22

Cyber22 er en beredskapsøvelse initiert og ledet av aktøren NB. Bakgrunnen for øvelsen var et behov for å gjennomføre flere øvelser på grunn av et omfattende og komplekst aktørbilde. I belysningen av det komplekse aktørbildet var det et behov for øving på roller, ansvar,

koordinering og samhandling. Det er med andre ord helt sentralt å øve på samvirke. En intern arbeidsgruppe startet arbeidet med øvelsen i mai 2021. Øvelsen skulle egentlig ha funnet sted januar 2022, men på grunn av restriksjoner som følge av situasjonen med covid-19-pandemien ble øvelsen utsatt til mai 2022. Følgende viser tabell 3 hovedmål for øvelsen.

Tabell 3: Hovedmål for øvelse Cyber22

Hovedmål for øvelsen
Effektivt håndtere en kompleks og tilsiktet digital hendelse.
Kriseorganisasjonen skal raskt oppnå situasjonsbevissthet og iverksette tidsriktige tiltak.
Samvirke mellom relevante aktører ivaretas.

Scenarioet i øvelsen bygger på det sikkerhetspolitiske landskapet har drastisk forverret seg de siste månedene. Dette har ført til at Norge har fått et svært anstrengt forhold til en av sine naboer. Motivasjonen til den ondsinnede aktøren er å vise styrke og skremme Norge gjennom et cyberangrep mot finansielle tjenester og IT-system. Beredskapsutvalget for finansiell infrastruktur får en sentral rolle i håndtering av hendelsen. Deltakerne på øvelsen er av de mest sentrale aktørene innenfor finansiell virksomhet.

Beredskapsutvalget for finansiell infrastruktur (BFI)

Beredskapsutvalget for finansiell infrastruktur (BFI) sikrer samhandling og koordinering i den Norske finansielle infrastrukturen, og de skal gjennom koordineringen komme frem til tiltak for å forebygge og håndtere krisesituasjoner som kan resultere i store forstyrrelser. Utvalget består av sentrale aktører i finanssektoren. Finanstilsynet har et overordnet ansvar for ledelse og sekretariat. BFI er et helt sentralt samhandlingsforum for at Finanstilsynet og NB kan holde samlet kontakt med de mest sentrale aktørene (Meld. St. 31, 2020-2021, s. 40). BFI vil dermed få en viktig rolle i øvelsen Cyber22, da det vil kreve rask etablering av et samhandlingsforum.

4. Teori

I dette kapittelet presenteres et utvalg av teori som anses å være relevant for studiens problemstilling og tema. Det teoretiske rammeverket er basert på akademiske verk innenfor tematikken. Det vil suppleres med funn fra dokumentstudiet der tematikken gjør seg relevant. Det er lagt vekt på å beskrive teori som kan sees i sammenheng med planlegging og gjennomføring av øvelsen Cyber22. Først gis det en teoretisk beskrivelse av beredskap, herunder beredskapsplanlegging der øvelse spesifikt presenteres. Deretter går jeg nærmere inn på hva krisehåndtering innebærer, og hvordan krisehåndtering kan sees i lys av cyberhendelser. Videre gis det en beskrivelse på håndtering av cyber i et systemteoretisk perspektiv. Det finnes ikke noe fullstendig teoretisk bidrag for hva samvirke som konsept er. Dermed har det vært et behov for å hente informasjon fra flere kilder som akademiske verk og offentlige dokumenter for å beskrive samvirkekonseptet i sin helhet. Avslutningsvis beskrives teorien om resiliens knyttet til cyber. Det fordi teorien anses som svært relevant i tilknytning til samvirke-konseptet.

4.1 Beredskap og beredskapsplanlegging

Beredskap handler i bunn og grunn om å være forberedt. Direktoratet for samfunnssikkerhet og beredskap (DSB) har definert beredskap som:

> Evne til å iverksette forhåndsplanlagte aktiviteter når det oppstår en ekstraordinær situasjon. Alle virksomheter med ansvar for kritiske samfunnsfunksjoner forutsettes å ha beredskapsevne (DSB, 2016, s. 29).

Det finnes utallige definisjoner og beskrivelser av begrepet beredskap. Staupe-Delgado & Kruke (2017) forsøker å konseptualisere begrepet i sin artikkel: «*Preparedness: Unpacking and clarifying the concept».* Gjennom den omfattende litteraturstudien finner forfatterne syv dimensjoner ved beredskapskonseptet. De tre første er de minimale kjennetegnene for beredskap: *aktiv, kontinuerlig* og *forutseende*. Den *aktive* dimensjonen av beredskapen gjør det mulig for *«sosiale enheter å reagere aktivt når en krise inntreffer»* (Tierny et al., 2001, s. 5). Det at beredskap forstås som aktiv tillegger den et fokus på aktiviteter og operativ kapasitet som ofte beskrives som evner og nødvendige oppgaver. Graden av trening og øvelser som involveres i forberedelsen vil kunne være avgjørende for beredskapen. Det hevdes at dersom det er mangel på aktivitet i dimensjoneringen av beredskapen blir planene foreldet (McConnell & Drennan, 2006; Delgado & Kruke, 2017, s. 216).

En viss grad av aktivitet kan derfor anses som et minimum av beredskap. Delgado & Kruke peker også på at det er et skifte, som innebærer et enda større fokus på resiliens og økt

tilpasningsevne. Dette skiftet anerkjennes som positivt i utvidelse av beredskapskonseptets beste praksis. Videre sees beredskap på som en *kontinuerlig* prosess. Det betyr at beredskap i seg selv ikke er et ferdig produkt, men en prosess som må jobbes med kontinuerlig for å opprettholde en beredskapsevne. Beredskapsplanen beskrives ofte som et levende dokument av fordi den hele tiden må oppdateres. Det *forutseende* handler blant annet om at beredskapen fokuserer på reduserende og akseptabel risiko. Det fordi vi ikke kan forutse alle situasjoner, men likevel ha en forståelse av at vi kan forebygge potensielle farer. Nytenking om risiko legger større vekt på usikkerhet og kompleksitet. Med en slik tenkning planlegges det for en uforutsigbarhet, samtidig som det tillater tilstrekkelig improvisasjon og fleksibilitet (Delgado & Kruke, 2017, s. 218). De minimale kjennetegnene er selve kjernen av konseptet og må være tilstede i enhver beredskapssammenheng.

I de bredere definisjonene av beredskap finner også forfatterne følgende maksimale kjennetegn: *sosial, planlagt, ikke-strukturelt* og *muliggjørende*. Ved at beredskap er *sosial* innebærer at beredskapen har en rolle i beskyttelse av befolkningen (Delgado & Kruke, 2007, s. 218). Videre er *planlegging* en veldig viktig del av beredskapsarbeidet (Alexander, 2016; Perry & Lindell, 2003 sitert i Delgado & Kruke, 2017, s. 218). Planleggingen befinner seg først og fremst i førkrisefasen. På denne måten sees beredskap som en del av en prosess i krisehåndteringen. Eriksen et al., (2021) definerer beredskap som *en forberedelse og utøvelse av konsekvenshåndtering ved uønskede situasjoner* (2021, s. 30). Det er viktig å poengtere at planlegging er mer enn bare skriftlige planer. Det er en kombinasjon av nøye systematisk arbeid og analyser for å identifisere uønskede hendelser samt øving, trening og oversikt over tilgjengelige ressurser (Delgado & Kruke, 2017, s. 219).

Det at beredskapen innebærer en *ikke-strukturell* dimensjon samsvarer med de minimale kjennetegnene. Det vil si at beredskapstiltak er aktive tiltak for å forutse problemer for å kunne håndtere krisene effektivt, og ha de ressursene som trengs på plass på forhånd. Beredskapstiltak sees i stor grad på som ikke-strukturelle tiltak. Derimot er det også skadebegrensende tiltak som kan for eksempel være fysiske barrierer som kan forstås som både strukturelle og ikke-strukturelle.

Det er likevel lagt vekt på en ikke-strukturell dimensjon i beredskapen fordi det er tiltak som aktivt går inn for å ta vare på sikkerheten (Delgado & Kruke, 2017, s. 219). Den utvidede definisjonen av beredskap innebærer ikke bare fokus på respons, men også økt fokus på å oppnå resiliens både i planleggingen før og i gjenopprettingen av en krise. På denne måten forstås beredskap som noe *muliggjørende* (Delgado & Kruke, 2017, s. 220). I denne studien sees beredskap i sammenheng med krisehåndtering, og som en forutsetning for å kunne håndtere fremtidige uønskede hendelser med de syv dimensjonene i grunn. Det er nødvendig i denne studien å se det i sammenheng med krisehåndtering, fordi det ønskes at en beredskapsøvelse skal være trening under så reelle forhold som mulig.

4.1.1 Øvelser

En sentral del av beredskapsarbeidet er øving og trening (Eriksen et al., 2021; Engen et al., 2016). Hvorvidt det skilles mellom trening og øving varierer både i offentlig dokumenter og litteraturen for øvrig. Engen et al., (2016) ser på trening som det fundamentale grunnlaget for øving, og beskriver trening som enkeltferdigheter som stilles som krav til enhver posisjon i utførelse av oppgaver, prosedyrer eller bruk av utsyr i en gitt arbeidssituasjon (2016, s. 363). Øving består av å teste og validere relevansen og effektiviteten til den enkeltes trening samt betrakte kvaliteten på samvirke mellom ulike aktører (Perry, 2003 sitert i Engen et al., 2016, s. 363).

Trening og øving kan inngå for enkeltindividers, organisasjoners og samfunnets forberedelse i å håndtere en uønsket hendelse. Trening og øving blir en kobling mellom beredskapsplanlegging med fordeling av ressurser på den ene siden, og håndtering av en uønsket hendelse på andre siden (Engen et al., 2016, s. 361). I denne studien sees øving og trening i sammenheng, og «øvelser» brukes heretter som et samlende begrep. *Øvelser* er et viktig moment i læringsarbeidet for håndtering av kriser, og et vesentlig element i *kompetanseheving* i virksomheter (Engen et al., 2016, s. 362; NOU, 2015: 13, s 221). Øvelser gir mulighet til å *teste* egen kompetanse og ferdigheter i en trygg setting samt evaluere prosedyrer, planverk, ressurser og utstyr (Engen et al., 2016, s. 363). Sommer et al., (2020) viser til kompetanseheving, testing og markering som de tre viktigste grunnene til hvorfor vi trener. *Markering* handler om å sende et signal som viser at aktørene tar utfordringer på alvor og viser at de er forberedt (Sommer et al., 2020, sitert i Eriksen et al., 2021, s. 240). Prosessen ved å forbedre responsaktører på hendelser, forbedrer evnen til samhandling, koordinering og kommunikasjonen i en organisasjon (Bartnes & Moe, 2017, s. 280).

Fullskalaøvelse

Det finnes flere typer øvelser, de vanligste er *tabletop-øvelser*, *funksjonelle øvelser* og *fullskalaøvelser*. Videre vil fokuset være på fullskalaøvelser, ettersom tabletop-øvelse og funksjonelle øvelser ikke tester samvirke fullt ut (Engen et al., 2016, s. 364). Fullskalaøvelser er av de mest omfattede, komplekse og realistiske øvingsformene. Slike øvelser bygger på et realistisk scenario og innebærer mulighet for høy stressfaktor. Målsetning med øvelsen er å teste hele eller store deler av beredskapsplanen og samvirke med andre relevante aktører. En utfordring for slike øvelser og som kan virke begrensende, er at det kreves en svært ressurskrevende planlegging og gjennomføring for å oppnå læringseffekt. Videre er et dilemma for øvingsplanleggere å skape et behov for realisme og usikkerhet. Realistiske øvelser øker både muligheten for innlevelse og læring. Engen et al., forklarer at gjenkjenning og usikkerhet bør være tilstede for å kunne oppleve scenario som realistisk. *Gjenkjenning* kan bidra til at øvingsdeltakere opplever mestringsfølelse og gir mulighet til å iverksette tiltak basert på kunnskap og egne erfaringer. Videre er *usikkerhet* et viktig moment, men som kan være vanskelig å spille inn. Usikkerhet kan skape økt stressnivå hos øvingsdeltakerne, som forbindes med tidspress, men det kreves god planlegging for å oppnå dette (Engen et al., 2016 s. 366).

Roller og aktører i øvelser

Krisehåndtering involverer flere aktører og berører enda flere mennesker samt virksomheter og organisasjoner. Øvelser er derfor en viktig kontaktflate mellom ulike organisasjoner som ofte jobber hver for seg (Engen et al., 2016, s. 290). En forutsetning for relevant øvingsplanlegging er en sammensetning av en gruppe mennesker med den nødvendige ekspertisen i organisasjonens beredskapsarbeid, samt funksjoner, prosedyrer og aktører som skal øves. Øvingsplanleggerne setter rammen for øvelsen, der de spesifiserer øvingsmålene og etablerer øvingsscenarioet som skal gi en relevant øvingsmulighet. De utarbeider en dreiebok som skal spille inn øvelsen. I dreieboken spesifiseres forventingene til responsen til øvingsdeltakere samt etableres en struktur for evaluering og læring i etterkant av øvelsen. Spillstab driver øvelsen fremover ved hjelp av innspill spesifisert i dreieboken, og forøvrig kan også øvingsledelsen ha funksjon som spillstab. Spillstab skal sørge for nok fremdrift, slik at deltakere både kan håndtere og få utbytte av øvelsen. Spillstaben fungerer også som responscelle for aktører som ikke spiller. I tillegg brukes markører i enkelte øvelser, markører er skuespillere som for eksempel spiller omkomne, skadde, tilskuere, pårørende eller journalister. Roller som observatører er de som kan ha nytte av å observere øvelsen, og evaluatorrollen har i oppgave å samle inn data og

erfaring som sammenfattes i en evalueringsrapport og tas med i læringsarbeidet (Engen et al., 2016, s. 356).

4.2 Krisehåndtering

Krisehåndtering er selve responsen fra samfunnet og organisasjoner for å begrense skader, samt forebygge og redusere konsekvensene av en krisesituasjon. Responsen innebærer en iverksettelse av responssystemer, beredskapsplaner og flere aksjoner på ulike nivå for å håndtere hendelsen (Njå et al., 2020, s. 194). Boin & McConnel (2007) beskriver krisehåndtering som en helhetlig prosess som involverer *forebygging, planlegging, akutt respons, gjenoppretting og læring.* Beredskapsarbeid som planlegging og trening er helt sentralt i forberedelsen på en krise. Videre poengterer forfatterne at også resiliens er viktig i forberedelsen på håndtering av kriser. Resiliens defineres som *«the ability to ´bounce back` after suffering a damaging blow"* (Boin & McConnel, 2007, s. 52 & 54). Resiliens vil utdypes nærmere i delkapittel 4.5.

I litteraturen skilles det mellom tre faser i krisehåndteringen. Akutt krisefase som er selve responsen på krisen. Etterkrisefasen som dreier seg om gjenoppretting og læring av krisen, og førkrisefasen som er den forberedende og forebyggende fasen. I denne studien er det tatt utgangspunkt i det utvidete krisebegrepet der fasene sees i sammenheng med hverandre (Engen et al., 2016, s. 264). På denne måten ser en ikke på en krise som en ekstraordinær hendelse som inntreffer uten forvarsel, men som en prosess der det er mulighet til å forebygge og forberede seg på krisehåndteringen. Ved en slik forståelse av krisebegrepet anerkjenner en også betydningen av å kunne kartlegge og identifisere trusler og risiko. Når dette er på plass, kan risiko håndteres gjennom en helhetlig tilnærming i beredskapsarbeidet.

4.2.1 Styring i kriser

Alle kriser må ledes og kriseledelsen har et overordnet, helthetlig ansvar for flere oppgaver. Blant annet å fatte beslutninger samt å sørge for at lover og regler overholdes. Å lede handler om å organisere slik at det er klart hvem som har ansvar for de ulike oppgavene. Videre må ledere ha kunnskap om hvilke ressurser som er tilgjengelig i tillegg til koordinering og kontrollering. Ledelsen har av den grunn også et ansvar for å sikre et samvirke, både i forkant av en krise, under en krise og i etterkrisefasen. Det er likevel ikke slik at det kun er kriseledelsen som fatter beslutninger. En krise kan være uoversiktlig med flere aktører med ulike roller og

mål. Informasjon kan endres, tidspress oppstår og kritiske verdier står på spill. Under slike forhold skal både innsatsmannskap og ledere fatte beslutninger (Njå et al., 2020, s. 194-195).

Hierarki i kriseresponsen

I kriseresponsen er det mange involverte på ulike nivåer, en vanlig inndeling er strategisk nivå, operasjonelt nivå og taktisk nivå. Strategisk nivå er den sentrale ledelsen i en organisasjon.

> Deres oppgaver er å lede og koordinere innsatsen for å ivareta virksomheten overordnede interesser for å sikre videre drift og ivareta virksomhetens omdømme – konsentrere innsatten ut mot virksomhetens interessenter og øvrige omgivelser (Lunde, 2019, s. 94).

Taktisk nivå befinner seg nærmest hendelsesstedet, det vil si ... *det fysiske eller virtuelle sted hvor en beredskapssituasjon har inntruffet eller har sitt utspring* ... (Lunde, 2019, s. 94). Deres oppgaver er å ... *lede og koordinere bekjempelse og ivaretakelse på eller nært til hendelsesstedet for å forhindre eller redusere på skade* ... Mellom strategisk og taktisk nivå er det operasjonelle nivået. Operasjonelt nivå skal ... *lede, koordinere og støtte taktisk nivå med kompetanse, kapasiteter og kommunikasjon* ... (Lunde, 2019, s. 94). I et større perspektiv kan det også inkludere det politiske nivået. Cyber22 innebærer et scenario av en slik karakter der politisk nivå kan gjøre seg aktuell i håndtering av hendelsen. Politisk nivå ... *skal ivareta lokale, regionale, nasjonale og internasjonale felles interesser som er truet eller utfordret som følge av den oppståtte beredskapssituasjonen – konsentrere innsatsen ut mot fellesskapets interessenter og øvrige omgivelser* (Lunde, 2019, s. 94).

Styringstilnærming

I litteraturen deles det grovt sett inn i to tilnærminger til styring: sentralisert og desentralisert styring. Sentralisert styring er en byråkratisk tilnærming med et begrenset antall ledere på toppen. Det hevdes at et slikt styringssett er best under stabile situasjoner der styringen skjer i et etablert sentraliserte ledelsesstrukturer (Engen et al., 2016, s. 303). Når det gjelder den andre styringsformen, er dette en desentralisert styring som følge av hva slakrisens karakter. I utgangspunktet er denne styringsformen egnet for kriser der de tilgjengelige ressursene brukes på et lokalt nivå. Dette kan kalles en «bottom-up» tilnærming, ved at lavere nivå i hierarkiet trekker ressurser fra nivået over. Dersom lokale responsstrukturer blir lammet og ikke klarer å håndtere krisen vil tilnærmingen gå fra desentralisert til en mer sentralisert tilnærming.

Dynes (1993) har sett på to modeller for tilnærming til styring, der han viser til militærmodellen (sentralisert styringsform) og problemløsningsmodellen (desentralisert styringsform). Militærmodellen bygger på teorien om at kriser består av kaos som krever håndtering i form av styring og kontroll. Ved forskning på organisert atferd i akutt krisefase viser det seg imidlertid at problemløsningsmodellen er mer effektiv. Denne modellen forutsetter tre faktorer for effektiv ledelse og krisehåndtering. (1) Sosial kontinuitet, (2) koordinering og (3) samarbeid. Poenget til Dynes (1993) er at krisehåndtering ikke krever en sentralisert styreform bestående av kontroll, men at organisasjoner må fokusere på å forstå de sosiale mekanismene og prosessene for å håndtere problemer som oppstår (Dynes, 1993, s. 7-8). Hvilken tilnærming som anvendes avhenger av beslutningstakere på ulike nivåer sin oppfattelse av situasjonen og krisens karakter.

4.2.2 Grenseoverskridende kriser

Et essensielt spørsmål i kontekst av denne studien er hva som skiller cyberhendelser fra håndtering av mer «tradisjonelle» krisesituasjoner, som for eksempel brann i bygg eller flom. Det vil være både likheter og ulikheter i håndtering av cyberangrep kontra en annen krisesituasjon, slik som det også vil være ulikheter i håndtering av brann i bygg og flom. Det er likevel hensiktsmessig å utdype hva cyber er, og hva slags utfordringer som er knyttet til håndtering av slike kriser.

I litteraturen kjennetegnes cyberkriser ofte som «transboundary crisis» eller på norsk «grenseoverskridende kriser». Rosenthal et al., (1989) påpeker at en krise tradisjonelt kan defineres som en hendelse som truer kjerneverdier eller livsopprettholdende systemer, og som krever en umiddelbar respons under forhold med høy usikkerhet. Det som skiller «transboundary crisis» fra den tradisjonelle krisedefinisjonen er dens tendens til ikke å være begrenset geografisk, politisk, sektorielt, økonomisk, sosialt og juridisk. Dermed kan «transboundary crisis» forstås som:

> A crisis which transcends political boundaries (such as geographical borders, jurisdictions or levels of governance), functional boundaries (such as sectoral, policy and industry domains) and time boundaries" (Rosenthal et al., 1989; Backman, 2020, s. 430).

Det er flere nøkkelpunkt i litteraturen som kjennetegner grenseoverskridende kriser. Blant annet kreves det en identifisering av kompleksiteten ved håndtering av en slik krise. Nettopp dette med kompleksitet pekte Snowden & Boone (2007) også på gjennom Cynefine rammeverket.

Cynefine er en teori som bygger på å identifisere krisens kontekst for å kunne ta gode beslutninger. I denne teorien påpekes det at kriser beveger seg fra det kompliserte til det komplekse, og fra det enkle til det kaotiske:

> Complex and chaotic contexts are unordered – there is no immediately apparent relationship between cause and effect, and the way forward is determined based on emerging patterns (Snowden & Boone, 2007, s. 72).

Så på hvilken måte er cyberdomenet komplekst? Det metaforiske eksempelet der en Ferrari er en komplisert maskin fordi det kreves ekspertise for å sette den sammen, imens en regnskog er kompleks fordi arter utryddes, værforhold endres og landsbruksprosjekter omdirigerer vannkilder – og dermed blir helheten langt mer en summen av delene *(*Snowden & Boone, 2007, s. 74). På samme måte kjennetegnes cyberspace med sine gjensidige avhengigheter tett vevd sammen av flere organisasjoner – bygget på det komplekse, der delene er av mindre betydning og helheten er signifikant.

Når en krise overskrider ulike grenser, der den for eksempel ikke bare rammer en organisasjon, men flere, oppstår det høy etterspørsel etter informasjon fra ulike aktører. Inkubasjonstiden av en cyberkrise inneholder perioder med langsom utvikling kombinert med rask eskalering og uforutsigbarhet. Moderne teknologisk utvikling kan være til støtte og verktøy ved kriserespons når det kommer til håndtering av «transboundary crisis». samtidig kan de også skape enda mer kompleksiteter i en allerede kompleks kriserespons. Vi utvikler og organiserer systemer som med sine gjensidige avhengigheter kan gjøre dem sårbare for feil. Problemet er her at vi modifiserer disse systemene for å gjøre dem sikrere samtidig som vi gjør de mer komplekse. Dersom komplekse systemer ikke er isolert fra hverandre, kan forstyrrelser spres raskt, og dette kan føre til enda større farer i systemet (Perrow, 1999; Backman, 2020, s. 431).

I en komparativ studie av Backman (2020) analyserer hun to ulike cyberkriser. Studien analyserer to ulike tidsperioder og to ulike typer cyberangrep (ikke-målrettet ransomware angrep & målrettet DDos (denial-of-service) angrep). Videre undersøker forskeren hvordan disse korrelerte med variasjon i «transboundary crisis» krisefunksjoner, og krisehåndteringsutfordringer under utførelse av sentrale krisehåndteringsoppgaver i en nasjonal kontekst. Funnene i studien viste at krisehåndteringsutfordringene i gjennomføringen av krisehåndteringsoppgaver var tilnærmet de samme til tross for ulikheter i både tid og angrepsmetode. Utfordringene viste seg å være i overenstemmelse med forventningene i litteraturen om «transboundary crisis». Forfatteren har kommet frem til noen funn fra studien

som hun viser til kan være relevant for å håndtere cyberkriser effektivt. Deriblant nevnes det et behov for å involvere og mobilisering av teknisk kompetanse som støtte, spesielt fra privatsektor og fra det internasjonale cybersikkerhetssamfunnet. Det viste seg at operatørene som var kreative, som improviserte og brukte praktisk tenkning under cyberkrisehåndtering hindret situasjonen fra å bli verre til tross for kompleksitet og mangel på forberedelse (Backman, 2020, s. 438).

Informasjonsdeling fremheves som essensielt. For å kunne skape god informasjonsdeling kreves det kommunikasjon og et tillitsforhold mellom de ulike aktørene. En suksessfaktor var derfor å forhåndsetablere både formelle og uformelle relasjoner på tvers av funksjonelle grenser. Tillit var en viktig faktor ved etablering av disse relasjonene. Rask formidling av riktig informasjon til offentligheten viste seg å være noen av de viktigste oppgavene for en effektiv cyberkrisehåndtering. Videre var fokuset på brobygging viktig. Den ene informanten påpeker at: *«Cyberkrisehåndtering er lagarbeid»* (Backman, 2020, s. 439). Evne og kapasitet til å bygge broer mellom flere ulike aktører, både mellom statlig og private organisasjoner, var viktig for å kunne håndtere cyberkriser på best mulig måte. I en rapport av European Union Agency for Network and Information (ENISA) utgitt i 2014, undersøkes det hva som skiller cyberkrisehåndtering fra generell krisehåndtering. Funnene viste at samarbeidsmekanismene var i stor grad basert på grunnleggende prosesser som brukes både i krisehåndtering generelt og i cyberdomenet. De fleste cyberhendelser utvikles ikke til en fullverdig krise, og håndteres derfor hovedsakelig i samsvar med fundamentale prosesser som er spesifisert i eksisterende krisehåndteringsplaner, spesielt på et strategisk nivå.

Det at cyberhendelser ikke håndteres som potensielle kriser kan svekke cybersikkerheten. Dersom en krise blir en bekymring på et strategisk nivå, vil det bety et skifte av mandater og ressurser på tvers av grenser og sektorer. Ettersom cyberdomenet ikke er geografisk bundet, er det helt nødvendig med samarbeid på tvers av grenser. Dermed blir rolleavklaring og hvem skal som inkluderes desto viktigere å avklare (Trimintzios et al., 2014, s. 33). En av de viktigste forskjellene identifisert i rapporten er måten hendelser behandles. Samtidig som det i generell krisehåndtering skilles hendelser i kriser og ikke-kriser, vil det i cyberkrisehåndtering være en gråsone mellom de to. Cyberkriseutfordringer fører med seg ekstra arbeidsmengde som gjør at dynamikken i krisen endres drastisk. Dette samsvarer også med kjennetegnene i «transboundary crisis». Hvor krisen endres betraktelig fra en sakte utvikling med oppturer og nedturer, til en jevn økning i intensitet etterhvert som hendelsen vokser seg større. Til den velter over i en full

krise som ikke bare er mer intens, langvarig og kontinuerlig. Det man ser med slike kriser er at de raskt går fra en krise lokalt i organisasjonen til at de løftes til et nasjonalt og politisk nivå (Trimintzios et al., 2014, s. 34). Kriser som er begrenset til å være lokalt/internt i organisasjonen vil ofte gå over til et nasjonalt eller politisk nivå etterhvert.

4.3 Systemteori

4.3.1 Normal accident theory (NAT)

NAT bygger på teorien om at ulykker kan forklares gjennom kompleksitet og kobling for hvorfor det skjer ulykker i systemer hos organisasjoner (Perrow, 1999, s. 62). Fokuset ligger på egenskapene i systemene, og dermed ikke konvensjonelle forklaringsfeil som operatørfeil, feil i design, lite erfaring eller utilstrekkelig trent personell. Dette skyldes at de fleste systemer kjennetegnes av slike feil, og at de dermed ikke tar hensyn til variasjoner i feilraten til ulike type systemer. Perrow hevder det finnes noe mer grunnleggende som bidrar til at systemene svikter, og viser til at det trengs en forklaring som baseres på systemets egenskaper (Perrow, 1999, s. 62). Tidligere i teorikapittelet har jeg definert cyberangrep som en uønsket hendelse. Perrow påpeker at ikke alle uønskete hendelser kan defineres som ulykker, men grader av forstyrrelser i systemene må være avgjørende for hva som defineres som ulykker, og skaden må være av rimelig betydning (Perrow, 1999, s. 64-65). Perrow definerer ulykker som følgende:

> An accident is a failure in a subsystem, or the system as a whole, that damages more than one unit and in doing so disrupts the ongoing or future output of the system (Perrow, 1999, s. 66).

Perrow vektlegger at definisjonene av hendelser og ulykker er viktige når en skal ta i bruk systemteoretisk analyse. *Systemer* kan deles inn i fire nivåer: enheter, deler, undersystemer og system. *Hendelse*r involverer kun skade eller feil på deler eller enheter selv om feilen kan påvirke systemet i den grad at det må stanses. *Ulykker* involverer skade på delsystemer eller systemet som helhet, og som gjør at det kreves umiddelbar stans av systemet. *Komponentfeilulykker* involverer en eller flere komponentfeil (del, enhet eller delsystem) som er koblet i en sekvens. *Systemulykker* involverer uventet interaksjon av flere feil. Det gjøres et skille på komponentfeilulykker og systemulykker på grunnlag av interaksjon, eller at feil er forventet eller midlertidig. I Perrows definisjon må systemulykker ha flere feil, og de vil sannsynligvis være uavhengige enheter eller undersystemer. En systemulykke kan likevel også starte som en komponentfeil, for eksempel en operatørfeil. Det er ikke kilden til ulykken som skiller de, det er tilstedeværelsen eller ikke av flere feil som samhandler på uventet måte (Perrow, 1999, s. 70-71).

Komplekse interaksjoner

Ifølge Perrow består systemer som er utsatt for systemulykker av komplekse interaksjoner og tette koblinger. I vår teknologiske og sosiale verden blir systemene stadig større og mer avhengige av hverandre, som dog utgjør sårbarheter som kan føre til ulykker. Interaksjon trenger nødvendigvis ikke være forvirrende eller komplekse. I et *lineært system* er det enklere å peke ut feilen, skru av systemet for så å fikse problemet. Utfordringene i *komplekse systemer* der ulike deler utgjør flere ulike funksjoner er problematiske. I et slikt system vil en feil kunne forplante seg til andre systemer også (Perrow, 1999, s. 72). I slike systemer er redundante løsninger ofte hovedforsvaret, samtidig som det også kan være en hovedkilde til feil. Hovedproblemet ligger da ikke i konvensjonelle feil, men kan skyldes selve kompleksiteten i systemet (Perrow, 1999, s. 73). Det er dette Perrow referer til som *komplekse interaksjoner* som han definerer som:

> Complex interactions are those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible (Perrow, 1999, s. 78).

Slike interaksjoner kan forstås som ulike forgreningsveier, tilbakemeldingssløyfer eller hopp fra en lineær sekvens til en annen på grunn av nærhet. Samtidig påpeker han at de fleste systemer er av en lineær karakter, men selv disse systemene vil ha minst én kilde til komplekse interaksjoner, som for eksempel at miljøet kan påvirke mange enheter eller deler av et system (Perrow, 1999, s. 75).

4.3.2 Systemtilnærming

Med utgangspunkt i Perrows (1999) NAT kan systemteori ifølge Leveson (2011) brukes for å styrke sikkerheten i systemer som kjennetegnes av organisert kompleksitet. I en sikkerhetssystemtilnærming analyseres det hvordan de tekniske og sosiale aspektene samhandler sammen i systemet som helhet (Leveson, 2011, s. 63). Systemtenkningen bygger på følgende idéer:

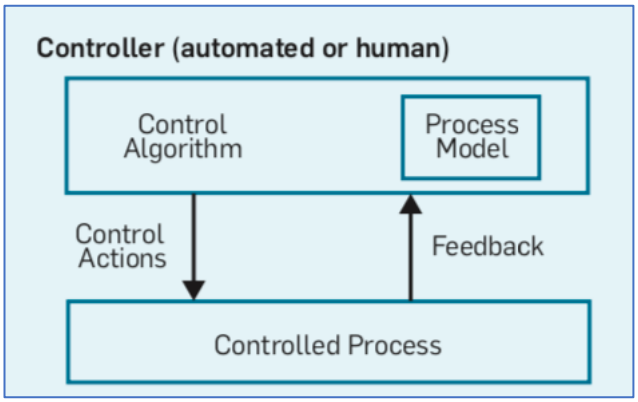
Hierarkisk kontrollstruktur og sikkerhetsbegrensninger

Modellen av systemet kan illustreres som en hierarkisk struktur i en organisasjon eller en sektor. Målet er å kunne forklare forholdene mellom de ulike nivåene. Hva som genererer nivåene, hva som skiller dem og hva som forbinder dem. Sikkerhet sees på som en fremvoksende egenskap i systemet som kommer av interaksjon mellom komponentene i systemet. Sikkerhet blir et spørsmål om vi har den nødvendige kontrollen. Hierarkiet er preget av kontrollprosesser som

opererer i grensesnittet mellom nivåene. *Sikkerhetsbegrensninger* kan omsettes til *krav* eller *begrensninger* for å sikre overordnet mål. Sikkerhetsbegrensninger brukes som et virkemiddel for å kontrollere eller tillate atferd på et lavere nivå. Dermed handler det ikke om det begrensede fokuset om å unngå feil, men heller hvordan en kan sikrer kontroll over de begrensninger som skal til for å sikre levering av betalingssystemer. Derav sikre det overordnede målet om finansiell stabilitet i eksempelvis finanssektoren. Ifølge Leveson (2011) oppstår feil og uønskede hendelser når kontrollfunksjonen er utilstrekkelig. Kommunikasjonskanaler mellom de ulike nivåene er dermed viktige for å sikre justeringer og tilpasninger. Det er nødvendig med en kontrollkanal som kommuniserer sikkerhetsbegrensningene til nivåer under, og en tilbakemeldingskanal som gir informasjon om effekten av sikkerhetsbegrensningene tilbake til nivået over. I sammenheng med denne oppgaven er det interessant å se på de funksjonene fordi det kan si noe om hvordan ulike nivåer fungerer i et samvirkeperspektiv (Leveson, 2011, s. 63-64).

Prosessmodell

Enhver kontrollfunksjon trenger en modell av prosessen. Dette er en oversikt over en menneskelig eller automatisert kontrollfunksjon. I denne oppgaven er det relevant å se på prosessmodellen som en mental modell hos en menneskelig kontrollfunksjon. En slik mental modell må inneholde informasjon om forholdet mellom systemvariablene, gjeldende tilstand og måter prosessen kan endre tilstand på. Modellen brukes for å bestemme hva slags kontrolltiltak og sikkerhetsbegrensninger som er nødvendig for å sikre ønsket drift. Tilbakemeldingskanalen fungerer dermed som en tilbakemeldingssløyfe for å opprettholde mest mulig nøyaktig bilde av modellen (Leveson, 2011, s. 87-88). Figur 3 illustrerer bilde av en kontroll- og tilbakemeldingssløyfe.



Figur 3: Kontroll- og tilbakemeldingssløyfe**.** Fra "Inside Risks An Integrated Approach to Safety and Security Based on Systems Theory" av Young & Leveson (2014), s. 33.

System-Theoretic Process Analysis for Security (STPA-Sec)

Med bakgrunn i dagens økte kompleksitet og intensivering av programvare-systemer har Young og Leveson (2013 & 2014) foreslått å utvikle en ny systemteoretisk tilnærming for å håndtere *security*-problemer, kalt STPA-Sec. I denne analysen bytter en ut den trusselfokusert tilnærming med en kontrollbasert tilnærming til sårbarheter.

> Hazards lead to safety incidents in the same way that vulnerabilities lead to security incidents. We believe that the key question facing today's security analysts is how to control vulnerabilities, not how to avoid (Young & Leveson, 2013, s. 3).

Cybersikkerhet har blitt portrettert som en taktisk utfordring. Der fokuset har vært å beskytte nettverk og informasjon fra trusselaktører. Forfatterne hevder at denne tilnærmingen til cyber hindrer fokuset på å sikre systemet og infrastrukturens funksjonalitetsevne som samfunnet er avhengig av. I praksis dreier det seg om å flytte fokuset fra beskyttelsen mot angrep (taktisk) til et bredere fokus på sosio-tekniske sårbarheter som bidrar til at forstyrrelser får forplante seg gjennom hele systemet (strategi) (Young & Leveson, 2013, s. 1). Analysen utføres på systemets funksjonelle kontrollstruktur som innebærer alle aspekter som fysiske, sosiale, logiske, beskyttelse av informasjon, drift og ledelsesaspekter. *STPA-Sec* innebærer hovedsakelig en risiko- og sårbarhetsanalyse og tar for seg tilsiktede handlinger i generering av årsakscenarier. Første etableres det systemtekniske grunnlaget for sikkerhetsanalysen. Det kritiske blir å identifisere hvilke konsekvenser som er å anse for å være uakseptable. I dette ligger spørsmålet om hvilke funksjoner som må sikres for å hindre forstyrrelse. Ved å identifisere hvilke kontrollhandlinger som kan være til trussel for systemet, for deretter å se på kontrollhandlingene, settes det inn sikkerhetsbegrensninger i form av krav. Det siste trinnet er å identifisere hvilke årsaksscenarioer som kan være årsak til brudd på sikkerhetsbegrensningene (Young & Leveson, 2014, s. 35; Young & Leveson, 2013, s. 3-4).

I analysen bør fokuset ligge på hvordan sårbarheter skal kontrolleres fremfor det å først identifisere alle truslene. For deretter å se på sårbarhetene som truslene kan utnytte som fører til konsekvenser. Gjennom en «top-down» struktur sees det først på systemsårbarheter, som sannsynligvis er langt færre enn trusler. Hvis sårbarhetene kontrolleres, kan tap forhindres på grunn av mange typer trusler og forstyrrelser. Forfatterne hevder også at en slik tilnærming løfter sikkerhetsproblemet, fra å beskytte nettverket til det overordnede problemet med å sikre

virksomhetens generelle funksjon. Analysen undergraver heller ikke trusler, men tar dette for seg mye senere i prosessen. Etter å ha generert en dypere systemforståelse av konteksten som truslene kan operere i og forstyrrelser som faktisk kan føre til kritiske tapshendelser. I dette perspektivet forkastes ikke tradisjonell sikkerhetstenking, men antyder at den er taktisk fokusert, og må forsterkes med en effektiv strategi for å lykkes (Young & Leveson, 2014, s. 33-35).

Forfatterne hevder det er flere fordeler med å gjennomføre denne analyseteknikken i sikkerhetsstyring i møte med cyberutfordringene. Først og fremst tar den for seg organisasjonens mål. I tillegg retter den seg mer mot de tingene som faktisk er innenfor kontroll av organisasjonens ledelse (Young & Leveson, 2013, s. 4). På denne måten blir cyber håndtert av både ledelsen og driftsteamet. For eksempel ved beslutning av prioriteringer uten hensyn til operatørenes kunnskap vil det sannsynligvis kunne oppstå et problem. Dette problemet vil kanskje ikke være synlige for sikkerhetsstaben, men vil være synlige for operatørene som krever tilgang for å utføre systemfunksjonene fra høyere nivå. Vellykkede sikkerhetsvurderinger krever en nøye prioritering. Ved å fastsette prioriteringer ved starten av vurderingen av systemet i motsetning til slutten, danner prioriteringene et rammeverk for å både fokusere og veilede sikkerhetsvurderingen. Denne evalueringen kan bare gjøres riktig med fordelen av å ha et perspektiv inn i den større, overordnede systemfunksjonen (Young & Leveson, 2013, s. 4).

4.4 Samvirke

I denne studien er samvirke et sentralt konsept, som må omtales nærmere for å tydeliggjøre konseptet og hvordan samvirke skal tolkes i kontekst av oppgaven. Samvirke kan virke noe svevende og lite målbart. Basert på litteratur og offentlig publikasjon vil en forsøke å beskrive noen grunnleggende momenter i tilknytning til konseptet samvirke. Samvirke er ikke et nytt begrep og har lang fartstid i tradisjonell krisehåndtering. I artikkelen til Aasland og Braut (2018) presenteres det historiske opphavet av begrepet og en drøfting av hvordan begrepet bør brukes i samfunnssikkerhetsarbeidet. «Virke», som er en del av begrepet, stammer opprinnelig fra det engelske ordet «work» og det tyske ordet «wirken». Samvirke betyr å arbeide eller virke sammen. Samvirke er også et unikt begrep i norsk sammenheng fordi det ikke lar seg så lett oversette til andre språk. Det nærmeste man kommer er det svenske ordet «samverkan» (Aasland & Braut, 2018, s. 186). Samvirke kom inn som et grunnprinsipp for alt beredskapsarbeid etter evaluering av hendelsene 22. juli 2011.

Ifølge Aasland & Braut var det uklarhet rundt samvirke som noe enn samordning og samarbeid. Samvirke skal sikre at flere relevante aktører nyttiggjøres med sin kompetanse sammen, hvor gjensidig tillit og respekt er grunnleggende faktorer (Aasland & Braut, 2018, s. 191). Samvirkeprinsippet presiserer kravet om samvirke mellom relevante aktører i arbeidet med forebygging, beredskap og krisehåndtering (St.meld. 29, 2011-2012 s. 39). Hensikten med samvirke-prinsipper er å få alle organisasjoner og virksomheter til å bruke sine ressurser og sin kompetanse til å løse utfordringer sammen. Dette forutsetter at aktørene tar hensyn til den gjensidige avhengigheten og ser ressursene som helhet. Felles beredskapsforberedelser som *øvelser* er dermed helt sentralt for å få til dette (Aasland & Braut, 2018, s. 195). En utfordring i realiteten er at samvirke vil kunne komme i konflikt med prinsippene for ansvar og likhet når de ulike ansvarsområdene skal samvirke med hverandre. Dermed for å skape best mulig samvirke er det noen klare forutsetninger som må være tilstede.

4.4.1 Tillit og kultur

Gjensidig *tillit* og god *kultur* kan sees på som grunnleggende forutsetninger for et godt samvirke. For å skape tillit mellom aktører er det nødvendig å kjenne til hverandres ressurser, kompetanse, kultur og organisering samt en egenvilje til å stille egne ressurser til disposisjon (Meld. St. 10, 2016-2017, s. 21). Den gjensidige tilliten handler også om å dele nødvendig informasjon i samarbeidet uten å undergrave hverandre (Salas, Sims & Bruke, 2005, sitert i Njå et al., 2020, s. 203). I praksis innebærer det en stor systemforståelse blant aktørene for at informasjonen deles (Njå et al., s. 193). Tillit innebærer troverdighet, persepsjon av organisasjon og det sosiale klimaet, og er viktige faktorer for å få til god kommunikasjon (Engen et al., 2016, s. 351). Et felles mål er å løse oppgaven på best mulig måte, dette forutsetter en etablering av kultur som innebærer en åpen holdning til hverandres perspektiv og kompetanse (Meld. St. 10, 2016-2017 s. 21). I studien gjort av Backman (2020) fremkom det fra intervjuobjekter at cybersikkerhet skaper sensitiv informasjon som ikke lett lar seg dele mellom aktørene, selv når det behovet for informasjonsdeling er tilstede. I den sammenheng understreket intervjuobjektene et behov for å skape tillit og å forhåndsetablere relasjonene mellom aktører som er involvert i cyberkrisehåndering (Backman, 2020, s. 433). Å forhånds etablere relasjonene mellom aktører kan også tenkes å bidra til å styrke tilliten mellom aktørene. God arbeidskultur og gjensidig tillit kan sees på som helt grunnleggende elementer for et optimalt samvirke.

4.4.2 Kommunikasjon, koordinering og informasjonsdeling

Kommunikasjon mellom responsaktører er avgjørende for nødvendig informasjonsdeling og koordinering. Det er en forutsetning for å få til et godt samvirke, og responsaktørene er avhengig av å kunne kommunisere horisontalt og vertikalt. Vertikal kommunikasjon på tvers av ulike responsorganisasjoner er avhengig av teknologiske kommunikasjonssystemer (Engen et al., 2016, s. 324). Flere organisasjoner har ofte ulike tekniske systemer for kommunikasjon og er teknisk heterogene, dette kan utfordre samvirke i krisesituasjoner. Under krisehåndtering av 22.juli viste det seg at den eneste felles plattformen for kommunikasjon var mobilnettet. Aktører hadde dermed ikke mulighet til å utveksle gradert informasjon på grunn av mangel på godkjente systemer for informasjonsutveksling (NOU 2015; 13, s. 244).

Krisekommunikasjon er en prosess som både består av forvaltning av kunnskap og styring av responsen (Coombs 2010, sitert i Engen et al., s. 324). Kunnskapsforvaltningen danner grunnlaget for en situasjonsforståelse, og underveis vil responsen kontinuerlig ha behov for kunnskapsgenerering for å få et oppdatert situasjonsbilde. Krisekommunikasjon kan defineres som «med formål om å få aktører til å tilpasse sin atferd til den informasjonen som kommuniseres i en krise» (Engen et al., 2016, s. 325). Et annet viktig aspekt med kommunikasjon er også en bekreftende kommunikasjon – om mottaker har forstått informasjonen som er gitt. Videre bør også kommunikasjonen styres av informasjonsbehovet for å danne et beslutningsgrunnlag for implementering og utførelser oppgaver (Salas, Sims & Bruke, 2005, sitert i Njå et al., 2020, s. 203).

Samvirke krever *koordinering*, det vil si å få alle involverte aktører til å jobbe effektivt sammen og å utfylle hverandre for å nå målet om best mulig håndtering av hendelsen. Koordineringen foregår ved at to eller flere aktører samarbeider gjennom å samordne sine aktiviteter i tid og rom, slik at de kan oppnå et felles mål (Larsson, 2002; Uhr, 2011 sitert i Njå et al., 2020, s. 199) For å sikre deling av relevant informasjon kreves det kriseledere som effektivt kan samle inn informasjonen, og at den relevante informasjonen kan deles mellom aktørene. Gjennom informasjonsdeling gis aktørene mulighet til å handle med sine egen kunnskap og kompetanse, og skaper en felles situasjonsforståelse. En felles situasjonsforståelse er helt sentralt for å kunne forstå hvilke oppgaver som skal løses (Wolbergs & Boersma, 2013 sitert i Njå et al., 2020, s. 201).

4.4.3 Felles mental modell

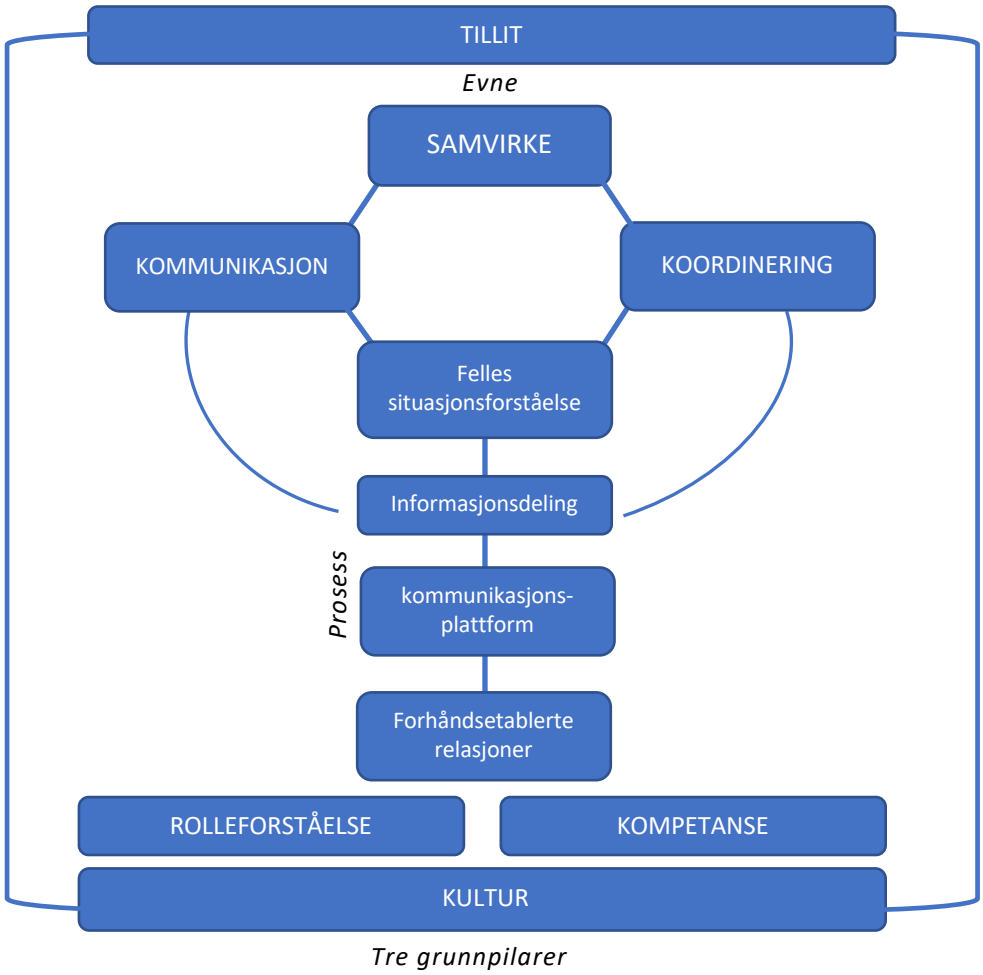
Felles mental modell handler om at aktørene utarbeider en felles situasjonsforståelse. Det er elementært at aktørene har en felles forståelse av situasjonen i beslutningsprosessen. En utfordring som kan hindre et godt samvirke er dersom aktørene ikke klarer å danne eller opprettholde en felles situasjonsforståelse (Eriksen, 2017, sitert i Njå et al., 2020, s. 202). Situasjonsforståelsen påvirker hvilke ressurser og tiltak som må settes inn for å lykkes. Situasjonsforståelsen hos lederne er dermed en kritisk faktor (Njå et al., 2020, s. 194). En felles mental modell beskrevet ovenfor kan knyttes til kriseresponsen. Lunde (2019) beskriver konseptet noe annerledes, der han forstår det som:

> ... en mekanisme der mennesker lager en beskrivelse av et systems hensikt og form, forklarer systemets fungering og tilstand, og benytter denne forklaringen til å forutsi fremtidige tilstander i systemet (Lunde, 2019, s. 158)

Ved en slik beskrivelse forstås modellen som forhåndsetablert. Dette klargjør hvilke forventinger som stilles til hvordan det dannes en situasjonsforståelse i en gitt krisesituasjon (Lunde, 2019, s. 158). Det vil si at dersom det allerede er etablert en felles mental modell om et gitt system vil en kanskje ha bedre grunnlag til å også skape en felles situasjonsforståelse. Det vil være nyttig å ha en slik felles mental modell for samhandling, beslutningstaking og for å vite hvilke avhengigheter funksjoner har til hverandre (Lunde, 2019, s. 158). Et praktisk eksempel på en felles mental modell er dersom en ser for seg et fotball-lag som spiller. Fotball-laget fører ulike pasninger til ulike spillere på banen. De ulike spillerne er bevisste på hvor ballen vil gå dersom ballen sendes videre til for eksempel kantspilleren. Dette vet spillerne fordi de på forhånd har etablert en enighet om taktikk og hvor ballen skal spilles. En slik mental prosess skaper et samhandlingsmønster som etter repetering ligger lagret i hukommelsen.

4.4.4 Samvirke-modellen

Basert på analysen av det teoretiske grunnlaget omkring samvirke har det blitt utarbeidet en forenklet modell som skal illustrerer forskerens egen forståelse av samvirke-konseptet. I figur 4 vises *samvirke* som en *evne* tilknyttet til *kommunikasjon* og *koordinering*. *Rolleforståelse*, *kompetanse* og *kultur* er tre grunnpilarer i modellen. En *felles situasjonsforståelse* fremmes gjennom en prosess som bygger på å ha *forhåndsetablerte relasjoner*, en felles *kommunikasjonsplattform* og *informasjonsdeling*. *Tillit* er plasser øverst fordi det gjerne er i samvirke tillit utvikles.



Figur 4: En modell basert på en sammensetning av det teoretiske grunnlaget av samvirke-konseptet.

Eksempel på modell av samvirke

For å forklare modellen har jeg tatt utgangspunkt i samvirke mellom nødetatene. Gjennom et *tillitsforhold* og *god kultur* evner nødetatene å *samvirke* under kritiske situasjoner. Tillitsforhold er noe som gjerne skapes i samvirke, og jeg har derfor valgt å plassere tillit over samvirke. Brann, politi og helse har ulike roller, men som gjennom klar *rolleforståelse og kompetanse* utfyller hverandre. Relasjonene mellom nødetat-aktørene er *forhåndsetablerte*, og samband brukes som *kommunikasjonsplattform* samt at det etableres IL-KO (Innsatslederenes kommandoplass) for nærhet og oversikt over skadestedet (Politidirektoratet, 2020, s. 154). Gjennom *informasjonsdeling* skapes en *felles situasjonsforståelse* for alle involverte aktører. *Kommunikasjon* og *koordinering* blir sentrale forutsetning for at *grunnpilarene* og *prosessen* kan utgjøre *evne* for et godt *samvirke*. Modellen kan både forstås under en konkret uønsket hendelse, men kan også forstås som en kontinuerlig prosess i et forebyggende perspektiv som for eksempel i arbeidet med cybersikkerhet.

4.5 Resiliens

Resiliens er et begrep som stadig har fått mer oppmerksomhet innenfor krisehåndtering og beredskapsarbeid. Opprinnelig stammer begrepet fra psykologien og økologien (Garmezy 1973; Holling, 1973 sitert i Kaufmann, 2013, s. 276), der resiliens betegnes som evnen til å takle belastninger og stress. Martin (2019) definerer resiliens som evnen til å forberede seg på, absorbere, reagere på, komme seg etter angrep og tilpasse seg nye forhold (Martin, 2019, s. 220). Videre gjør han et skille mellom aktiv og passiv resiliens. Aktiv resiliens handler om læring av motgang, imens passiv resiliens er evnen til å komme seg fra en hendelse og oppnå normalitet. I lys av at cyber-risiko i stor grad kan kjennetegnes som usikre og dynamiske vil det være umulig å stoppe ethvert angrep. Den iboende usikkerheten gjør det vanskelig å beskytte seg mot enhver mulig cyberhendelse. En bedre strategi kan dermed være å styrke den proaktive beskyttelsessikkerheten for å håndtere uventede forstyrrelse samtidig som systemets evne til å komme raskt tilbake til normalitet styrkes (Martin, 2019, s. 30).

4.5.1 Fem dimensjoner av cyber-resiliens

Dupont (2019) definerer fem dimensjoner av cyber-resiliens. Den *dynamiske* dimensjonen er at resiliens kan oppnås gjennom en kontinuerlig prosess som inkluderer aktiviteter før, under og etter krisen. Aktivitetene inkluderer forberedelse på å møte ulike risikoer, implementering av risikoreduserende tiltak og å dempe negativer virkninger av uønsket hendelser (Dupont, 2019, s. 6).

Den *nettverksbaserte* dimensjonen handler om at resiliens ikke kan fremmes isolert, men må fremmes gjennom nettverksbaserte koblinger. Det med bakgrunn i de gjensidige avhengige sosio-tekniske systemer som befinnes i komplekse nett. Et sterkt nettverk med interorganisatorisk koblinger kan aktiviseres på kort varsel for å gi ressurser og kompetanse i en krisesituasjon. Dette kan lette både kommunikasjon og koordinering (Dupont, 2019, s. 6).

Den *praktiserende* dimensjonen handler om at en grundig planleggingsinnsats kan øke kapasitet og styrke mellommenneskelige tillit og relasjonelle bånd. Kriser er ikke like, dermed er «planer» av liten betydning, men selve «planleggingen» er avgjørende. Improvisasjon, ferdigheter og fleksibilitet er avgjørende faktorer for å håndtere krisen (Dupont, 2019, s. 7).

Den *tilpasningsdyktige* dimensjonen handler om at fleksible organisasjoner raskt kan omfordele ressurser. Slike organisasjoner har utviklet en kultur som anerkjenner improvisasjon og delegert beslutningstaking som faktorer for å være bedre forberedt på å møte uventete farer. Videre kan fleksibilitet oppnås gjennom redundans og mangfold. I cybersikkerhet refereres redundans til «tilgjengeligheten av flere beskyttede tilfeller av kritiske ressurser (informasjon og tjenester)", mens mangfold defineres som "bruken av et heterogent sett med teknologier for å minimere virkningen av angrep og tvinge motstandere til å angripe flere forskjellige typer teknologier. Mangfold minimerer avhengigheten av en enkelt teknologi eller tjeneste hvis feil kan vise seg å være katastrofal for en hel organisasjon, mens redundans øker mengden ressurser som er tilgjengelig for å håndtere en feil ved å gi svingnings kapasitet (Dupont, 2019, s. 7).

Den siste dimensjonen omtales som en *kontroversiell* eller *omstridt* dimensjon av cyber-resiliens. Denne dreier seg om det som utfordringer knyttet til kost-nytte i en organisasjon. Selv om de fleste organisasjoner har overlevelsesevne som konsensusmål så er det en rekke faktorer som hindrer implementering av tiltak for å fremme resiliens. Det beskrives som en ytelses-orientert rasjonalitet som søker å øke produktiviteten, og dermed kreves det kompromisser mellom effektivitet og resiliens. Kostnad og innsatsen som kreves for å øke resiliens i en organisasjon kan anses for å være for høye eller rett og slett uforholdsmessige i forhold til risikoen. Mangel på en felles risikoforståelse blant ledere og medarbeidere kan føre til en undervurdering av sannsynlighet og alvorlighetsgrad av mulige uønskede hendelser. Som igjen påvirker intensiver til å forbedre beredskap og fremme resiliens (Dupont, 2019, s. 7).

5. Resultater og analyse av datainnsamling

I dette kapittelet presenteres resultater samlet inn våren 2022 fra dokumentstudier, intervjuer og observasjonsdata. Resultatene er kategorisert med tilhørende tema som skal besvare den øvrige problemstillingen. Empirien har til hensikt å besvare oppgavens problemstilling i lys av de teoretiske betraktningene fra kapittel 4.

> ***«På hvilken måte operasjonaliseres samvirke i planprosess og gjennomføring av beredskapsøvelsen Cyber22, og hvilken innsikt gir dette i samvirke som strategi for cyber-beredskap?»***

I Delkapittel 5.1 presenteres datamaterialet som beskriver samvirke og hvordan informantene tolker samvirke i sammenheng med Cyber22. Videre i delkapittel 5.2 sees samvirke i sammenheng med cybersikkerhet. Her vises det til utfordringer og kompleksiteten i cybertematikken. Delkapittel 5.3 gjengir datamaterialet knyttet til planleggingen og gjennomføringen av Cyber22. Her presenteres min tolkning av hvilke data som er relevant for å svare på forskningsspørsmålene og den øvrige problemstillingen. For at leseren skal kunne gjøre sin egen vurdering av den innsamlede empirien har jeg forsøkt å konkretisere hvilke data som er hentet fra dokumentstudier, intervju og observasjon.

5.1 Samvirke

I stortingsmelding (St.meld. nr. 22 (2007-2008)) sees det spesielt på samvirke og samordning – der regjeringen i perioden 2009-2012 ønsket å særlig legge vekt på samarbeid og samvirke for å sikre helhetlig og samordnet krisehåndtering på sentralt, regionalt og lokalt nivå (St.meld. nr. 22 (2007-2008), s. 9). Behovet for denne meldingen understrekes med at:

> Ingen sektor kan alene forebygge, redusere, hindre eller håndtere fremtidens samfunnssikkerhetsutfordringer. Regjeringen vil derfor tydeliggjøre betydningen av samvirke og samarbeid i møte med fremtidens risiko-, trussel- og sårbarhetsbilde ... (St.meld. nr. 22 (2007-2008), s. 9).

5.1.1 Innføringen av samvirkeprinsippet

I rapporten fra 22. juli-kommisjonen gjennomgås terrorangrepene som fant sted i regjeringskvartalet og på AUF-leiren på Utøya den 22.juli 2011. Bakgrunnen for utredningen var et behov for å besvare tre nøkkelspørsmål: hva skjedde, hvorfor skjedde det og hvordan kunne samfunnet la dette skje? Målet med undersøkelsen var derav å trekke lærdom ut av hendelsen (NOU 2012: 14, s. 13). Funnene fra rapporten tilsa at det ikke var én enkelt årsak

alene, men flere momenter som førte til svikt i håndteringen. I sin helhet oppsummeres følgende funn fra rapporten:

> Mangel på evne til å koordinere og samhandle, svakhet som gjelder informasjons- og kommunikasjonsteknologi, lav evne til å erkjenne risiko og ta lærdom fra øvelser, evnen til å bruke planer var for svak, ledelsens evne og vilje til å klargjøre ansvar, etablere mål og treffe tiltak for å oppnå resultater har vært utilstrekkelig (NOU 2012: 14, s. 16).

I en melding til Stortinget (Meld. St. 29, (2011-2012)) redegjør regjeringen for tiltak som skal bidra til å styrke arbeidet med samfunnssikkerhet og beredskap. I denne meldingen trekkes spesielt frem:

> ... store tverrsektorielle hendelser med gjensidig avhengigheter, inkludert IKT-sikkerhet ... En kompliserende faktor er at også flere infrastrukturer er koblet sammen på tvers av landegrenser, og at arbeidet med å sikre kritisk infrastruktur dermed har en grenseoverskridende faktor. Økende grad av kompleksitet i samfunnet og avhengigheter på tvers av sektorer innebærer også et stort behov for samarbeid på tvers av ansvarsområder, både når det gjelder det forebyggende beredskapsarbeidet og i krisehåndtering (Meld. St. 29, (2011-2012), s. 9).

Som et tiltak for å sikre god samhandling mellom aktører, innføres samvirkeprinsippet som et hovedprinsipp på lik linje med nærhet-, ansvar- og likhetsprinsippene i krisehåndtering og beredskapsarbeidet:

> Samvirkeprinsippet stiller krav til at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering (Meld. St. 29, (2011-2012), s. 39).

Utvalgte punkter fra rapporten gir en begrunnelse for hvorfor et fjerde prinsipp ble etablert:

> De øvrige prinsippene kommuniserte i for liten grad nødvendighet for et samvirke mellom ulike aktører samt behovet for å se totale ressurser i sammenheng. Erfaringer fra en rekke hendelser og øvelser har vist hvilken betydning samvirke har for hvordan en krise håndteres. I tillegg til at man i for liten grad har fremhevet kravet om samvirke mellom aktører (Meld. St. 29, (2011-2012), s. 39).

Innføringen av samvirke som prinsipp ville gi noen føringer i krisehåndtering og beredskapsarbeidet. Herunder omtales disse:

> ... gir krav til aktører både på sentralt, regionalt og lokalt nivå til å samordne sitt beredskapsarbeid med andre, og der prinsippet om samvirke må reflekteres i ulike virksomheters planverk herunder under rutiner og prosedyrer som ivaretar dette og virksomheter må vektlegge samvirkeøvelser med relevante aktører (Meld. St. 29, (2011-2012), s. 39).
>
> ... i tillegg vil man få et prinsipp som er gjennomgående uavhengig av hva slags kriser det er tale om, eller hvilket nivå de håndteres på (Meld. St. 29, (2011-2012), s. 39-40).

> ... et tydelig krav til at alle aktørene har et selvstendig ansvar for å sikre et best mulig samvirke. Dette understreker behovet for at alle virksomheter og nivåer har et aktivt og bevisst forhold til gjensidige avhengigheter og hvilke aktører det vil være nødvendig å samhandle med, både når det gjelder forebyggende arbeid og i beredskapssituasjoner (Meld. St. 29, (2011-2012), s. 40).

Både i dokumenter og intervjuer fremstår konseptet samvirke som noe udefinerbart. I offentlige dokumenter nevnes samvirke ofte i bruddstykker og bisetninger. Nøkkelinformantene har likevel en enstemmig oppfatning omkring begrepet samvirke. Først og fremst anerkjenner de samvirkebegrepet i stor grad slik det er definert i selve prinsippet. Samtidig påpeker de at det er rom for tolkning av hva et godt samvirke innebærer i praksis.

> «Da er jo det prinsippet litt opp til tolkning, for det sier jo at man i fredstid skal danne relasjoner som gjør at du lett skal kunne samvirke i en nødsituasjon…»

Nøkkelinformantene forklarte også at det ikke finnes et minstekrav til samvirke, men det er likevel et krav til at organisasjoner skal samvirke godt med berørte interessenter for å redusere konsekvensene av en hendelse. En nøkkelinformant trekker frem et de har fått større fokus på samvirke som følge av 22.juli-terroren. Dette fokuset har blant annet bidratt til at NB har jobbet i større grad med interessentanalyser, aktørkart og å møte folk i en tidlig fase.

5.1.2 Aspekter ved samvirke

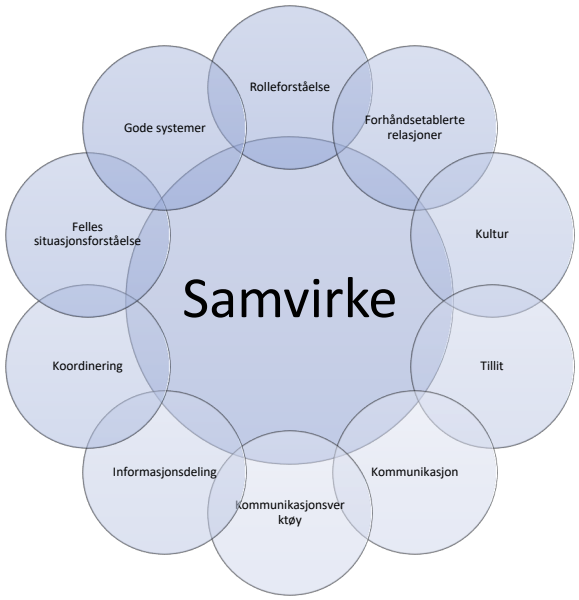
Det var flere aspekter med samvirke som kom frem i intervjuene. Det er likevel vurdert å ta med de aspektene som i større grad ble redegjort for. Til tross for at samvirke kan oppfattes som et nokså ubestemmelig konsept, har nøkkelinformantene det tydelig klart for seg hva som er viktig for å styrke samvirke i beredskap og krisehåndtering. Samtlige informanter påpeker at samvirke er komplekst og det dreier seg om noe mer enn et samarbeid.

> «Samvirke, handler om å få noe eller å få noen til å fungere sammen. Altså det skal virke sammen for å kunne utnytte en økt kapabilitet. Jeg tenker at det går utover det å samarbeide... så samvirke skal faktisk sikre en økt effekt. Det mer folkelige ordet på norsk som kan forstås på samme måte er samhandling.»

I en NOU gitt til forsvarsdepartementet (NOU 2016: 19) beskrives samhandling for sikkerhet.

> Nasjonen Norge er ikke sterkere enn det svakeste ledd, og reell samhandling for sikkerhet er den viktigste forutsetningen for å lykkes i å forbedre Norges sikkerhet – skritt for skritt. (NOU 2016: 19, s. 18).

Nøkkelinformantene peker på både menneskelige, teknologiske og organisatoriske faktorer som må legges til grunn for at samvirke skal fungere optimalt. I figur 5 vises en oversikt over funn som har betydning for et godt samvirke.



Figur 5: Oversikt over funn som har betydning for samvirke

Rolleforståelse og forhåndsetablerte relasjoner

Myndighetene poengterer et behov for samvirke i arbeidet med cybersikkerhet, samtidig må også ansvarsprinsippet legges til grunn for samarbeidet. Ansvarsprinsippet innebærer at virksomheter som har ansvar i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser.

> Dette forutsetter at roller og ansvar er avklart og at de relevante aktørene har god situasjons- og konsekvensforståelse. Det må være tilstrekkelig koordinering, samarbeid og deling av informasjon mellom sentrale aktører som har ansvar for å avdekke og håndtere alvorlige digitale angrep (Departementene, 2019, s. 19).

En forutsetning for god samhandling er når en fordeling av ansvar og myndigheter etter loven, legger til rette for samhandling mellom de sentrale aktørene innenfor forebyggende sikkerhet på tvers av samfunnssektorene. Utvalget ser på samhandling som noe helt avgjørende for det forbyggende sikkerhetsarbeidet i Norge. God samhandling oppnås først og fremst ved en balansert tilnærming til ansvarsprinsippet og samvirkeprinsippet (NOU 2016: 19, s. 19). Nøkkelinformantene trakk frem det å avklare samvirke som helt sentralt for å få til et godt samvirke.

> «... samvirke må være **avklart**, det vil si hvem er det man skal samvirke med og når.»

Ved å avklare samvirke kan en oppnå betydelig rolleforståelse og kompetanse om funksjoner, der samvirke- og ansvarsprinsippet balanseres. Når informantene peker på det å avklare samvirke handler det om å kjenne interessentene sine på forhånd. Denne prosessen illustreres i figur 6.

Figur 6: Prosess for å oppnå økt rolle- og funksjonsforståelse

Det er da viktig å kunne svare på følgende spørsmål: Hvem er det som er aktuelle å samvirke med, er kontaktinformasjonen og relasjon opprettet? Den ene informantene påpekte at den største trusselen mot akseptabel håndtering er ansvarsfraskrivelse. Informanten forklarte: «dersom alle skyver ansvaret bort fra seg, om det er organisasjonen eller imellom aktørene.» Dermed handler det om å tydeliggjøre hva som er mandatet til aktørene og funksjonsdelingen mellom aktørene. I en uønsket hendelse vil det være viktig å være klar over hvilket mandat de har, og at de på forhånd vet hvem som skal kontaktes. I et systemteoretisk perspektiv for å oppfylle målene rolleforståelse og kompetanse om egen funksjon, kreves det en sikkerhetsbegrensning som kan oversettes til krav. Krav kan være en sertifisering eller annen bestemt type opplæring som kan tjene en god funksjons- og rolleforståelse.

Kultur og tillit

I intervjuene ble også kultur nevnt som en avgjørende organisatorisk faktor for å styrke samvirke. Det var spesielt tre sider av kultur som ble uthevet: Åpenhet, sikkerhetskultur og psykologisk trygghet. Det nevnes i NOU: 2018: 14 at tillit og åpenhet er grunnleggende forutsetning for å få til samhandling:

> ... det er helt avgjørende at et IKT-sikkerhetssenter legger tillit og åpenhet til grunn for samhandlingen med andre ... Det krever betydelig samhandling med både offentlige og private aktører, og nettopp åpenhet og tillit fremheves av sentrene i Nederland og Storbritannia som viktige faktorer for å oppnå dette ... (NOU 2018: 14, s. 84).

Åpenhetskultur beskrives av nøkkelinformantene som det å ufarliggjøre samvirke ved å bygge nettverk og ved å dele erfaringer og kunnskap. Å ufarliggjøre samvirke handler om å la folk bli kjent med hverandre. En av informantene viser til et eksempel, der innsatsledere opplevde samvirke som betydelig bedret etter at de hadde møttes flere ganger over kaffekoppen. En annen informant påpeker at det handler om å by på seg selv når en treffes på tvers av virksomheter.

> «... prater man med hverandre og deler informasjon så er det lettere å samvirke ...»

Informanten fortalte at det er mye informasjon som kan deles som ikke er underlagt sikkerhetsloven. Samtidig kan en streng sikkerhetskultur føre til at informasjon holdes tilbake. Dette kan være en hemsko for sikkerheten. Det er også ulik kultur i de forskjellige miljøene, der en kan oppleve å få lite tilgang på informasjon fordi vedkommende ikke er i akkurat *det* miljøet.

> «... fordi man ikke er en del av det nettverket, du er ikke på innsiden av organisasjonene. Du er ikke godkjent, autorisert, du får ikke tilgang ...»

En annen informant viser til teorien om psykologisk trygghet som en ramme for hvordan et godt samvirke skal oppnås. Psykologisk trygghet defineres av Edmondson som:

> a shared belief that the team is safe for interpersonal risk taking (Edmondson, 1999, s. 354).

Teorien om psykologisk trygghet intensiverer en læringsatferd innad i et team eller en organisasjon ved at medlemmene våger å søke tilbakemelding, dele informasjon, spørre om hjelp, snakke om utfordringer og tester nye idéer (Edmondson, 1999, s. 371). Et godt samarbeidsklima er preget av tillit og åpenhet, der det er trygt å ta mellommenneskelige risikoer uten bekymringer for konsekvenser (Edmondson, 2004; 2005; 2012 sitert i Sagabraaten, 2019, s. 2).

Kommunikasjon

Nøkkelinformantene trekker frem kommunikasjon som helt sentralt for å kunne samvirke. I kommunikasjon handler det også om noe mer enn det å kommunisere i seg selv.

> «Det handler om kunnskap om de man kommunisere med, hvem som trenger informasjon fra meg og hvem jeg kan trenge informasjon fra.»

Likeledes er det noen praktiske elementer som må være tilstede. I intervjuene nevnte samtlige informanter at det var viktig å ha oppdaterte varslingslister og kommunikasjonslinjer, disse må også være testet slik at man vet at de fungerer. Det er de tingene som må være på plass i en førkrisefase.

> «Det nytter ikke å ha tenkt på at du skulle snakket med noen, også kommer krisen også skal du snakke med noen, og da har du ikke telefonnummeret til den kontakten en gang ...»

Målet er at det skal være tilgjengelige kommunikasjonslinjer og oppdaterte varslingslister for å nå det overordnede målet om å muliggjøre kommunikasjon. Dette målet omsettes i systemtenkning (Leveson, 2011) til *begrensninger*. Det blir et krav om å måtte oppdatere varslingslister og teste kommunikasjonslinjer slik som informanten forklarte. En

sikkerhetsbegrensning kan være dersom sikkerhetsloven ikke tillater bruken av et kommunikasjonsverktøy på bakgrunn av konfidensialitet. Dette fører til at det må etableres andre kommunikasjonslinjer som tillater en sikker kommunikasjon.

Kommunikasjonsbegrensninger er et tema under intervjuene, da dette kan være en utfordring ved tilsiktede situasjoner der virksomheten er underlagt sikkerhetsloven. Dersom sensitiv informasjon skal kommuniseres så kreves det bruk av spesielle rom eller spesielle kommunikasjonssystemer. En lignende problemstilling er kjent fra Gjørv-kommisjonens utredning. Kommisjonen peker på mangelen på et godt skriftlig informasjonsdelingssystem som en betydelig faktor for hvorfor situasjonen ble slik den ble (NOU 2012: 14, s. 109). I øvelsen Digital 2020 var en av hovedkonklusjonen utfordringer med informasjonsdeling over den digitale flaten når aktørene er underlagt sikkerhetsloven.

> «Det var vanskelig med samvirke digitalt, fordi informasjon som er underlagt sikkerhetsloven, er vanskelig å ta på teams.»

I tilfeller der ordinære kommunikasjonsverktøy ikke lar seg bruke, bør det være en kontrollfunksjon som setter krav om alternative kommunikasjonsprosedyrer. Intervjuene indikerer at informantene er bevisst på for å nå målene om kommunikasjon må kravene gjennom sikkerhetsbegrensningene overholdes. Hvordan og hva som kommuniseres under en cyberhendelse har også stor betydning for samvirke og for en felles situasjonsforståelse. En informant forklarte i denne sammenheng at:

> «De taktiske, altså operatørene som sitter med it-systemene, problemet med dem er at de snakker sitt språk som andre ikke forstår. Så du må ha noen som omsetter IT-terminologi til språket til direktører og lederen, topplederne. Det er noe som vi ser ofte, for det blir så kryptisk ikke sant, og de skjønner egentlig ikke hva dem sier.»

En annen informant forklarte at det ikke nødvendigvis er så viktig hva «det» kalles, så lenge det er enighet i hva det er snakk «om». I tillegg påpeker informanten at det er minst en person i kriseledelsen som har et IKT-perspektiv, og som da kan det tekniske aspektet. Informantene forklarer at fagkunnskap på cyber må trekkes inn i kriseledelsen. Hvis ikke kriseledelsen har kompetanse på cyber vil problemstillingene være vanskelige å forstå. Målet i dette tilfellet er å sikre kommunikasjon for å dermed oppnå en felles situasjonsforståelse mellom ledelsen og operatørene som sitter med IKT-systemene. Tilbakemeldinger fra ledelsen om at informasjon fra operatørene kan oppfattes som kryptisk fører til at kontrollfunksjonen tillegger sikkerhetsbegrensing i form av krav om IKT-kompetanse i kriseledelsen.

Informasjonsdeling og felles situasjonsforståelse

Ifølge Gjørv-kommisjonen gir informasjonsdeling både bedre oversikt, økt koordinering og bedre kunnskapsgrunnlag når beslutninger skal tas (NOU 2012: 14, s. 109). I en utredning (NOU 2015: 13) beskrives utfordringer og dilemmaet mellom samhandling og informasjonsdeling. En manglende informasjonsdeling kan føre til en svekket felles og oppdatert situasjonsforståelse.

> Et effektivt samarbeid på tvers av organisasjoner krever at tekniske systemer kan kommunisere og utveksle informasjon, og at de samarbeidende organisasjonene kan samvirke ved å bruke utstyret. I mange tilfeller er disse organisasjonene teknisk heterogene og har ulik kommunikasjonskultur og organisasjonsstruktur. Dette utfordrer samvirke og samarbeid i praktiske krisesituasjoner (NOU 2015: 13, s. 244).

Fra et sikkerhetsperspektiv har en regulert informasjonsdeling en svært nødvendig funksjon. Det har til hensikt å beskytte sårbarheter i organisasjoner og virksomheter. Dette kan også omsettes i systemteorien til en sikkerhetsbegrensning:

> Selv om samhandling og informasjonsdeling er nyttig og nødvendig, har utstrakt deling av informasjon også en skyggeside. At flere gis tilgang til informasjon, og at systemer kobles sammen, gir økt sårbarhet. Det blir derfor viktig også å gjøre en verdivurdering av informasjon og kartlegge behovet for beskyttelse av sensitiv informasjon gjennom tilgangskontroll og kryptering (NOU 2015: 13, s. 244).

God sikkerhetskultur dreier seg om noe mer enn å beskytte informasjon. En av informantene trekker frem ledelsesaspektet som sentralt for å fremme god sikkerhetskultur. «Ledere som evner å lytte til sine rådgivere, evne til å prioritere og å ta gode beslutninger.» I dette ligger det en innstilling til hva som er akseptabel håndtering og risikonivå. Kompetanse på ledelsesnivå er sentralt der en informant påpeker at det handler om:

> «... kompetanse og kjennskap til hvordan man skal lede under en cyberhendelse.»

Informanten trekker her inn stikkord som åpenhet og transparens for å få til en god sikkerhetskultur mellom ledelsen og personalet i organisasjonen. Informanten understreker at det ikke betyr at man skal være helt åpen og si: «dette er våre svakheter» til andre aktører.

> «Det handler om en forståelse for aktørene man samarbeider med, være åpen i fredstids også når det gjelder kommunikasjon i koordinering.»

En av nøkkelinformantene fortalte om et rapporteringsansvar som de har til en sentral aktør. Informanten påpeker at de har stor glede av å ha et godt samvirke i lang tid før treninger

> «... det er enklere å varsle og informere, og man vet også bedre nå hva de forventer i rapporteringen, enn det vi gjorde før. Vi har blitt bedre på kunnskapsdelingen.»

Dette tyder på at kontrolløren som kan være tilsynsmyndigheter eller sikkerhetsmyndigheter har gjennom sine sikkerhetsbegrensninger gitt tydelig krav i prosedyrer til NB for hvordan det skal varsles, hvem som skal varsles og hva rapporten skal inneholde. Det kan tolkes ut ifra utsagnet at det tidligere ikke har vært like tydelig på hva som skal deles, og nye sikkerhetsbegrensninger er dermed iverksatt for å ivareta informasjonsdeling og rapportering.

Koordinering og gode systemer

Koordinering er et nøkkelord som går igjen under flere spørsmål i intervjuene om temaene samvirke og krisehåndtering. Koordinering og tydelig kommunikasjon tilsammen legger et grunnlag for et felles bilde av situasjonen (Comfort, 2007, s. 191). Den ene informanten forklarte at det trengs en tilnærming som krever økt koordinering, fordi trusler i cyber krever en helt ny dimensjon av koordinering i forhold til andre trusler de har jobbet med tidligere. Det krever at alle har et felles og effektivt rammeverk, en fleksibilitet i tilnærmingen, en kjent metodikk og en god ledelse. I tillegg er det viktig å ha koordinert internt, hvem det skal samvirkes med eksternt. For operatørene som overvåker IKT-systemene er en god struktur og godt rammeverk en forutsetning

> «... også ha en god systematikk for hvordan man løfter det og varsler videre inn i virksomheten er jo veldig viktig. For det vi ser at de som ikke har etablert den siste delen av det, sitter gjerne og håndterer feilene selv, altså IT-folkene.»

Operatørene som ser på loggene og skjermene ser hva som skjer og hva som har skjedd. I et finanssystem kreves det at slike hendelser løftes opp, med hensyn til forretningsimplikasjonene, slik at flere kan se på den totale risikoen. En beredskapsorganisasjon kan settes på som en koordinerende muskel for å håndtere en hendelse. Når lederne har økonomi og administrativ bakgrunn er det ledelsesperspektivet og kulturen som er viktig i en slik hendelse. Det er som en annen informant sa: «det handler om å skape et fellesskap for å håndtere det.» En koordinerende funksjon blir da satt inn som et krav for å ivareta ressursallokering og kommunikasjon mellom hierarkinivåene i systemet.

5.2 Betydningen av samvirke i arbeidet med cybersikkerhet

I Nasjonal strategi for digital sikkerhet påpekes det at god digital sikkerhet ikke er en målsetting myndighetene kan nå alene (Departementene, 2019, s. 9). I strategien vektlegges et krav om samhandling og partnerskap mellom relevante aktører. Videre sies det at utfordringer skal løses i fellesskap, slik at interessenters sikkerhetsbehov blir ivaretatt (Departementene, 2019, s. 6). Figur 7 viser en oversikt over relevante funn som presenteres i *dette* delkapittelet.

Figur 7: Oversikt over funn i delkapittel 5.2

5.2.1 Forebyggende risikobasert arbeid

Et forebyggende risikobasert arbeid vektlegges for å forhindre uønskede digitale hendelser (Departementene, 2019, s. 13). Ulike kompetanser, kunnskaper og kapasiteter i offentlige og private virksomheter kan utfylle hverandre.

> Digitale sårbarheter krever at aktører arbeider tettere sammen, dette innebærer å øve på håndtering av krisesituasjoner, felles kompetanseheving, gjensidig hendelsesvarsling og å dele informasjon om trusler og sårbarheter (Departementene, 2019, s. 9).

Det er tydelig enighet blant nøkkelinformantene at det forebyggende risikobaserte arbeidet står helt sentralt i arbeidet med cyber og samvirke. Hvor det i grunn handler om et økt samarbeid i et forebyggende perspektiv. Nøkkelinformantene forklarte at de jobber risikobasert og målbasert med cybertematikken for å kunne kartlegge et risikobilde.

> «... hva som kan ramme Norges bank og hva er det som har rammet oss. Også ser vi på de risikoene, og jobber med de sårbarhetene og truslene som vi ser kan ramme oss ...»

Utsagn fra intervju samt offentlige dokumenter antyder at NB er en sterk sikkerhetsorganisasjon. Det vil si at de følger gitte krav fra øvrige nivåer i den hierarkiske kontrollstrukturen. Myndighetene vil på et høyere nivå kunne stille krav til sikkerhetsstyring nedover i systemet ved hjelp av for eksempel veiledere. Som nevnt i delkapittel 5.1 inngår også arbeidet med relasjoner, kartlegging av ansvarsområder, aktørnettverk og informasjonsutveksling. Dette er arbeid som må jobbes med kontinuerlig i en tidlig fase.

> «Jeg tenker at de som ikke har jobbet godt i førfasen, vil ha veldig mye å ta tak i med tanke på god risikostyring for etterlevelse. Det å være forberedt.»

I Nasjonal strategi for digital sikkerhet hevdes det at økt samarbeid gir en bedre situasjonsforståelse, bedre beslutninger og økt tilgang på ressurser (Departementene, 2019, s. 9). Departementene peker på en intensivering og videreutvikling av samarbeidet for å kunne møte sikkerhetsutfordringer som stadig er i endring. Det påpekes også at næringslivets rolle står helt sentralt når det kommer til ivaretakelse av digital sikkerhet, med sine kompetanser og ressurser er næringslivet en driver for digitalisering og innovasjon. Videre må alle aktører se utover seg selv for å ivareta digital sikkerhet (Departementene, 2019, s. 9). Samtidig som samarbeid mellom virksomheter er viktig for å utnytte kompetanse og ressurser, innebærer det også en risiko for at helhetlig sikring ikke blir godt nok ivaretatt. Kombinasjonen av fravær av risikostyring og gode nok avtaler mellom virksomheter er kontaktflateutfordringer for virksomhetene og den øvrige nasjonale sikkerheten (NSM, 2022, s. 23)

Dialog mellom myndighetene og aktører i finanssektoren skal legge til rette for samarbeid om strukturelle løsninger, sikre finansielle tjenester som samfunnskritisk funksjon og håndtering av ekstraordinærere situasjoner (Meld. St. 31, (2020-2021), s. 10). I en NOU gitt til Justis- og beredskapsdepartementet i 2018 pekes det på et behov om å utarbeide ny lov for IKT-sikkerhet til alle samfunnskritiske virksomheter og offentlig forvaltning. Også her beskrives behovet for ytterlig samhandling innenfor cyberdomenet.

> ... virksomheter er avhengige av lange og komplekse digitale verdikjeder. I prinsippet kan alle IKT-systemer bli benyttet som mellomledd i angrep mot andre egentlige mål (NOU 2018: 14).

I denne utredningen vises det til ulike faktorer som er viktig for å fremme god samhandling ved IKT-sikkerhet. Deriblant nevnes samordningsarenaer. Samarbeid på slike arenaer omfatter alt fra langsiktig kompetansebygging til informasjonsutveksling knyttet til konkrete saker (NOU 2018: 14, s. 30). IMF (Det internasjonale valutafondet) gjennomførte en omfattende vurdering av det norske finansielle systemet i 2020. Følgende vises det til en vurdering og anbefaling som er relevant i en cyber-kontekst:

> Norges arbeid med cyberrisiko karakteriseres som avansert, og IMF fremhever at systemet for informasjonsdeling mellom myndighetene er godt etablert på dette feltet. Rapporteringen av cyberhendelser bør likevel styrkes ved å etablere klarere terskel-verdier for rapportering og tydeligere spesifisering av hva som skal rapporteres (Meld. St. 31, (2020-2021), s. 25).

5.2.2 Hendelseshåndtering

I intervjuene var terminologien *krise* et tema, blant nøkkelinformantene var det en samsvarende forståelse av krisebegrepet. Krise sier noe om alvorlighetsgraden av en hendelse og det tvinger virksomheten til å sette en krisestab. Det utløser noen myndigheter og roller som organisasjonen nødvendigvis ikke har i det daglige.

> «... du får ansvarsforholdet opp på et visst nivå, som understreker at dette er en situasjon, en krise, som potensielt kan bli noe ganske stort. Det er sånn vi tenker om risiko også, vi tenker potensialtenking.»

Den ene informanten påpeker også at det å måtte definere en hendelse som en krise kan være en barriere for en god håndtering.

> «... det må være en krise for at vi skal gjøre noe. Hva om det er en alvorlig situasjon, hvis noen truer deg, men ingen har sagt at det er en krise. Skal man ikke håndtere det?»

Informanten understreker at uavhengig om termen krise brukes, handler det om å bruke samme tilnærming for mindre alvorlige situasjoner ved å sikre tilpassede kapabiliteter.

Deteksjon som en beredskapsfase

En av informantene forklarte at det er nødvendig med gode systemer for varsling om cyberhendelser. Nettopp fordi cyberhendelser forekommer hele tiden, og derfor er det nødvendig med en god systematikk for varsling. Varsling og gode rapporteringssystemer er helt essensielt, og informanten forklarer at det er veldig mange virksomheter som sliter akkurat med dette.

> «... men man begynner å ta innover seg den IT-kontinuitetsfasen som er deteksjon. Du bør ha med deteksjon som en egen fase i beredskapen for å kunne jobbe godt med cyberrisikoen. Den største utfordringen ligger gjerne her. Det er åpenbart når alle skjermene blir svarte, men hva med når man har indikatorer på at noe er i ferd med å skje.»

Som påpekt ovenfor er gode systemer og rammer nødvendig, og da spesielt gode deteksjonssystemer for ulike alarmsett. Det er som informanten sier, en del av en IT-kontinuitetsfase. Rammer for hvordan de ulike deteksjonene blir håndtert begrenses fra nivået over til nivået under i systemmodellen. Rapportene for deteksjon vil fungere som en tilbakemelding til nivået over.

Proaktiv metode

I NB følges metoden «proaktiv metode». Når det erklæres en krise av kriseleder utløses roller og mandater. Rollen koordinator er innført for å støtte kriseleder i gjennomføring av krisemøtene, og for å holde struktur og følge proaktiv metode.

> «... Så når noe skjer for eksempel innenfor cyberdomenet i Norges Bank så vil det gjennomføres en grovvurdering. Da vil de som sitter med problemet, de som sitter med risikoen sammen med en koordinator gjennomfører den første vurderingen... Hvordan kan det her ramme noen andre i banken? Hvordan kan det her ramme noen andre utenfor vår virksomhet? Hvordan kan det her ramme våre oppgaver? En grovvurdering av potensialet. ... Hvis cyberdomenet rammer HR, at det er persondata som er ute av drift eller eksponert, eller om det er noe av det konfidensielle at det er oppgjørssystemet.»

Videre forklarte informanten at man så setter inn umiddelbare tiltak og varsler strategisk nivå, for deretter å mobilisere en operasjonellkrisestab ved behov. Når dette foregår jobbes det med samhandling parallelt. De taktiske nivåene er allerede i gang med hendelseshåndteringen uavhengig om hendelsen er definert som en krise eller ikke. Deretter tar kriseleder med seg koordinator og loggfører inn på et møterom eller digitalmøteflate. Innkalling gjennomføres av GSOC (Global Security Operation Centre) i krisehåndteringsverktøyet NBCIM (Norges Bank Crisis Information Management).

> «... Når det er gjennomført møtes man, gjennomfører et første møte med tiltak, også er det en aksjonsfase også kommer det nye statusmøter frem til det er håndtert også remobiliseres det.»

Nøkkelinformanten forklarer at de har det som kalles en fleksibel krisestab, det vil si at de kan trekke inn fagressurser der det trengs. Fleksibilitet anses som en viktig forutsetning i hendelseshåndtering. Fleksibilitet med tanke på omfordeling av ressurser og delegert beslutningstaking er faktorer som faller *under den tilpasningsdyktige dimensjonen* for å styrke cyber-resiliens. En slik styringstilnærming peker også i retning av en desentralisert «bottom-up» tilnærming i håndteringen. Hvor det jobbes oppover i systemet, imens ressurser trekkes nedover i systemet der det trengs. Dynes (1993) hevder at denne styringstilnærmingen ivaretar sosial kontinuitet, koordinering og samarbeid.

Koordinator-rollen er en slik rolle som styrker opp under en slik tilnærming. Informanten trakk frem at det ikke nødvendigvis er så mange virksomheter som har en slik rolle. Det vil si de gjerne bare har en operasjonellkriseleder som har resten av staben med seg.

> «... men vi har valgt å legge til en sånn kombinerende funksjon, fordi vi har gode erfaringer med det fra andre steder... Forsvaret for eksempel der har du en som er sjef og han har alltid med seg en stabssjef eller en NK. Den personen har ansvaret for å sørge

> for at det er tilrettelagt slik at sjefen kan ta gode beslutninger. Det er det som er tanken bak koordinatorrollen som Norges Bank har.»

Ifølge informanten er det nettopp den proaktive stabsmetodikken som ivaretar håndteringen av en hendelse. Dette gjøres ved at det er etablert en forhåndsdefinert metode for hvordan en skal håndtere beredskapssituasjoner. Ved å skape forutsigbarhet og trygghet i samarbeidet forskånes beredskapsledelsen for bruk av unødvendig kapasitet. Dette kan gi økt stresstoleranse, ettersom man vil da kunne bruke kapasiteten til å håndtere selve beredskapssituasjonen (Lunde, 2019). Metoden bygger på en systemtenkning som Leveson også fremlegger i sin teori, der en hendelse kontinuerlig kontrolleres og styres gjennom iverksettelse av beslutninger, tilbakemelding og kontroll. Det blir på samme måte en tilbakemeldingssløyfe som gjør at aktøren kan sette inn nye sikkerhetsbegrensninger ettersom hendelsen utvikles. Det blir en kontinuerlig prosess i en bevegelse frem og tilbake til det samme punktet i prosessen. Med bakgrunn i at et cyberangrep kan treffe en og flere virksomheter bredt, blir samvirke og den tradisjonelle tredelingen enda mer relevant.

En informant forklarte at det er usikkerhet knyttet til om en hendelse bare treffer oss eller om den treffer andre. Eksempelvis i en stor privat bank eller et kraftkonsern, hvor det er en konsernledelse og mange selskaper under seg som selvstendige enheter.

> «... Det er hensiktsmessig å ha en tredeling, altså taktisk nivå dem som jobber med selve hendelsen. I cyber er det ikke noe redde liv og miljø, det er gjerne konsekvensene for selskapet, virksomheten altså driften... Også har du det operasjonelle nivået, der koordineringsnivået er som en "informasjonshub" som sikrer at alt sammen skjer. De har en dialog, et utvalg av folk og utstyr som gjør at du kan ha det bildet, koordinere og får tatt beslutninger på riktig nivå. Du har gode tiltak som gjør at du få redusert konsekvensene. For det er jo bare tiltakene som reduserer konsekvensene, så der koordineres alt.»

Hierarkiet i kriseresponsen er med på å sikre informasjonsutveksling og dermed en felles situasjonsforståelse fra taktisk nivå til strategisk nivå. Som informanten forklarte så er tredelingen i kriseresponsen særlig viktig. Taktisk nivå jobber med problemet, og strategisk nivå må oppnå den samme situasjonsforståelsen for å kunne ta gode beslutninger.

5.2.3 Gjensidige avhengigheter i den finansielle infrastrukturen

Finansmarkedsmelding publiseres hvert år av regjeringen, en melding om finansmarkedene som tar for seg ulike aspekter som utsiktene for finansiellstabilitet, endringer og reguleringer i finansmarkedet, digitalisering, kapitaltilgang og mer (Meld. St. 31, (2020-2021), s. 7). Innledningsvis beskrives den digitale sårbarheten i den finansielle infrastrukturen som:

> ... betalingssystemene og andre systemer som er nødvendige for at økonomiske transaksjoner skal kunne gjennomføres. Den finansielle infrastrukturen i Norge er i hovedsak robust. Driften har også etter utbruddet av koronaviruset vært stabil, og tjenestene ut til kundene har fungert som normalt, selv om mye av driften det siste året har skjedd fra hjemmekontor. Det har til nå ikke vært sikkerhetshendelser i det norske finansmarkedet med konsekvenser for den finansielle stabiliteten (Meld. St. 31, (2020-2021), s. 8).

I sårbarhetssammenheng med vekt på den finansielle infrastrukturen (betalingssystemene og andre systemer for økonomisk transaksjoner) har finansdepartementet i 2019 gjort en tilstandsvurdering av dette. Hovedfunnene fra tilstandsvurderingen var at den finansielle infrastrukturen i Norge i all hovedsak er robust. Denne vurderingen var i samsvar med analyser fra NB og Finanstilsynet i deres årlige rapporter om den finansielle infrastrukturen (Meld. St. 31, (2020-2021), s. 14-15).

Selv om infrastrukturen beskrives som robust er finansielle tjenester pekt ut som en kritisk samfunnsfunksjon av regjeringen som blant annet innebærer at infrastrukturen er avhengig av digitale løsninger. Dette fører til en årvåkenhet angående sårbarheter, sikkerhet og beredskap i den finansielle infrastrukturen. Økte avhengigheter i IKT-systemer fører med seg både fordeler og ulemper, der fordelen innebærer en effektivisering og bedre tjenestetilbud:

> ... en kritisk samfunnsfunksjon som er avhengig av digitale løsninger. Det krever særlig oppmerksomhet om sårbarheter, sikkerhet og beredskap. Økt digitalisering av finansielle tjenester og infrastruktur bidrar til effektivisering og et bredere tjenestetilbud ... (Meld. St. 31, (2020-2021), s. 14-15).

Virksomheter er knyttet sammen i lange og komplekse verdikjeder. NSM peker på investering som en del av virkemidlene for å kartlegge sårbarheter. Uoversiktlige verdikjeder gjør det dermed vanskelig å beskytte viktige nasjonale verdier (NSM, 2022, s. 8). Et tiltak som må gjøres er å kartlegge verdikjedene og øke sikkerhetsstyringen av leverandører og underleverandører (NSM, 2022, s. 9). NB er i første posisjon på logiske systemer som er utsatt for tilsiktet cyberangrep. Samtidig kan også underleverandører være utsatt for sabotasje eller inntrengere. En informant forklarte at fokuset på leverandørsikkerhet og leverandørkunnskap i fredstid er viktig.

IKT-systemenes utfordringer krever ekstra fokus med tanke på sårbarhet, sikkerhet og beredskap. Hvor sårbarheten ligger i den økte avhengigheten i komplekse IKT-tjenester i sektoren samt en mer kompleks utkontraktering med flere leverandører.

> ... økt avhengighet av IKT-tjenester gjør også tjenestene og foretakene mer utsatt for operasjonell svikt og cyberangrep. Systemsvikt i større finansforetak eller sentrale infrastrukturforetak kan få store økonomiske konsekvenser og i ytterste konsekvens true den finansielle stabiliteten (Meld. St. 31, (2020-2021), s. 14-15).

En informant forklarte at finansiell infrastruktur og betalingssystemet er sterkt sammenkoblet. Derfor har NB fokus på systemrisikoen, hvordan avbrudd i betalingssystemet kan få effekt utover den ene enheten eller virksomheten, og hvilke samfunnsøkonomiske konsekvenser det kan innebære.

> «... Derfor kan det ikke håndteres alene og kan bare håndteres gjennom god samhandling.»

Det som er nevnt i avsnitt 5.1.2 viktig med å ha om kunnskap om hvem en skal samvirke med, og hvilken rolle- og funksjonsforståelse som er etablert. Hva verdikjeden består av, og hvem som er interessentene er ting som må være avklart.

> «Det er ting som må være avklart før noe skjer. Så hvis det skjer en cyberhendelse så må jeg ha telefonnummer til de jeg trenger å snakke med. Jeg må vite hva slags oppgaver og roller de har i det daglige, og hvilke oppgaver når det er en krise. Hva slags myndighet de har, Hva slags myndighet jeg har ... Kan du skru av det systemet der? Du er en underleverandør av meg. Kan jeg skru av det eller kan du gjøre det? Kan jeg fysisk gjøre det, kan du nekte meg å gjøre det? Hvem eier systemet? Hvem leverer det? Hvor sitter serveren? Kunnskap er en viktig faktor.»

En systemforståelse var flere av informantene inne på ved spørsmål omkring samvirke under cyberhendelser. Det kan tolkes som at en overordnet forståelse av systemet er viktig i cyber-domenet der det er flere gjensidige avhengigheter. Et annet aspekt ved den gjensidige avhengigheten er at deler av IKT-driften i finanssektoren er flyttet ut av Norge. NB har pekt på at det er vanskelig for den enkelte systemeier å håndtere konsentrasjons- og systemrisikoen knyttet til IKT-leverandører. De har dermed foreslått for Justis- og beredskapsdepartementet at det bør utredes nærmere hvordan sentrale IKT-leverandører og datasentre best kan underligge tilsyn. Utflyttingen fra Norge må skje på en forsvarlig måte, som ivaretar banker og finanssystemet som helhet. Finanstilsynet legger vekt på oppfølging av at bankene skal gjøre grundige risikoanalyser og vurdere ny eller endret utkontraktering, og der tilsynet kan iverksette tiltak overfor uforsvarlig utkontraktering (Meld. St. 31, (2020-2021), s. 39). En konsekvens av utkontrakteringen kan være en svekket intern kompetanse i norske finansvirksomheter:

> Selv om det er klare rammer i regelverket for hva slags oppgaver som kan utkontrakteres, er det en fare for at bankenes egen IKT-kompetanse svekkes, og at den norske finansnæringen ikke vil få dekket sitt fremtidige kompetansebehov innen kritiske områder (Meld. St. 31, (2020-2021), s. 39).

5.2.4 Kompleksiteten i cybertrusselen

Finanssektoren er en av de sektorene som har lengst erfaring med sikkerhet og risikostyring, der arbeidet med risiko er implementert i alle faser av operasjoner og i alle ledd i organisasjonen (NSM, 2022, s. 29). Angrepene mot den finansielle infrastrukturen i Norge øker imidlertid fra år til år, og finansforetakene må forholde seg til et trusselbilde i kontinuerlig endring (Meld. St. 31, (2020-2021), s. 39). Det er også et taktskifte i cyberaktivitet mot Norge, fra 2019 til 2022 viser NSM til en tredobling i antall alvorlige hendelser og cyberoperasjoner (NSM, 2022, s. 9). Risiko knyttet til IKT i finanssektoren beskrives som kompleks – ved at den stadig er i endring, dens økning og dens gjensidige avhengigheter i systemer.

> ... høy endringstakt, mer kompliserte systemer og stadig lengre verdikjeder kan øke risikoen... I tillegg innebærer digitalisering og økt avhengighet av IKT i finanssektoren nye risikoer ... (Meld. St. 31, (2020-2021), s. 39).

I rapporten Risiko 2022 trekkes kompleksiteten frem ved beskyttelsen mot alvorlige trusler. Det eksemplifiseres med det alvorlige cyberangrepet som rammet Stortinget i mars 2021. Kompleksiteten beskrives med bakgrunn i en rekke sammensatte hendelser som rammer ulike sikkerhetsområder. Blant annet strategiske investeringer som gir fremmede stater tilgang til viktige verdier, vårt høyteknologiske samfunn som er svært sårbart og koronapandemien som utfordret Norges sikkerhet ved at mennesker ble plassert på hjemmekontor. Dette er bare noen få eksempler på kompleksiteten i sikkerhetsarbeidet (NSM, 2022, s. 6). Kompleksiteten i cybertrusselen er et gjennomgående tema i alle intervjuene. Cyber-risiko er sammensatt, det vil si at det er flere faktorer som spiller inn samtidig finnes det ikke en enkel løsning på utfordringene.

Usikkerhet i beslutningsgrunnlaget

Informantene peker på flere faktorer som utfordrer cyber generelt og samvirke i arbeidet med cybersikkerhet. Usikkerhet og det ukjente knyttet til cybertrusler utfordrer flere faktorer. Blant annet nevner en informant at det utfordrer kunnskapen.

> «Det utfordrer jo en del av de faktorene ... kunnskap om kompetanse, forståelse for og trygghet i.»

En annen informant illustrerer kompleksiteten som en snøball som bare blir større og større, før den helt til slutt ruller over deg. Ved at det er ukjent kreves det at beslutninger må tas på et usikkert grunnlag. En annen informant forklarte at man kjenner gjerne ikke mekanismene bak

et angrep. Fra et ledelsesperspektiv handler det om å ta beslutninger på et i usikkert grunnlag i et domene som man kanskje vet lite om i utgangspunktet. En annen utfordring knyttet til beslutninger i cyberangrep, er hvem som skal ta beslutningene.

> «... det er ikke alt man får lov til å gjøre selv, en del ting slik som cyberrisikoen kan medføre store utfordringer for en virksomhet, og da er det typisk mandatene som ligger på toppnivå altså strategisk for beslutningstaking som påvirker likhetsprinsipp mellom dagligdrift. Hva gjør de vanligvis og hva beslutter de vanligvis? Det bør de beslutte i en hendelse også.»

En av informantene poengterer at den organisasjonen som er der i det daglige er best egnet til å håndtere krisen. Det er hensiktsmessig å kunne støtte seg på det eksisterende i en organisasjon.

> «Det er linjen som fremdeles gjelder, både generelt internt og på tvers. De samhandlingspunktene mellom eksterne organisasjoner i en krise bør brukes også i fredstid».

Ledere må vurdere om beslutningene som tas er hensiktsmessige. For eksempel ved tilsiktede cyber-hendelser som ransomware angrep, også kalt løsepengevirus, finnes det retningslinjer som sier at det ikke skal betales ut løsepenger. Likevel er det noen ganger dessverre hensiktsmessig å betale ut løsepengene.

> «... Samtidig ser man at trusselaktører klarer å evne å endre seg hele tiden, og det skjer så raskt og det er så dynamisk, at flere og flere bedrifter blir presset til å betale ut løsepenger.»

Konsekvensene ved cyberangrep

NB har også i sin årlige rapport om den finansielle infrastrukturen viet et kapittel til cybersikkerhet. Trusselbildet beskrives følgende:

> Digital kriminalitet mot finansforetak øker i omfang, og finansiell sektor har under korona-pandemien blitt rammet oftere enn andre bransjer (Norges Bank, 2021b, s. 19).

NB peker på Solarwinds-angrepet for å demonstrere hva slags hendelser man må være forberedt på. Selv om dette angrepet ikke var direkte rettet mot finansiell infrastruktur, så poengterer NB at hendelsen er relevant og bør brukes som grunnlag for å styrke cybersikkerheten. Konsekvensene av cyberangrep på finansiell infrastruktur beskrives som:

> Cyberangrep på finansiell infrastruktur kan medføre stans eller forsinkelser i transaksjoner og tap eller manipulering av sensitiv informasjon ... En mulig konsekvens av et cyberangrep er at IKT-systemer ikke lenger fungerer eller ikke kan benyttes fordi operatøren ikke lenger kan stole på at data er korrekte, slik at betalinger ikke kan gjennomføres. En stans i betalingssystemet vil ganske raskt kunne få konsekvenser for finansiell stabilitet (Norges Bank, 2021b, s. 19).

Konsekvensene ved at en større bank eller et sentralt infrastrukturforetak blir satt ut av spill over noe tid som følge av svikt i IKT-systemer kan true den finansielle stabiliteten (Meld. St. 31, (2020-2021), s. 39). Følgende nevnes noen forhold som kan virke risikoreduserende:

> ... økt mangfold av aktører og løsninger kan virke risikoreduserende hvis transaksjoner og tjenester kan utføres i flere, delvis uavhengige systemer. Utviklingen så langt viser imidlertid at den nye tjenesteytingen i hovedsak har skjedd innenfor eller i forlengelsen av eksisterende infrastruktur (Meld. St. 31, (2020-2021), s. 39).

I tillegg påpekes det også at IKT-driften i finanssektoren består av et relativt lite antall sentrale tjenesteleverandører og datasentre som også leverer tjenester til andre sektorer. Leverandørene kan han ha mer ressurser og kompetanse til å utvikle robuste løsninger, og kan dermed bidra til å redusere risikoen for uønskede hendelser i systemet. Derimot er utfordringen større dersom problemet oppstår hos en sentral tjenesteleverandør, da det kan få ringvirkninger til store deler av finanssystemet (Meld. St. 31, (2020-2021), s. 39). På bakgrunn av at et cyberangrep på et enkeltsystem kan få konsekvenser for andre deler av eller hele det finansielle systemet. Gir det et behov for regulering og koordinering. NB peker på motstandsdyktighet mot cyberangrep i finanssektoren, og mener det er et behov for at dette styrkes. Videre sies det også at for å motvirke cyberrisiko har de arbeidet med et bredere perspektiv enn tilsyn og overvåking av enkeltsystemet (Norges Bank, 2021b, s. 19 - 20).

Innovative tilnærminger for å håndtere cybertrusselens kompleksitet

Næringslivets rolle står helt sentralt når det kommer til ivaretakelse av digital sikkerhet. Med sine kompetanser og ressurser er næringslivet en driver for digitalisering og innovasjon (Departementene, 2019, s. 9). En informant understreker at cybertrusselen er kompleks, og da krever det en innovativ tilnærming. I en risikoanalyse handler det om å prioritere, hvis ikke blir den svært omfattende og uoversiktlig. Den tradisjonelle risikostyringen der det tas utgangspunkt i det kompliserte, hvor årsak fører til en effekt er utfordret av inntoget til cyber.

> «... men så beveger vi oss over til det komplekse, der årsak henger sammen med effekt, de påvirker hverandre og alt er på grunn av digitalisering, fordi alt henger sammen med alt nå.»

Det at trusselaktører har en evne til å endre seg hele tiden gjør det spesielt vanskelig for en virksomhet å holde tritt med hva som er de aktuelle truslene til en hver tid.

> «... hva har jeg som bedrift av verdier som jeg må verne til enhver tid, og hvordan finner trusselaktørene nye måter å komme seg inn i systemet mitt på ...»

En informant forklarte at hendelser knyttet til brann eller arbeidsulykke er konkrete hendelser som har blitt jobbet med i alle år. I motsetning til cyberangrep som kan være så mye forskjellig.

> «... En brann er en brann uansett, mens et cyberangrep det er tyveri av data, det er ransomware, det er tjenestenekt angrep, det er så mye forskjellige typer cyberangrep ...»

Derfor er de risiko- og sårbarhetsvurderingen som gjøres i forkant viktige. Det å gjøre verdivurderinger knyttet til virksomheten, og vurdere hva som kan være motivasjonen til trusselaktøren.

> «... det å forstå trusselaktøren er egentlig kompleksiteten i hva som er et cyberangrep, og hva er min bedrift sine verdier, og at det er i det hurtige tempoet vi ser, stadig nye teknikker og måter å komme seg inn på ...»

Ved å øke virksomheters ledere og ansattes bevissthet og kompetanse om trusselbildet og sikkerhetsarbeidet vil det kunne bidra til å styrke nasjonal sikkerhet. Rapportering om sikkerhetshendelser er essensielt for å øke risikoforståelsen og for å bygge et felles nasjonalt situasjonsbilde (NSM, 2022, s. 9). Det understrekes også at man må ivareta et helhetlig og sektorovergripende perspektiv. Dette for å kunne fange opp avhengigheter, bidra med faglig bistand og kvalitetssikring innenfor de ulike samfunnssektorene. Det beskrives at trusselbildet som de enkelte virksomheter står overfor, særlig innenfor cyber-domenet, i mange tilfeller er av sektorovergripende karakter (NOU 2016: 19, s. 19).

Systemets omfang

I analysen av intervjuene er det fremtredende at det er nødvendig med en helhetlig forståelse av systemet finanssektoren er bygget på. En systemforståelse er sentralt i det forebyggende arbeidet i styrkingen av cybersikkerhet. På bakgrunn av at cyber på mange måter er så nytt for mange og komplekst handler det også om at en del ting må være avklart. Som nevnt i delkapittel 5.1.2 dreier det seg om å kartlegge interessentene. Samtidig som aktørene kartlegges er det også nødvendig å bygge kompetanse på funksjonsområdet de ulike aktørene har i en cyber-hendelse.

> «Det er det som er så blir komplekst når man snakker om en cyberhendelse i finanssektoren, fordi hvem er det som er på statlig nivå, hvem er på myndighetsnivå, hvem er bankene, det spindelvevet av aktører i finansnæringen, hvem er det som eier infrastrukturen? ... sånn fungerer den tekniske løsningen bak banksystemet vårt, sånn fungerer infrastrukturen vår. Dette her er bankenes rolle i infrastrukturen. Hvis du har alle aktørenes rolle klart for deg, da vil du klare å samvirke.»

Det er likevel vanskelig å oppnå en fullstendig forståelse av et system som er så sammensatt av både det tekniske, organisatoriske og de menneskelige aspektene.

> «... det er vanskelig for en økonomisk direktør som sitter med konsekvensene av cyberangrepet som kan skje og forstå hva en IKT direktørs system er bygget opp. Så i hvertfall ha en overordnet forståelse av systemet, kanskje ikke på teknisk nivå. Forstå hva som kan stoppe leveransen til den andre enden, og forstå hva som kreves, hvilke tiltak som må iverksettes for å forbedre ting.»

5.3 Cyber22

Beredskapsøvelsen Cyber22 har vært selve analyseenheten i denne studien. Slike storskala øvelser tilhører sjeldenheten og er helt unikt for finanssektoren. NB er initiativtaker og leder for øvelsen, og selv om angrepet rammer NB så treffer angrepet også bredt og dermed også nasjonalt.

> «Det vil være en nasjonal krise, ikke bare en Norges bank krise.».

Økt samfunnssikkerhet er derfor en av flere positive sider med øvelsen. Som en del av trusselbildet har cyber-delen kommet de siste årene som en naturlig del av øvelser og trening. Cyber22 er den første sektorøvelsen i finanssektoren og det har ikke blitt trent så stort før. Informanten forklarte at cyberøvelser ofte trenes på taktisk nivå og ikke hele kriseriggen. I NB har de også det nøkkelinformantene kaller innadrettet treninger for å trene på kompetanse i kriseorganisasjonen.

> «Fagmessig hvordan man håndterer og hvordan man kommuniserer internt. Også har man simulert samvirke, men man har ikke trent så mye samvirke. Vi har noe i departementet, også på cyber, men ikke med så mange som under Cyber22. Det er unikt.»

NB har også noe de kaller varseltreninger, der BFI varsles og varsler videre igjen til aktørene. Varseltreninger er å anse som hensiktsmessig, det kommer frem fra både offentlige dokumenter og intervjuer med informantene at varsling og deteksjon er viktig for det forbyggende arbeidet i cyberdomenet.

Cyber22 er en komplisert øvelse å arrangere og gjennomføre. Øvelsen foregår i sanntid, det vil si at øvelsen spilles i den tiden som er akkurat nå. Bakteppet for øvelsen tar utgangspunkt i verden som den er reelt når øvelsen startet. Det vil si at verden er på vei ut av covid-19 pandemien og at den sikkerhetspolitiske situasjonen er kraftig forverret.

> «... Hva betyr dette for ressursallokering for en ny hendelse? ... I lys av Ukraina-situasjonen har Justis- og beredskapsdepartementet gitt økt bevilgning til NSM for alarmtjenester og diverse tiltak for å forbedre cybersikkerheten. Så det er helt klart at vi spiller et så tidsaktuelt scenario som faktisk kunne ha skjedd når som helst.»

Med bakgrunn i scenarioets omfang er det en utfordring å få en slik øvelse til å bli reell og å få involvert nok deltakere.

> «... når vi lager slike type beredskapsøvelser så vil vi jo gjøre det så realistisk så mulig og gjenkjennbart som mulig, og da er media en viktig komponent i det.»

Øvelsen har som mål å få til et godt samvirke, denne målsettingen har planleggingsgruppen brukt gjennomgående for å oppnå bedre håndtering, også i forberedelsesfasen. Gitt at en får til et godt samvirke vil dette også kunne bidra til et annet hovedmål, nemlig å forbedre sikkerheten på cyber.

5.3.1 Bakgrunn for øvelsen

Alle aktører og virksomheter med ansvar for kritiske samfunnsfunksjoner og som er avhengig av IKT-tjenester har på vegne av departementene et eget ansvar for å gjennomføre nødvendige øvelsesaktiviteter på området (NOU, 2015: 13, s. 105). Det øves for lite, både på samordning og koordinering på tvers av etater og virksomheter. Det poengteres at manglende øvelser kan blant annet bidra til å forsterke uklare rolle- og ansvarsforhold i hendelseshåndtering (NOU, 2015: 13, s. 106). Myndigheter setter sikkerhetsbegrensing til blant annet til NB som har ansvar for finansielle infrastruktur. Sikkerhetsbegrensningene innebærer at finansaktørene må gjennomføre øvelser for å i sikre gode rolle- og ansvarsforståelse for å ivareta et godt samvirke.

Cyber22 ble initiert av NB med bakgrunn i evalueringen etter øvelse Digital 2020. Øvelse Digital 2020 er en nasjonal tverrsektoriell digital sikkerhetsøvelse, som DSB hadde ansvaret for å planlegge, gjennomføre og evaluere (Direktoratet for samfunnssikkerhet og beredskapsarbeid, u.å.). NB har med utgangspunkt i funn tatt et initiativ til å lage en ny øvelse spesifikt for finanssektoren. Tilbakemeldingen i den systemteoretiske modellen ble da evalueringen av Digital2020. Dette viste at øvelser er en god måte for å kunne evaluere samvirke. Begge øvelsene Digital2020 og Cyber22 går under samme krav, men Cyber22 er en spesifikk måte å gjennomføre kravet på ny med hensikt å forbedre samvirke i finanssektoren.

> «... hovedkonklusjonen fra digital 2020. Vi hadde behov for enda mer samvirke, vi har utfordringer med deling over den digitale flaten når man er underlagt sikkerhetsloven ...»

5.3.2 Planleggingsfasen

Planleggingsprosessen var et sentralt tema under intervjuene av nøkkelinformantene. Planleggingen av Cyber22 går i to spor, den ene internt i Norges Bank og den andre eksternt med de eksterne aktørene. I startfasen hadde informantene det de kaller *precyber*, en øvelse der

de gikk igjennom det de kaller for den *«visuelle samvirkeanalyse»* (se avsnitt 5.3.3 og vedlegg 5). Meningen med dette var å kartlegge samvirke.

> «Hvor er det samvirke inntreffer under en cyberhendelse, og gjøre det så smidig så mulig før øvelsen.»

I det interne sporet ble det gjennomført rolletrening og trening i operasjonell krisestab gjennom den *visuelle samvirkeanalysen*. Det ble også gjennomført trening på strategisk krisestab gjennom bevisstgjøring, rolletrening og den *visuelle samvirkeanalyse*n. I det eksterne sporet er det gjennomført workshops med de eksterne som også er en gjennomgang av samvirkeanalysen. Under slike workshops reflekterer de eksterne deltakerne rundt samvirke og egen rolleforståelse, som gjør at man kan peke på hvor samvirke er bra og hvor det er potensial for forbedring. Dette medførte at Finansdepartementet etterspurte en kunnskapsutveksling med NB. Under kunnskapsutvekslingen reflekterte de rundt hva som skjer hvis oppgjørssystemet går ned, potensialet og verstefallsscenario.

> «Da er vi inne på det med helhetsforståelse, systemforståelse... Da fikk vi økt forståelse for det, vi fikk pratet en del og de fikk spurt masse spørsmål.»

Dreieboken i øvelsen er basert på dreieboken fra Digital 2020, denne ble videreutviklet med innspill fra de eksterne aktørene for å tjene formålene å skape realisme i øvelsen og muliggjør øving for alle deltakerne. I planmøtene har de bevisst trent elementer for å gjøre stabene, risikoeierne og direktørene trygge på den generelle gjennomføring. Dette med bakgrunn i at øvelsen spilles i reell tid.

> «Vi vet ikke hva deltakerne vil gjøre, vi må bare agere på det som skjer. ... så har vi trent lederne av stabene, risikoeierne og direktørene. Slik at de blir trygge på en generell gjennomføring, men også trygg på selve casen. ... De får så mange koordineringsutfordringer, dermed vil det være mer en nok læring som oppstår, men da får vi også positiv læring også, ikke bare negativ læring. Vi må ha litt god følelse. Det er bærebjelken i planprosessen, vi har vært opptatt av involvering og samhandling.»

En annen informant forklarte også at de har involvert avdelingene som egentlig ikke er med på øvelsen. Ved å ha én til én møter med de som kunne tenke seg å sitte i stabene.

> «...også har vi sagt dette vil grovt skje, nå har du muligheten til å øve din avdeling hvis du vil. Du kaller inn folkene som du vil ha med deg i øvelsen den dagen. Om det bare er for å få informasjon eller om de skal jobbe med en case. Da er det opptil risikoeierne selv å involvere sitt eget personell for å sikre at sin avdeling går.»

Med bakgrunn i pandemien covid-19 ble øvelsen utsatt fra 2021 til 2022. Dette medførte at planleggelingsgruppen fikk enda lenger tid til å dimensjonere øvelsen. Blant annet førte dette med seg at man fikk reflektert rundt media sin rolle.

> «... cyber er jo et tema som den vanlige mann i gata sliter å forstå hva det egentlig er snakk om ... Så det var nok noe vi ikke hadde sånt fokus på helt i starten, at media må jo faktisk sitte og oversette disse tingene og sette det i en kontekst.»

Media sin rolle i spillstaben er å oversette hva en slik hendelser betyr for folks økonomi.

> «... hva det betyr det for sparepengene til folk, hva betyr det for hva du og jeg ser på kontoene våre, om vi kan betale mat i butikken også videre.»

Utforming av scenario

Fullskalaøvelse er en kompleks øvingsform. Dette kan skyldes at scenario både skal oppleves, og at det skal være realistisk. Informantene forklarte at for å få til et godt scenario må man ha en forståelse av konsekvensbilde, altså hva innebærer det ved at disse hendelsene skjer og hvordan blir aktørene rammet. Under Cyber22 er det oppgjørssystemet som rammes. En informant forklarte at sektoren har trent svært lite på nasjonale cyberhendelser slik som de nå har trent i denne øvelsen. På tross av at det har vært fokus på å få på plass et godt scenario, så har involvering av andre aktører i utarbeidelse av scenario vært det viktigste.

> «... det er komplisert å sette it-folkene og de andre fagfolkene sammen og komme opp med en gjennomgående god case. Så det har vi måtte jobbet med parallelt med at vi får dem riktige folkene med, og begynne med å ha interaksjon mellom ulike virksomheter og fagdimensjoner for å kunne få til en bra case, som i størst mulig grad tilfredsstiller alle sammen.»

I tillegg har de i samhandling mellom andre aktører og deltakere lagt vekt på åpenhet, ikke nødvendigvis åpenhet om scenariet, men hva et mulig konsekvensbilde kan være. En informant forklarte at det er for stort fokus på at ikke skal vite scenariet, men påpeker at dette ikke er hensiktsmessig måte å håndtere cyber-øvelser på.

> «... på cyber da, så kan det bare bli til at man kaster dem inn i et stort hull ... også blir det jo masse bortkastede investeringer, fordi det gir jo ikke noe mestringsfølelsen.»

5.3.3 Visuell samvirkeanalyse

NB sitt mål og hovedfokus har vært å operasjonalisere samvirke også i forkant av øvelsen. Dermed har de kartlagt interessentene i en omfattende analyse og utarbeidet et praktisk verktøy for å gi en bredere forståelse av hvem som inngår i finanssystemet. Dette førte til en innovativ fremstilling av interessentanalyse i det de kaller en *visuell samvirkeanalyse* (se vedlegg 5).

Kartlegging av interessenter

I sammenheng med at samvirke er forbedringspotensialet har det i planleggingsfasen vært sentralt å gjøre gode interessentanalyser for å kartlegge hvem NB faktisk skal samvirke med

dersom oppgjørssystemet blir utsatt for et angrep. I utgangspunktet er det eieren av øvelsen, NB, som har jobbet med å forstå det grove skadebildet. Deretter er det identifisert hvilke virksomheter som er viktige interessenter. Interessentene er begrenset til finans og sikkerhetsmyndighetene. Da den overordnede målsettingen er samvirke, har de brukt denne målsettingen gjennomgående for en bedre håndtering i forberedelsesfasen.

I prosessen med kartleggingen av interessentene har involvering, nettverksbygging og en forståelse av systemet vært sentralt for å forbedre samvirket. I tillegg har hele prosessen frem til øvelsen lagt et grunnlag for å skape relasjoner ved å gå gjennom alle varslingslister.

> «Det skaper en tosidig forståelse av hva som kreves for å avgi informasjon, informasjonsutveksling, hvilke maler som finnes, hvilke varslingslister, hva som trengs for å løse problemet.»

En slik prosess er både kostbar og tidkrevende, da det kreves en del jobb og kartlegging for å få orden på nettverket. Det er også nødvendig å ha kunnskap om hvordan de tekniske løsningene som finnes i baksystemet, hvordan infrastrukturen fungerer, og hvilken rolle de ulike bankene og aktørene har i denne infrastrukturen. Denne forståelse av systemet legger grunnlaget for selve samvirke både i forkant, under, og etter en hendelse. I analysen av interessentene går man inn og ser hvem som er viktige, hvor god kommunikasjonen har man dem, og om kommunikasjonslinjene er på plass. I forklaringene til informantene ligger det en avklaringsprosess og en utvidet systemforståelse. Det var en klar oppfordring fra Departementene at alle aktører må se utover seg selv for å ivareta digital sikkerhet (Departementene, 2019, s. 9). Dette viser at NB ikke kun ser på det interne systemet, men det eksterne også – dermed systemet som helhet.

Beskrivelse av nettverks-kartet

I litteraturen finnes det samvirkeanalyser illustrert i enkle matriser. Den visuelle samvirkeanalysen er en helt ny måte å visualisere og fremstille samvirke på. Informantene forklarte at de er ikke kjent med en lignende samvirkeanalyse. Det er brukt en programvare kalt *MindManager*, der en visualiserer informasjonen i et slags tankekart. NB er i sentrum i deres kart, også er det tatt utgangspunkt i scenarioet i Cyber22 der oppgjørssystemet er kompromittert. Utfra NB er det som et spindelvev av den interne strukturen i organisasjon med avdelinger.

> «Norges bank består av stort system med x-antall mennesker, så hvem helt konkret skal vi samarbeide med?... så hvis man trykker inn på Norges Bank så får man en liste med

avdelingene, strukturen og organisasjonen. ... så kan man utvide den valgte avdelingen igjen, så kan en komme helt ned på personnivå.»

Tidlig i prosessen startet plangruppen med å verifisere og bredde ut nettverket. Dette er gjort i samarbeid med direktørene i NB for å kunne tegne et bilde av avhengigheten mellom de eksterne interessentene. Ut ifra dette validerte nøkkelinformantene grovt godheten i samhandlingslinjene som er beskrevet i tabell 4.

Tabell 4: Beskrivelse av godhet i samhandlingslinjene

Fargekode	Beskrivelse
Grønn	En kjent relasjon. Kontaktinformasjon er etablert, det er kjente varslingsrutiner, og samhandling er trent og evaluert.
Gul	Relasjonen er kjent, men ikke trent eller øvd.
Rød	Relasjonen er ikke kjent, ikke trent eller øvd.

I verktøyet er det tegnet opp en hierarkiskstruktur med myndighetsnivået øverst med de ulike departementene, etterfulgt av de som har direkte innvirkning i scenariet for NB. For eksempel DNB som er under norske banker. Et viktig moment i prosessen har vært å inkludere alle nivåene i utforming av kartet. Dette for å skape eierskap for de eksterne aktørene til verktøyet, samtidig som de kunne kvalitetssikre analysen. Dette gjorde at de fikk lagt til informasjon som de ikke var klar over. Informantene forklarte at prosessen har medført at direktørene har fått en bedre forståelse av systemet der de ser linjer og tydeligere ansvarsroller av hvem som har ansvar for koordineringen i en hendelse.

«... her må vi ha en "informasjonshub" og en "koordineringshub" som er i den staben. Vi må få omsatt dette på en god måte ut mot de aktørene som er relevante i en prioritert rekkefølge... Også får man gjort et skille mellom hva toppledelsen tar av koordinering og hva operasjonelt tar av koordinering inn mot de ulike aktørene.»

En idé bak analysen er ifølge informantene å kunne sette inn alle nivåer i et stort system. Der en tilslutt kan se for seg statsministerens kontor, alle departementene rundt, og de ulike næringene og sektorene som kan knyttes til departementene igjen.

«... Når man sitter inni dette verktøyet og legger til aktører, legger til personer, grupperinger, får opp interessentkartet, prøver å skissere ut hvem som har koblinger hvor, så blir det til slutt så stort at du kan gjøre det med hele Norge for å sette det helt på spissen.»

Betydningen av planleggingsfasen

Nøkkelinformantene er tydelig på at planfasen har vært helt avgjørende. De er alle enige om at det er i den forebyggendefasen grunnlaget for samvirke legges, der god koordinering, og

forståelse for hverandre sine roller og ansvar er forutsetninger. Det er brukt mye tid på å analysere samvirke-kartet, og bli kjent med aktørene. Det er ikke kjent at det er blitt gjort noe lignende i finanssektoren i Norge.

> «... men det vi gjør nå er det som er med på å bygge kultur, det å bygge god beredskap. ...»

I planprosessen opplevde informanter fra plangruppen at Cyber22 og den visuelle samvirkeanalysen skapte interesse hos mange, også utover deltakere, da ordet spredde seg i nettverk.

> «... Så du har eksempler på store norske konsern som tar kontakt på grunn av det vi jobber med, fordi de naturlig har et cyberfokus.»

I tillegg har fokuset på samvirke og cybersikkerhet ført til fagutvikling ved at mennesker er satt sammen i planprosessen. En av informantene ønsket å ta tak i informasjonssikkerhet i finansnæringen, dermed ble det opprettet dialog mellom Nasjonale sikkerhetsmyndigheter og NB.

> «De hadde ikke opprettet den dialogen uten at det hadde krevd større initiativ, den kommer automatisk nå.»

Som nevnt tidligere inviterte også Finansdepartementet, ledere i NB og sentrale fagfolk til et seminar der konsekvenspotensialet ble drøftet. Dette førte til at departementet fikk økt kunnskap om håndtering av slike hendelser. I tillegg har NB koblet IT-miljøene sammen med forretningsmiljøet. Dette for å skape forståelse og løsninger i fellesskap.

> «Som mandater, kan IT stenge systemer hvis de oppdager det? IT lever jo ofte i den formeningen, imens for eksempel til en stor privat bank i Norge, så er det så komplekst fordi det får fordeler for den ene dimensjonen, og ulemper for en annen dimensjon. ... Sånn at de lederne for de ulike avdelingene må treffes, optimalt sett før IT stenger systemet.»

Planfasen har også påvirket risikoeierne i den forstand at de har fått økt forståelse for risikoen. Dette resulterer i at ramme- og planverk ble oppdatert. Nye relevante ressurser blir ansatt eller omskolert. I tillegg ser NB et tydeligere behov for samvirke i store virksomheter med kontinuitetsstaber, da de ulike stabene må jobbe sammen.

> «... får mer effekt gjennom samvirke hvis dem setter seg sammen på grunn av den trusselen. Det er et direkte biprodukt av planprosessen, med den virtuelle samvirke analysen så ser dem at de må sitte sammen...»

Hovedmålsettingen med øvelsen var å forbedre det interne og eksterne samvirke. Nøkkelinformantene har likevel oppnådd flere gode effekter som også vil ha betydning for den øvrige beredskapen.

5.3.4 Gjennomføring- og evalueringsfasen

Øvelse Cyber22 er en omfattende fullskalaøvelse bestående av sentrale finansaktører i sektoren. Hovedmålene for øvelsen var samvirke, effektiv håndtering, rask situasjonsbevissthet og iverksettelse av tiltak. Under øvelsen ble spillstab, strategisk og operasjonelt nivå i NB observert. Scenarioet som deltakerne ble eksponert for var komplekst. Øvelsen startet med at tele- og kraftselskaper ble rammet av cyberangrep som forstyrret deres tjenester. Dette kunne etterhvert oppfattes som en avledningsmanøver på det egentlige angrepet som rammet NB. Dette angrepet ble rapportert til NSM, og ble referert til som en pågående sikkerhetshendelse. På dette tidspunktet hadde de ikke full oversikt over situasjonen, og fokuset var dermed å oppnå situasjonsbevissthet og nøytralisere angrepet.

Basert på varselet fra NSM mottar flere finansaktører varsel om sårbarhet. En underleverandør av NB melder om kompromittering[3] til NSM. NBs beredskapsteam (Global Security Operation Centre) som har første ansvar for fysisk sikkerhet, varsler om alvorlig sårbarhet i systemene til underleverandør (Basefarm) av samfunnskritiske systemer. Det blir satt krisestab i NB. Det går flere varsler og tilbakemeldinger mellom de eksterne aktørene for å få en felles situasjonsbevissthet. Som observatør var det en utfordring å observere det eksterne samvirke mellom alle aktørene. Funn fra resultatene knyttet til samvirke til de eksterne deltakerne kom frem i evaluering fra øvelsesdagen.

Samvirke i operasjonell og strategisk krisestab

Den operasjonelle krisestaben bestod av flere fagpersoner fra NB. En av deltakerinformantene forklarte at det å ha en stor krisestab både har fordeler og ulemper. I øvelse Cyber22 opplevdes en stor krisestab som uproblematisk, og tvert imot bidro det til bedre samvirke internt i NB. Dette fordi at deltakerne var bevisst i sin rolle, og at de ikke forstyrret sentrale personer i krisestaben under viktige diskusjoner. Innledningsvis ble det gjort en grovvurdering av hvem som skulle sitte i krisestaben. Dette kan tolkes som en kvalitetssikringsfunksjon av

[3] «Kompromittering» betyr å røpe eller bringe til fare. I denne kontekst betyr det at data blir borte eller ikke lenger kan stoles på.

koordinatoren. På denne måten involveres fagpersonene som har viktige funksjoner. Informanten beskriver at det gjorde dem mer robuste.

> «... når noen fra staben måtte ut så hadde man nok ressurser.»

Det forutsetter at de som sitter i staben har god rolleforståelse, og at de som diskuterer ikke blir hemmet av at det er flere personer i rommet. Dette ble ikke observert som en utfordring under øvelsen. I den strategiske krisestaben satt en sentral del av kriseledelsen. Både strategisk og operasjonell krisestab evnet å følge den proaktive metoden. Koordinator-rollen i operasjonell krisestab blir pekt ut av samtlige informanter som svært nyttig.

Informasjonsdeling og felles situasjonsforståelse

En sentral del av samvirke er å ivareta informasjonsinnhenting og -utveksling. Under Cyber22 utgjorde operasjonell krisestab det koordinerende leddet i øvelsen. De hadde god nytte av ulike informasjonsforum blant annet NBOK, BFI og GSOC med kobling til NFCERT.

> «... som forenklet kommunikasjon, det gjorde det lettere for oss å ta beslutninger og å få en felles situasjonsforståelse.»

Ettersom øvelsen bestod av flere ulike aktører, kan det potensielt bli veldig mange kommunikasjonskanaler. Informanten trekker frem BFI som et forum der man får samlet alle bankene sammen for informasjonsutveksling.

> «... Spørsmål vi hadde til bankene, tok representanten fra NB med seg, også ved neste møte hadde vi da fått svar. Det forenklet prosessen veldig.»

I tillegg fikk man et samlet svar i en kommunikasjonskanal som allerede var etablert. Under observasjon av evalueringen ble BFI også trukket frem som positivt for situasjonsoppdatering fra de eksterne deltakerne. Med bakgrunn i at selve problemet i scenarioet lå i IT-systemene, var det helt essensielt å få informasjon fra de som jobber med systemene. En av informantene fra operasjonell krisestab forklarte at de visste hvem de skulle kalle inn som jobbet direkte med problemstillingene og som kunne orientere dem.

> «... Det er ikke så mye vi kan gjøre med det ... Det er om å gjøre å finne ut hvor det er, hva slags komplikasjoner det kan medføre og hva som er potensiale for en slik hendelse.»

Det var i hovedsak NBCIM som ble brukt til loggføringer og tavler. NBCIM er krisehåndteringsverktøyet som brukes for informasjonsbeskrivelse og informasjonsdeling. Funksjonen til loggføreren er å transkribere det som blir sakt samtidig som man trekker ut det som er essensen. Det ble observert under øvelsen at loggfører i operasjonell krisestab ønsket

gjerne en tydeligere kommunikasjon på elementer som var viktig i loggføringen. Foruten dette fremstod det både i intervju og observasjon at loggføring i operasjonell krisestab fungerte godt.

I tillegg til NBCIM ble det også brukt andre digitale verktøy til ulike funksjoner i det interne samvirke. Som for eksempel innkalling og informasjon på e-post, og at det ble opprettet kanal i Microsoft Teams for en mer uformell dialog mellom møtene.

> «... Tre forskjellige verktøy også er det egentlig ikke noe enighet om hva som skal brukes til hva. På e-post kommer innkallinger, ikke noe annet. Det kunne vi nok ha blitt enig om ...»

Det at man kunne ha avklart kommunikasjonsverktøy og funksjon på forhånd kom frem i observasjon av operasjonell krisestab. Deltakerne opplevde det som positivt med fleksibilitet i bruk av verktøy, der det ble observert at teams-kanal ble trukket frem som nyttig av deltakere i operasjonell krisestab. Under observasjon av øvelsen fremkommer det at tidspress var en sentral utfordring, samtidig ga det også positive effekter. Informanten fra operasjonell krisestab påpekte at arbeidsfordelingen mellom strategisk og operasjonelt var bedre enn det har vært før. Dette kunne ifølge informanten skyldes at tidspress gjorde at man ble tvunget til å separere mer, og at strategisk krisestab ikke fikk tid til å gå ned i detaljer. Innledningsvis sitter avdelingsdirektørene og diskuterer potensialet. Under observasjon av første møte på strategisk poengteres det at de skal støtte operasjonelt slik at de kan ta gode beslutninger for å komme seg videre i situasjonen. I dette ligger det også en ivaretakelse av det eksterne samvirke med interessentene. En informant forklarte i intervju at det var lite kommunikasjon mellom strategisk nivå på tvers av de eksterne.

> «Det tror jeg er viktig å ha i en skarp situasjon at vi har kontakt på strategisk nivå. Åpne kontaktlinjer og sikre en felles forståelse av situasjon. Det jobbes mye mellom taktisk og operasjonelt, men man bør også etablere kontakt mellom toppledere.»

Fra observasjon fremkom det at situasjonsbeskrivelsen og potensialet ble godt diskutert på det strategiske nivået. Dette kan tyde på at informasjonsflyten fra taktisk og operasjonelt nivå ble ivaretatt. I tillegg var det fokus på å bevare kontinuitet som er viktig for å opprettholde tillit i et forretningsøyemed. Kommunikasjonsflyten ble observert til å være god mellom de sentrale lederne og rådgiverne i krisestaben til strategisk. Dette fordi de var tydelig med hverandre i kommunikasjonen samtidig som de viste evne til å lytte. De kommer effektivt inn på umiddelbare tiltak. Med bakgrunn i at det i en tidlig fase ikke var fullstendig oversikt over situasjonen og at det var tidskritisk, var det positivt at strategisk nivå opplevdes som effektive

i håndteringen. De evnet å diskutere bredt med tanke på situasjonen raskt kunne endre seg. De nevnte også beredskapsløsninger til systemene relativt tidlig dersom det skulle være nødvendig.

Bruken av den visuelle samvirkeanalysen

Den visuelle samvirkeanalysen var opprinnelig ikke planlagt brukt under håndteringen. Den var foreløpig laget til kartlegging, og for å vise godheten i samhandlingslinjene. Hos spillstaben og den operasjonelle krisestaben var den visuelle samvirkeanalysen hengt opp som en plakat. Dette gjorde det enkelt for deltakerne å få oversikt over aktørnettverket i tilknytning til scenarioet. I strategisk krisestab kan det fremstå som at analysen ikke ble brukt i like stor grad. Sentrale roller i operasjonell krisestab brukte den visuelle samvirkeanalysen aktivt for å få oversikt over kommunikasjon med aktørene.

> «... Fikk en oversikt over hvem vi hadde snakket med og hvem vi ikke hadde snakket med. Kvalitetssikret at vi hadde kommunikasjon med de vi skulle ha kommunikasjon med.»

I den visuelle samvirkeanalysen vises ingen prioriteringsrekkefølge på kontaktene. En av informantene forstod det slik at den ble brukt til å fordele kontakter fremfor å prioritere. Det er vanskelig å si helt konkret hvordan den ble brukt. Dersom en prioritering er hensiktsmessig, er dette noe som kan jobbes med. På en annen side fungerte analysen som en effektivisering av prosesser. Dette frigjorde mental kapasitet under en tidskritisk hendelse. I tillegg fikk en oversikt over det som ofte kan oppleves som uoversiktlig og komplekst under en cyberhendelse, nemlig hvem man faktisk skal samvirke med.

Krisekommunikasjon

I mediaspillstaben satt fem personer som simulerte omverden gjennom media, som en kanal for å beskrive dagens situasjon i Norge. Et komplekst scenario som var svært vanskelig å oversette til vanlige folk i gaten. Media sin jobb var å tolke hva som er konsekvensene.

> «Hva er situasjonene, hva har dette å si for konsekvensene på sparepengene mine, lånet mitt ...»

Samvirke var målet for øvelsen. Samtidig utartet øvelsen seg slik at budskapsutvikling og mediestrategi ble en sentral del av det. Blant annet savnet mediaspillstaben at NB tok eierskap til krisen.

> «... Det var svært utfordrende for media og danne seg et helhetlig bilde av situasjonen og krisen.»

Informanten forklarte at for å få til et godt samvirke må budskap og strategi være koordinert. Dette blir spesielt synlig i scenarioer som kan oppfattes som tekniske og komplekse.

> «... Man sliter med å oversette hva er det som har skjedd. Betalingssystemene er nede, hva betyr dette? ...»

I evaluering etter øvelsen ble det også trukket frem av eksterne deltakere at de savnet informasjon om hva som skjedde i bransjen. Videre opplevde også eksterne deltakere at det var enklere å få informasjon fra media enn fra de man skulle fått informasjon fra. I Beckmans (2020) studier var også et sentralt funn at rask formidling av riktig informasjon til offentligheten var en av de viktigste oppgavene for en effektiv cyberkrisehåndtering. En av deltakerinformantene fra operasjonell krisestab påpekte i intervju, i etterkant av øvelsen, at det ideelt sett kunne blitt sendt ut en pressemelding tidligere. Informanten forklarte i en slik pressemeldingen kunne NB formulert at de var utsatt for et cyberangrep på oppgjørssystemet. Det er usikkert om det var spilltekniske grunner til at det ikke ble sendt ut pressemelding på et tidligere tidspunkt. En deltakerinformant fra operasjonell krisestab forklarte at det i øvelsen begynte å dreie seg om hvordan kommunisere ut informasjon. Det ble påpekt med forbehold om ar det på dette tidspunktet enda ikke var gjennomført en endelig evalueringsrapport. Informanten forklarte:

> «Jeg mener likevel at NB må se på alle de pressemeldingene NB ga ut. Er det forbedringspunkter i prosessen for hvordan man får ut informasjonen ...»

Det er ikke kjent gjennom denne studien hva som er NB sine prosesser og rutiner for pressemeldinger under en cyberhendelse. Slik hendelsen utviklet seg i Cyber22 bør NB ifølge informanten se på rask informasjonsdeling som et læringspunkt.

> «Det man vet når man har et angrep er at man må ut med informasjon. Jeg tenker strategisk kunne laget en strategi med en gang på hvordan man skal få ut informasjon.»

En informant forklarte at samhandling og koordinering som skjer internt i en virksomhet kan ha store ringvirkninger og konsekvenser for det som skjer eksternt. Media og kommunikasjon er et eksempel på dette. Informanten forklarte at det handler om å ha en god prosess for hvordan møte media i komplekse scenarioer. Likeledes må en ha kunnskap om konsekvensbilde når for eksempel betalingssystemer tas ned. Tilbakemelding fra media var at deltakerne hadde en profesjonell holdning i møte med media, de var tilgjengelige ved å følge opp på telefon og e-post. I tillegg virket det som at alle deltakervirksomhetene hadde god medieovervåkning.

Manglende situasjonsbevissthet

Under observasjon av Cyber22 ble det tidlig drøftet om det kunne være brudd på konfidensialitet, integritet eller tilgjengelighet i oppgjørssystemet NBO. Tilbakemelding fra taktisk nivå pekte på brudd på integritet ved at det var en endring i fire av nihundre transaksjoner i oppgjørssystemet. I etterkant av øvelsen hadde en av informantene i operasjonell krisestab reflektert over spørsmålet, hva slags juridiske utfordringer de endrede transaksjonene kunne innebære.

> «... så her burde vi nok tatt inn juristene våre, og man kom ikke inn på de spørsmålene med transaksjonene. Det kunne ha noen følger i etterkant, legale virkninger, men ikke akkurat hvordan krisen ble løst på.»

Deltakerinformant fra operasjonell krisestab forklarte i intervju at det var usikkerhet, men at det opplevdes som en oversiktlig usikkerhet. En annen deltakerinformant forklarte at det alltid vil være usikkerhet i beslutningsgrunnlaget.

> «... Man skal bestandig ønske at man vet mer ...»

Tidlig i øvelsen visste ikke deltakerne hva det var, og hvilke innvirkninger hendelsen kunne få. Dette ble klarere utover øvelsen. Informanten forklarte videre at det er en avveining mellom hvor godt beslutningsgrunnlag man skal måtte ha, og når beslutninger må tas fordi det er tidskritisk. Akkurat under Cyber22 opplevde informantene at de hadde nok grunnlag når beslutningene ble tatt.

> «Vi mente at vi hadde nok grunnlag når beslutningen ble tatt. Det betyr ikke at grunnlaget ikke kunne blitt bedre, men vi mente at det ikke var verdt å vente på for å få et bedre grunnlag ...»

Det var heller ikke følgeproblemer på tross av problemstillingene som dukket opp underveis. Dette vil si at det var mulig å rette opp i problemene som ble oppdaget. En informant fra operasjonell krisestab oppfattet det slik at øvelsen var lagt opp til å sjekke noen prosedyrer og rutiner, og dermed ikke bidra til flere vanskelige problemstillinger. Det var også tydelig fra plangruppen at øvelsen skulle gi mestringsfølelse hos deltakerne og trening på prosessen for håndtering av en cyberhendelse. Også en annen informant forklarte at scenario gjerne ikke er et verstefallsscenario fordi man har såpass gode forsvarsmekanismer mot et slikt angrep. Selv om sannsynligheten for hendelsesscenarioet er vurdert til lav, innebærer likevel et slikt scenario store konsekvenser, og dermed anses det å være et relevant scenario.

> «Jeg mener vi skal øve på det ... for få testet ut hvordan vi agerer med cyber eller integritetstap i sentrale data. Det er viktig å øve på. En ting er forsvarer, en annen ting er robusthet. Hvordan klarer vi å håndtere det når vi faktisk bli angrepet.»

Kontra en tabletop-øvelse der alle deltakerne sitter rundt et stort bord opplevdes denne øvelsen i større grad realistisk og nyttig. Selv for de som satt sentralt i NB, så ikke hele bildet hele tiden.

> «Det er en påminnelse og opplevelse at i en kompleks situasjon så har man ikke hele situasjonsbilde hele tiden, og sånn vil det være virkeligheten. Det å kjenne på at alle ikke vet alt hele tiden er en del av virkeligheten ...»

Fokuset på mestring i øvelsen har ifølge en annen informant vært et bevist valg for å skape en vilje til å gjenta det. Her legger informanten til at man ikke har mulighet til å jobbe med beredskap i det sivile samfunnet, hvor hen peker på at NB først og fremst er en sentralbank, og ikke en beredskapsinstitusjon.

> «... at deltakerne er for det meste er i flytsonen, men blir presset ut av flytsonen av og til gjør at det blir en positiv opplevelse. Det må være mestring for å skape denne viljen. Man må lære å gå før man kan løpe ...»

5.4 Oppsummering av analysens funn fra det empiriske materialet

Som et resultat av analysen av de empiriske funnene viser tabell 5 en oversikt over de mest sentrale funnene. Til funnene innenfor hver analysekategori er det utarbeidet noen spørsmål som vil videre gjennomgås i diskusjonskapittelet. De øvrige forskningsspørsmålene tilknyttet hver analyse kategori vil også diskuteres i sammenheng med spørsmål til drøfting.

Tabell 5: Sentrale funn og spørsmål til diskusjon

Forskningsspørsmål	Analyse kategori	Empiriske funn	Spørsmål til drøfting
Hva er samvirke?	**Samvirke** ▪ Innføring av samvirkeprinsippet ▪ Aspekter ved samvirke	På bakgrunn av tidligere hendelser og øvelse Digital 2020 kan det forstås som at NB har blitt mer bevisst på betydningen av samvirke i beredskapsarbeidet. En utvidet forståelse av konseptet samvirke viser til konkrete elementer som aktøren har operasjonalisert for å forbedre samvirke.	Vil en utvidet forståelse av samvirke samt en bevisstgjøring føre til bedre samvirke? På hvilken måte operasjonaliseres samvirke? Hvilke utfordringer finner man i operasjonaliseringen av samvirke?
Hvorfor er samvirke viktig for å oppnå god cybersikkerhet i finanssektoren?	**Betydningen av samvirke i arbeidet med cybersikkerhet** ▪ Forebyggende risikobasert tilnærming ▪ Hendelseshåndtering ▪ Kompleksiteten i cybertrusselen	Myndighetene krever at aktørene skal jobbe tettere sammen gjennom en forebyggende risikobasert tilnærming for å håndtere cybertrusselen. Cyberhendelser krever gode systemer for håndtering. Systemer og prosesser som legger til rette for et godt samarbeid mellom aktører.	Hva betyr det at aktørene skal jobbe tettere sammen gjennom en forebyggende risikobasert tilnærming? Trengs det nye tilnærminger og strategier for å håndtere cybertrusselen?
I hvilken grad oppnås samvirke i planlegging og gjennomføring av Cyber22?	**Cyber22** ▪ Planleggingsfasen ▪ Den visuelle samvirkeanalysen ▪ Gjennomføring og evaluering	Omfattende planlegging av øvelsen har lagt grunnlag for en bedre beredskap. Fokuset på samvirke i beredskapsøvelsen Cyber22 resulterte blant annet i fremstilling av samvirke-analysen. I denne visuelle fremstillingen kan det forstås som at aktørene har oppnådd en bredere og mer helhetlig systemforståelse. Under øvelsen viste det seg at god systematikk er svært fordelaktig i komplekse scenarioer.	Kan planlegging og gjennomføring av øvelsen bidra i intensivering av samvirke? På hvilken måte bidrar de fundamentale prosessen i det interne samvirke til et bedre eksternt samvirke? Hva er sammenhengen mellom formålet i øvelsen og designet av øvelsen?

6. Diskusjon

Det følgende kapittelet presenterer oppsummering og diskusjon av de resultater som ble analysert i forrige kapittel. Kapittelet er delt inn i de tre forskningsspørsmålene som ble presentert i kapittel 1. Under hvert forskningsspørsmål oppsummeres viktige poeng fra diskusjonen. Det første forskningsspørsmålet drøfter den analyserte fortolkningen av samvirke og viser til hvordan plangruppen av Cyber22 har operasjonalisert samvirke. Under det andre forskningsspørsmålet drøftes betydningen av samvirke som strategi for cyberberedskap. Under det tredje forskningsspørsmålet diskuteres læringsmålet samvirke i øvelsen og hvordan dette ble oppfylt i øvelsen.

6.1 Hva er samvirke?

Som følge av denne studien kan samvirke-konseptet tolkes i flere retninger. Samvirke-prinsippet i seg selv gir ikke en uttømmende beskrivelse av hva et godt samvirke innebærer. Det blir den eller de som anvender prinsippet som må vurdere hvordan samvirke-prinsippet faktisk skal tolkes og til slutt operasjonaliseres i arbeidet med forebygging, beredskap og krisehåndtering. Samvirke-prinsippet lyder som følgende:

> Myndigheter, virksomheter eller etater har et selvstendig ansvar for å sikre best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering (Meld. St. 10, 2016-2017, s. 20).

«Selvstendig ansvar for å sikre ...» kan forstås som et objektivt krav fra myndighetene. På den annen side kan «*sikre best mulig samvirke med relevante aktører»* forstås som subjektive krav. Det vil si at det avhenger av hvordan den «virksomheten» eller «etaten» tolker og forstår *best mulig,* og hvem som er *relevante aktører*. Under planlegging av øvelse Cyber22 viste det seg etterhvert at flere og flere aktører var *relevante aktører* å samvirke med. Den omfattende analysen av samvirke, utført av plangruppen i samarbeid med andre, resulterte i den *visuelle samvirkeanalysen*. Det spindelvevet av et nettverk vokste seg stadig større. I det store bildet kunne nok Cyber22 hatt enda flere deltakere og samarbeidspartnere, men for at øvelsen skal være gjennomførbar måtte planleggingsgruppen på et tidspunkt si stopp.

Analysen som ble gjort for å konseptualisere samvirke i teorikapittelet var sammenfallende med analysen som følge av intervjumaterialet. Empiri og analysematerialet tydeliggjorde samvirke-modellen som ble presentert i teorikapittelet. I tillegg tydeliggjorde både intervjudata og observasjonsdata hvordan man i praksis kan operasjonalisere samvirke-prinsippet.

6.1.1 Operasjonalisering av samvirke

Rolleforståelse

I Levesons (2011) systemteoretiske perspektiv kan samvirke også forstås som prosessen i et hierarkisk system der de ulike nivåene gjensidig påvirker hverandre ved å påføre sikkerhetsbegrensninger på nivået under og gi tilbakemeldinger til nivået over. Resultater og analyse viste at aktørene evnet å sette seg selv inn i det hierarkiske systemet. De la vekt på kompetanse om egen og andres *rolle* som viktig for å få til et godt samvirke. På den andre siden viste også gjennomgangen av den visuelle samvirkeanalyse, kan ha tydeliggjort egen rolleforståelse, da man tydeligere ser ens egen roller i det store systemet. Samtidig ble også andres roller og funksjoner tydeliggjort ved å konkret visualisere hvordan disse henger sammen i det gitte scenarioet samvirkeanalysen er bygget på. Dette peker også da i retning av hvilken funksjon og ansvarsområdet de ulike rollene får under en slik hendelse. Den økte rolleforståelse etablerte også ny kunnskap som synliggjorde at flere av stabene burde sitte sammen for å få til et godt samvirke.

Å avklare roller og ansvar kan forstås som svært hensiktsmessig både i operasjonalisering av samvirke- og ansvarsprinsippet. Hvordan dette skal operasjonaliseres kan også diskuteres ut ifra et systemteoretisk perspektiv. Der man med hensyn til overordnede mål skal omsettes til nivåene under. I en virksomheter der IT-aktørene må ta hensyn til forretningsimplikasjoner blir bevisstgjøring rundt roller og ansvar desto viktigere. Å håndtere en cyberhendelse i et IT-perspektiv kan bety å stenge systemene, fra et forretningsperspektiv er det mulig at det å stenge systemene ikke nødvendigvis alltid er hensiktsmessig. Sikkerhetskrav som overordnet nivå pålegger nivået under, kan være krav om varsling til nivået over. Krav bør inneholde klare terskelverdier og tydelig spesifisering i hva som skal rapporteres (Meld. St. 31, (2020-2021), s. 25). Av resultatene anses det at en NB har etablert en slik modell. Dette kan forstås som føringer som er med på å operasjonalisere en tydeligere rolle- og ansvarsforståelse. Krav om kurs i IT-sikkerhet og virksomhetsstyring er kontrollkrav som også kan bidra til å forsterke kompetanse og rolleforståelse i organisasjonen.

Forhåndsetablerte relasjoner

I tilknytning til rolleforståelsen viste resultatene at det bør tilstrebes å *forhåndsetablere relasjoner*. Hvem skal man samvirke med og når? Dersom dette ikke er etablert kan det påvirke aktørenes evne til effektiv håndtering, og dermed også hemme et samvirke. Dette kan knyttes

til både kultur, tillit og det praktiske et godt samvirke innebærer. Av det praktiske handler det gjerne om at man har kontaktinformasjon til de som skal involveres i et samarbeid og rapporteres til under en cyberhendelse. Funn i Beckmans (2020) studie pekte også på å forhåndsetablere relasjoner som en suksessfaktor for god håndtering i cyberdomenet. Dette forsterket informasjonsutvekslingen mellom aktørene. Det å kjenne til hverandre og prate sammen på en generell basis kan tenkes å være en form for operasjonalisering ved å etablere relasjoner. Å etablere relasjoner krever at aktørene selv tar initiativ til dette. I den *visuelle samvirkeanalysen* er samvirke og kontakten mellom de ulike aktørene tydelig visualisert med grønn, gul eller rød strek mellom aktørene. Som følge av analysens utforming kan den bidra med å forsterke behovet for å etablere en slik kontakt, og opprettholde kontakten. Dette forutsetter da at aktørene kontinuerlig gjennomgår og vedlikeholder analysen. Dette diskuteres nærmere under avsnitt 6.2.1.

Kultur og tillit

En god *kultur* kan fremmes gjennom åpenhet og kjennskap mellom aktørene. I teorien om cyber-resiliens omtales en kultur der en anerkjenner improvisasjon og delegert beslutningstaking. Kultur er et stort tema å diskutere som innebærer flere perspektiver. I relasjon til å fremme et godt samvirke er åpenhetskultur helt klart en side av kultur som gjør seg gjeldende i denne studien. Resultatene viste at en åpenhetskultur kan også være utfordret av en streng eller nødvendig sikkerhetskultur. Ved informasjonsdeling kreves det både kunnskap og evne til å balansere lovverket for hva som kan deles og ikke. Det kan også tenkes at kombinasjonen av mangel på kompetanse og en streng sikkerhetskultur er faktorer som kan hindre deling av informasjon. Samtidig er det myndighetene sitt ansvar som pålegger sikkerhetsbegrensninger, å tydeliggjøre kravene om hva som skal deles.

Psykologisk trygghet kan bidra til å fremme en åpenhetskultur. Samtidig som det er nødvendig for et samvirke, så er det ikke helt enkelt å operasjonalisere det. God ledelses- og organisasjonsstruktur som lar medarbeidere våge å gi beskjed, og som tillater å feile er forutsetninger. I cyber-resiliens nevnes improvisasjon, noe som peker i retning av en tolking at dersom en tillater rom for improvisasjon så bør det også være rom for å feile. Økt *tillit* kan være et resultat av å forhåndsetablere relasjoner og en åpenhetskultur. I den praktiserende dimensjonen av Cyber-resiliens skal en grundig planleggingsinnsats styrke den mellommenneskelige tilliten. Cyber22 innebærer en omfattende planleggingsinnsats. I hvilken grad det har styrket tillit mellom aktørene er vanskelig å si, men legges teorien om cyber-

resiliens (Dupont, 2019) til grunn, så skal det ha bidratt til å styrke tilliten og dermed også motstandsdyktigheten i en hendelse.

Kommunikasjon, koordinering og informasjonsdeling

Kommunikasjon mellom aktørene er en forutsetning for at de skal kunne virke sammen. I et responssystem er kommunikasjon helt nødvendig, og der operasjonelt nivå oppfattes som å være bindeleddet for kommunikasjon og koordinering (Lunde, 2019). Koordinator-rollen som NB viser til, er en rolle som skal sikre informasjonsutveksling slik at ledere kan ta beslutninger på bakgrunn av et oppdatert situasjonsbilde. Dette kan bidra til å støtte det interne samvirket i organisasjonen. I tillegg kan også den visuelle samvirkeanalysen bidra til å styrke interorganisatoriske koblinger som letter kommunikasjon og koordinering. Dette innebærer den nettverksbaserte dimensjonen av cyber-resiliens, der resiliens ikke kan fremmes isolert, men må fremmes gjennom koblinger mellom organisasjoner og aktører (Dupont, 2019).

Informasjonsdeling er sentralt både i et langsiktig forebyggende perspektiv, også i håndteringen av en uønsket hendelse. På den ene siden er det utfordrende for hver enkelt aktør som er underlagt sikkerhetsloven å gjøre en vurdering på hva som kan deles. Det forutsetter at aktørene har kompetanse og en forståelse av lovverket. På en annen side forutsetter det også at myndigheter og ledelsen tydeliggjør behovet for informasjonsutveksling, slik at de gjør det lettere for hver enkelt aktør å ta gode vurderinger. Det bør også komme frem tydelig krav om hvordan informasjon skal deles, slik at konfidensialitet ivaretas på en sikker måte. I en hendelse kan det oppstå utfordringer med deling over den digitale flaten. Det krever dermed at dette er trent på, slik som det er gjort i Cyber22. Samtidig må det settes inn visse sikkerhetsbegrensninger, der en ser det er sårbarheter knyttet til deling over den digitale flaten.

Felles mental modell og gode systemer

I et stort finanssystem finnes ulike aktører med forskjellig bakgrunn og kompetanse. Under hendelseshåndteringer er aktørene avhengig av å klare å etablere og opprettholde en felles situasjonsforståelse. Det er først og fremst gjennom informasjonsdelingen aktørene får mulighet til å handle, da de vil forstå hvilke oppgaver som skal løses (Wolbergs & Boersma, 2013). Dersom det i forkant av en hendelse ikke er jobbet nok med det man i teorien kaller en felles mental modell, kan det være utfordrende å ha en felles situasjonsforståelse. Dette er forenelig med Levesons systemteori. Det er mye nytt knyttet til håndtering av cyberhendelser. Ved å planlegge og gjennomføre en slik øvelse, der det også er gjennomført en omfattende

samvirkeanalyse, går NB opp nye samhandlingsmønstre. Den visuelle samvirkeanalysen har vært et verktøy som kan ha bidratt til å oppnå en felles mental modell. Det er på mange måter er operasjonalisering av den felles mentale modellen. På samme måte kunne en også brukt systemteorien til Leveson for å avdekke sårbarheter i systemet ved å se på kommunikasjonen mellom de ulike nivåene og aktørene. Likevel har NB i den visuelle samvirkeanalysen avdekket sårbarheter ved å trekke fargede linjer mellom aktørene for å beskrive kontakten. I tillegg har NB satt de ulike miljøene sammen for å oppnå en felles forståelse av systemet. Med bakgrunn i at cyber er såpass nytt er det helt essensielt å ha gode systemer for håndtering. Å ha god systematikk gjør også aktørene tryggere i håndteringen. Usikkerhet er moment som tydeliggjør seg på bakgrunn av at cyber er et komplekst domene å jobbe i. Derfor er det hensiktsmessig å gjøre både de som tar beslutningene på strategisk nivå, i dette tilfelle risikoeierne eller direktørene, og de som jobber direkte med hendelseshåndteringen på taktisk nivå, trygge på metoden i håndteringen.

Oppsummering

Analysen av samvirke hentet fra teorien var sammenfallende med informantenes oppfatning av samvirke-prinsippet. Gjørv-kommisjonen konkluderte tilbake i 2011, at det var manglende samvirke, på lik linje fant NB også utfordringer med samvirke i evalueringen av øvelse Digital 2020. Denne bevisstgjøringen har tydelig påvirket NB til å jobbe med å operasjonalisere samvirke gjennom en innovativ tilnærming i den visuelle samvirkeanalysen, og ved å gjennomføre en fullskala beredskapsøvelse for finanssektoren. I denne drøftingen av samvirke kom det frem konkrete elementer i samvirke-konseptet som NB har operasjonalisert i planleggingen og gjennomføring av Cyber22.

6.2 Hvorfor er samvirke viktig for å oppnå god cybersikkerhet i finanssektoren?

Myndigheter har gjennom offentlige publikasjoner presisert at det kreves et økt samarbeid for å kunne håndtere de digitale truslene på en god måte (Departementene 2019). Dette samsvarer med den *nettverksbaserte* dimensjonen i Duponts (2019) teori om cyber-resiliens, der man i cybersikkerhet må se utover seg selv for å forebygge og håndtere cyberhendelser. Dupont argumenterer med de samme argumentene som norske myndigheter. Verden er blitt kompleks. Med bakgrunn i de gjensidige avhengighetene i sosio-tekniske systemene, kreves det et økt samarbeid både internt i organisasjoner og på tvers av virksomheter. Denne studien har vist at NB ser betydningen av samvirke for å oppnå god cybersikkerhet.

6.2.1 En systemtilnærming for å håndtere cybertrusselen

Kompleksiteten som cybertrusselen er omfattet av gjør at den kan både treffe bredt og at den stadig er i endring. Av den grunn at det er umulig for en organisasjon å påvirke trusselen, bør fokuset i det forebyggende risikobaserte arbeidet være hvordan man kan kontrollere sårbarhetene. Ifølge Young & Leveson (2013) handler det om å avdekke de sosio-tekniske sårbarhetene som bidrar til forstyrrelser i systemet. Nærmere bestemt flyttes fokuset fra beskyttelse av nettverkssystemer, til strategi for hvordan håndtere sårbarheter i komplekse systemer. Denne tankegangen utfordrer den tradisjonelle risikostyringen. I dette ligger en systemforståelse eller det som tidligere er omtalt som en felles mental modell.

Når det gjelder samvirke så handler det gjerne om aspekter som kommunikasjon mellom aktørene, som inkluderer hendelsesvarsling og informasjonsutveksling. I det systemteoretiske perspektivet dreier det seg om å fange opp systemets evne til å ivareta kommunikasjonslinjene mellom de ulike nivåene. Det handler om å se systemet som en helhet og dermed til syvende og sist ivareta *verdiene* eller *felles mål* omsatt fra Levesons (2011) systemteori. Dette avhenger av at det kommuniseres tilpasninger og tilbakemeldinger mellom nivåene og at menneskene i organisasjonen eller sektoren etablerer en felles mental modell.

Spesielt for finanssektoren så handler det ikke kun om beskyttelse av systemene, det handler også om å redusere konsekvensene som følge av påkjenning på systemer. Konsekvenser i form av økonomiske verdier og tap av omdømme. I et større perspektiv kan det ut ifra systemmodellen by på utfordringer når det er forskjeller mellom private og offentlige virksomheters overordnede mål. Med bakgrunn i at denne studien kun tar for seg en konkret virksomhet så kan det anses som en svakhet at det ikke kan konkluderes her på bakgrunn av resultatene. Likevel viste resultater fra en masteroppgave (Caspari, 2021) at ulike prioriteringer mellom ansvarsområdet svekket samvirke mellom offentlig og private sektorer. Resultatene fra *denne* casestudien av Cyber22 viste at ulike mål innad i en organisasjon kan utfordre håndteringen av cyberhendelser. Dette ble belyst med utfordringene knyttet til de ulike aktørenes IKT- og forretningsperspektiv. Resultatene viste at det å sette de ulike miljøene sammen kan bidra til å oppnå en felles forståelse av systemet. Det kreves en sterk sikkerhetsorganisasjon for å opprettholde en slik modell. Dette krever at aktørene jevnlig opprettholder den mentale modellen ved hjelp av sikkerhetsbegrensninger som pålegges de ulike nivåene, og at man i organisasjonen legger til rette for at aktørene kan utveksle informasjon. Av resultatene fremkom det at det er BFI er en sentral samordningsarena både for

informasjonsdeling og konkrete saker. Det å ha en forhåndsetablert kanal var svært nyttig for informasjonsutveksling i øvelsen.

Cyberdomenet utfordres også stadig av nye underleverandører, som kan føre til at organisasjoner mister kontroll over sårbarheter som rammer underleverandøren av et IKT-system. Myndighetene påpeker at verdikjeden må kartlegges og fokuset bør være å øke sikkerhetsstyring av underleverandørene (NSM, 2022). Young & Leveson (2013) mener at formålet i sikkerhetsstyringen er å forhindre og begrense kontrollhandlinger som kan føre til tap i et verstefallsscenario. En stor virksomhet vil kunne ha flere tjenester som leveres av eksterne leverandører. Kompleksiteten i omfang og utfordringen med å holde en oppdatert oversikt over disse vil være krevende for enhver virksomhet. I STPA- Sec er kontrollering av sårbarheter elementært. Dette fordi det sannsynligvis er langt færre systemsårbarheter enn trusler. Tanken er at dersom virksomheter kan kontrollere disse kan de også håndtere en rekke trusler.

Analysen av resultatene viste at prioritering i sikkerhetsstyring er hensiktsmessig når det kommer til hendelser som kan defineres som *grenseoverskridende kriser*. Dette fordi cyberdomenet ikke bestemmes av geografiske, økonomiske og politiske grenser. Dermed kan en hendelse som ikke nødvendigvis var ment for å treffe virksomheten likevel treffe den. Solarwinds-angrepet demonstrerte akkurat denne problemstillingen. Som følge av analysen av resultatene sett i sammenheng med teorigrunnlaget, er det hensiktsmessig i risikostyringen å fokusere på å forstå hva som er den enkeltes virksomheters verdier. Dette for å videre avdekke sårbarhetene som systemet er omfattet av i beskyttelse av verdiene. I tillegg må det samsvare med myndighetenes overordnede mål for å oppnå økt samfunnssikkerhet.

Ved bruk av den visuelle samvirkeanalysen har NB analysert samvirke i et cyberhendelsesscenario. I den visuelle samvirkeanalysen analyseres samvirke i et nettverk av aktører. Selve analysen gir en beskrivelse av godhet til samvirke, fordi den visualiserer kommunikasjons- og relasjonslinjene mellom aktørene både internt i NB, men også eksternt med relevante interessenter. For eksempel Finansdepartementet fra offentlig sektor eller Den Norske Bank (DNB) fra privat sektor. Ved å sette samvirke inn i et system kan man analysere samvirke ut ifra Levesons (2011) systemteori. De ulike nivåene mellom aktørene i verktøyet demonstrerer hvordan systemet henger sammen, og hvem man skal samvirke i det gitte

scenarioet som analysen baseres på. På denne måten forenkler analysen prosessen for aktørene, og gir en større forståelse av hvordan systemet faktisk henger sammen.

I den visuelle samvirkeanalysen avdekkes sårbarheter i samvirke både internt og eksternt. Verktøyet demonstrerer dette, der fargekoden viser om det er behov for å forbedre forbindelser mellom interessenter. Forhåpentligvis kan verktøyet bidra til en mer effektiv hendelseshåndtering, et økt samarbeid mellom virksomhetene også muligens i fremtiden på tvers av sektorer. Likevel i cyberdomenet der alt henger sammen med alt, er det en utfordring i et systemsikkerhetsperspektiv å avgrense systemet. Ved hjelp av en interessentanalyse blir det bestemt hvilke aktører som settes på kartet og hvilke aktører som utelates. Dermed er det vesentlig å vurdere hvor stort kartet trenger å være for at det bidrar til et godt samvirke i hendelsen. Rom for improvisasjon og fleksibilitet er også viktig, scenarier kan raskt endres og nye aktører kan bli relevant å samvirke med.

6.2.2 Håndtering av cyberhendelser

Håndteringen av en cyberhendelser krever samvirke mellom alle nivåene i en virksomhet. Selv om det er operatører på taktisk nivå som sitter og jobber med IKT-systemene, kreves det i en finansvirksomhet at alvorlige hendelser løftes opp til strategisk nivå. For at man skal kunne gjøre gode vurderinger i cyberhendelser er deteksjon en forutsetning for håndteringen. Utfordringen med cyberhendelser er at det forekommer ofte. På den andre siden er nødvendigvis ikke alle hendelser like alvorlige. Om og når cyberhendelser skal defineres som en krise ble fremkom også i resultatene. Utfordringen er om det ikke håndteres som en krise, men så viser det seg at hendelsen utvikler seg til å bli det. Cyberhendelser kan kjennetegnes som perioder av langsom utvikling kombinert med perioder med rask eskalering og uforutsigbarhet. Dersom det ikke er trent på og etablert gode fundamentale prosesser for hvordan håndtere hendelser i cyberdomenet kan dette svekke samvirke fra taktisk til strategisk nivå. Dersom en hendelse blir en bekymring på strategisk nivå, vil det skje en endring i mandater og en allokering av ressurser som vil kunne bidra til å dra ned konsekvensene av hendelsen. Med bakgrunn i at cyberdomenet ikke er geografisk bundet gjør at det er helt nødvendig å varsle det videre opp i virksomheten. Da hendelsen kan ha konsekvenser for andre virksomheter utover en selv. Det handler nødvendigvis ikke om en cyberhendelser kalles for en krise eller ei. Det som betyr noe for den faktiske håndteringen vil være fremgangsmåten som er etablert for hvordan man skal gripe fatt i problematikken. Å få til et godt samvirke på tvers

av virksomheter er helt nødvendig både i hendelseshåndtering og i et langsiktig forebyggende perspektiv for å fremme god cybersikkerhet.

Oppsummering

Resultatene og analysen fra dokumentstudier og intervjudata demonstrerte betydningen av samvirke i forebygging og håndtering av cyberhendelser. Kompleksiteten i aktørnettverket og det faktum at cyberhendelser kan treffe bredt skaper usikkerhet og gjør det utfordrende å definere systemet. Prioritering og fundamentale prosesser sees på som hensiktsmessig når en skal bukte med kompleksitet, der cyberangrep er konstante og stadig endres. Ser man forskningsspørsmål én i sammenheng med forskningsspørsmål to fremkommer det at det å etablere relasjon og nettverk i en tidlig fase er hensiktsmessig under håndtering av cyberhendelser. Dette underbygges også av andre studier referert til i avsnitt 4.2.2 kommunikasjon i teorikapittelet.

6.3 I hvilken grad oppnås samvirke i planlegging og gjennomføring av Cyber22?

Samvirke lar seg vanskelig måle kvantitativt, men kan vurderes ut fra en kvalitativ evaluering. Basert på resultatene vurderes samvirke i den sammenheng på bakgrunn av analysen som er gjort av samvirke-konseptet som følge av teori og analyse av resultatene. I beredskapsøvelsen Cyber22 er samvirke operasjonalisert i hele prosessen.

Denne studien viste at planleggingsfasen til Cyber22 var vesentlig for å fremme samvirke. Det var i planleggingsfasen grunnlaget for å oppnå hovedmål om økt samvirke før øvelsen ble lagt. Dette viser at planleggingen er vel så viktig som gjennomføringen. Om ikke viktigere, fordi det er selve forutsetningen for å skape læring og trening i gjennomføring av øvelsen. Samvirke er en systemegenskap som produseres gjennom interaksjoner i systemet. Dermed blir det ikke noe tydelig skille mellom planleggings- og gjennomføringsfasen. Man samvirker alltid, og øvelsen blir et verktøy for å få til bedre samvirke etter øvelsen. Cyber-resiliens fremmes blant annet gjennom en *praktiserende* dimensjon (Dupont, 2019). I lys av denne teorien kan planlegging av øvelsen ha bidratt til å øke kapasitet og styrket mellommenneskelige relasjoner, både for det interne samvirke i organisasjonen og det eksterne samvirke tvers av virksomheter. Involvering av både interne og eksterne deltakere fremstår som fundamentet i prosessen. En svakhet ved studien er at man gjerne skulle hatt intervjudata fra de eksterne deltakerne for å få en enda bredere kunnskap om deres opplevelse av samvirke. På den andre siden fikk en gjennom

observasjon av evalueringen en konsis tilbakemelding fra de eksterne deltakerne. Hovedmålet samvirke oppnås også i planleggingsprosessen av øvelsen. Plangruppen virker å forstå beredskap som *muliggjørende (*Delgado og Kruke, 2017) som innebærer at de ikke bare har fokus på en effektiv respons, men også fokus på å oppnå resiliens i planlegging, før og i gjenoppretting av en cyberhendelse. Det fremstår også som de ser på en krise som noe som ikke plutselig inntreffer, men som en hendelse som kan forebygges. Fokuset plangruppen hadde på samvirke førte også til den innovative tilnærmingen til interessentanalysen i utforming av den visuelle samvirkeanalysen. Gjensidige avhengigheter og flere interessenter i sektoren førte til et behov for å kartlegge disse. For at den visuelle samvirkeanalysen skal nyttiggjøre seg er det nødvendig at det settes inn en kontrollfunksjon slik at NB kan oppdatere oversikten i sanntid. Dette forutsetter at det legges til en tilbakemeldingsfunksjon. Ved forutsetningen for at samhandlingslinjene vurderes til grønn, bør en jevnlig evaluere disse. En anbefaling er å etablere en praksis som gjør at man i sanntid vedlikeholder analysen. I lys av teorien kan analysen også forstås som et verktøy for å øke systemforståelsen. Resultatene viste også at den fungerte som et praktisk verktøy, da den ble brukt for å få oversikt i håndteringen under øvelsen.

Det sies at beredskap er aktivt, og dermed vil graden av trening og øvelser som involveres i forberedelsen kunne være avgjørende for beredskapen (Delgado og Kruke, 2017). Der mangel på aktivitet i dimensjoneringen fører til at rammeverk foreldes. Utfordringen med planlegging av fullskalaøvelser er at er det både tidskrevende og kostbart å gjennomføre. Det er utfordringer som kan knyttes til den *omstridte* dimensjonen i cyber-resiliens (Dupont, 2019). På bakgrunn av NB har bevilget både økonomiske og menneskelige ressurser i Cyber22, tolkes det at det er en felles risikoforståelse blant ledere og medarbeidere i organisasjonen. I prosessen av planlegging og gjennomføring av øvelsen har både ledere og medarbeidere i organisasjonen fått en økt felles forståelse av risiko som igjen har ført til revidering av plan- og rammeverk. Det fremstår av resultatene at NB har fokus på resiliens og økt tilpasnings evne. Deltakerne opplevde øvelsen som relevant, der samvirke ble godt trent gjennom kommunikasjon i samhandlingslinjene. Det at deltakerne opplevde usikkerhet og tidspress i øvelsen er et viktig moment og viser at øvelsen var godt planlagt (Engen et al., 2016). Dette kan ansees å gi god trening både på å håndtere stress og for å teste om kriseorganisasjonen er robust.

Under øvelsen Cyber22 dreiet mye av kommunikasjonen seg om samvirke med media. Det var vanskelig i observasjon å fastslå hvilken rolle media har i finanssystemet. Spørsmålet en kan stille seg er om de er en del av systemet, eller en del av omgivelsene til systemet. Det at de

inkluderes i øvelsen kan tilsi at de anerkjennes i større grad som en del av systemet. En finansorganisasjons som NB er avhengig av befolkningens tillit til den finansielle infrastrukturen og betalingssystemene. Dermed er omdømmet viktig i håndteringen av en cyberhendelse. I et samvirkeperspektiv oppleves media som sentral i samvirke, der medieovervåkning fremstår som viktig for alle deltakerne i øvelsen. I resultatene fremkom det at prosess knyttet til samarbeidet om mediehåndtering på operasjonelt og strategisk nivå har forbedringspotensial. I lys av dette kan en anbefaling til NB være å avklare media sin rolle i systemet og undersøke om det er noen forbedringspunkter i prosessen for hvordan en får ut informasjonen.

Spillutviklingen i øvelsen fremstod som en lineær prosess. Dette kom frem i resultatene der det ble påpekt at etterhvert som NB fikk oversikt over hendelsen oppstod det ikke nye problemer underveis. Det kan også fremstå fra informantenes perspektiv at øvelsen var lagt opp til å teste utvalgte prosedyrer. Dette forstås som å være et bevisst valg av plangruppen, på samme måte som at de bevisst var åpne om konsekvensbilde i forkant av øvelsen. Engen et al., (2016) peker på *gjenkjenning* som bidrag til at øvingsdeltakerne opplever mestringsfølelse. Mestring har vært et fokus fordi plangruppen ønsket å skape en vilje hos deltakerne til å gjenta det. I tillegg argumenterer plangruppen med at NB ikke er en beredskapsinstitusjon, og dermed ønsket de å skape gode opplevelser knyttet til det å øve.

På bakgrunn av at spillutvikling fremstod som lineær kan en diskutere om det tillot deltakerne nok improvisasjon. I lys av tidligere hendelser som utfordret samvirke, kan en hevde når samvirke virkelig slår inn er det foruten om prosedyrene. Samvirke skal bidra til å kunne håndtere komplekse fenomener, nye situasjoner eller et overveldende arbeidspress. Å tillate improvisasjon i mobiliseringen slik at samvirke oppleves som en felles bekjempelse av trusselen, kan sees på som et viktig læringspunkt når virksomheter skal teste samvirke fullt ut. Øvelsens hensikt var å ivareta samvirke mellom relevante aktører. Det vil være naturlig å spørre på hvilken måte det er sammenheng mellom øvelsens hensikt og øvelsens design. På en annen side har de vært bevisste i valgene i utforming av øvelsen Cyber22. Dette har vært et naturlig steg fra NB sin side. Det å kaste deltakerne i et sort hull som en av informantene påpekte er ikke hensiktsmessig når mestring og vilje til å øve er fordelaktig for beredskapsarbeidet i et lenger tidsperspektiv. Øvelsen danner grunnlaget for mer samhandling, som igjen bidrar til at man øver på mer komplekse scenarioer senere.

Oppsummering

Ved å arrangere en sektorøvelse med interne og eksterne aktører legges det til rette for å øve på samvirke. Aktørene involveres både i planleggingen og som deltakere i gjennomføringen av øvelsen. Kartlegging av samvirke har vært viktig i presisering av hvem NB anser å være interessenter i hendelsesscenarioet. Ved å etablere relasjoner på tvers av virksomheter, og ved å gjennomføre en øvelse har NB etablert et system som definerer hvem NB er avhengig av å samvirke med i det scenarioet som presenteres i øvelsen. Under øvelsen får deltakerne testet kommunikasjonslinjer, verktøy og metoder som skal støtte opp under koordinering og kommunikasjon i håndteringen. Ved å gjøre dette får deltakerne en opplevelse av hva som fungerer bra og hva som fungerer mindre bra i samvirke. Blant annet kom det frem av resultatene fra observasjon og intervju etter øvelsen, at krisekommunikasjon via media er viktige i et samvirkeperspektiv. Øvelsen er designet for å skape mestringsfølelse hos deltakerne. Dette er et bevisst valg av øvingsledelsen for å styrke beredskapen i organisasjonen i et langsiktig perspektiv.

7. Konklusjon

I dette kapittelet vil følgende problemstilling bli besvart:

> ***På hvilken måte operasjonaliseres samvirke i planprosess og gjennomføring av beredskapsøvelsen Cyber22, og hvilken innsikt gir dette i samvirke som strategi for cyber-beredskap?***

Denne studien har vist at arbeidet med intensivering av samvirke står helt sentralt i forebygging og håndtering av cyberhendelser. Dette har bakgrunn i sårbarheter som kommer av gjensidige avhengigheter i sosio-tekniske systemer. For å håndtere den dynamiske og grenseoverskridende trusselen cyberangrep kan karakteriseres som, er man avhengig av et samarbeid i lang tid før en hendelse inntreffer. Deteksjon, varsling og informasjonsdeling til myndigheter er nødvendig for å kunne forebygge og minimere konsekvensene av cyberangrep. Et dypdykk i samvirke-konseptet har vist at man kan konkretisere og beskrive samvirke, og derav peke på faktorer som både styrker og hemmer et samvirke. Oppgavens konstruktivistiske perspektiv kombinert med teorigrunnlaget om cyber-resiliens og sikkerhetssystemteoretisk betraktninger, har vært veiledende for hvordan jeg har tolket datamaterialet og til slutt konseptualisert samvirke. Sammenfatningen av datamaterialet om samvirke viste at teori, dokumentstudier og intervjudata fra informantene var sammenfallende. Selv om teorigrunnlaget og dokumentstudier kunne peke i en retning i samvirke-konseptet, var det likevel intervjudata av informantene som i større grad ga en fullstendig beskrivelse.

Konseptbeskrivelsen og funn fra informantenes operasjonalisering av samvirke i Cyber22 ga noen konkrete punkter på hvordan man kan intensivere samvirke. Samvirke operasjonaliseres på flere områder før og under Cyber22. De mest fremtredende funnene knyttet til operasjonalisering av samvirke er forhåndsetablering av relasjoner, gjennomgang av den visuelle samvirkeanalysen, involvering av eksterne deltakere og betydningen av krisekommunikasjon via media. På bakgrunn av at Cyber22 er den første fullskala beredskapsøvelsen for finanssektoren, var det hensiktsmessig å fokusere på mestringsfølelsen hos deltakerne, fremfor å teste deltakernes evne til improvisasjon og fleksibilitet. En kan konkludere med at økt mestring hos deltakerne er viktig i et lengre perspektiv når fremtidige øvelser skal gjennomføres. I tabell 5 oppsummeres sentrale aspekter med samvirke og hvordan disse ble operasjonalisert i Cyber22. I planlegging og gjennomføring av øvelsen ble samvirke demonstrert som en strategi for å håndtere cyberhendelser i finanssektoren. Samvirke foregår

hele tiden, både før, under og etter øvelsen. Det er elementene i operasjonaliseringen av samvirke som er nyttige å se på når en skal svare på «...hvilken innsikt gir dette i samvirke som strategi for cyber-beredskap?» Dersom samvirke skal være en strategi for å forebygge og håndtere cyberhendelser er det nødvendig at aktører evaluerer og kartlegger det interne og eksterne samvirke, slik det ble gjort i Cyber22. Å sette inn konkrete tiltak rettet mot samvirke kan bidra som en strategi for cyber-beredskap. Tiltak oversettes i denne oppgaven til operasjonalisering av samvirke (se tabell 6).

Tabell 6: Operasjonalisering av samvirke

Aspekter ved samvirke	Operasjonalisering av samvirke
Kommunikasjon, Informasjonsdeling Felles situasjonsforståelse	- Oppdaterte varslingslister og kommunikasjonslinjer - Samordningsforum - IKT-kompetanse i kriseledelsen - Kunnskapsutvekling og seminarer - Samhandlingsforum - Bruken av krisehåndteringsverktøy og andre digitale verktøy for kommunikasjon - Fokus på krisekommunikasjon via media
Koordinering	- Proaktiv metode i hendelseshåndtering - Etablere koordinator-rollen i operasjonell og strategisk krisestab - Samordningsforum - Den visuelle samvirkeanalysen
Forhåndsetablerte relasjoner	- Involvering av eksterne deltakere i øvelsen Cyber22. - Seminarer og workshops - Den visuelle samvirkeanalysen
Kompetanse Rolleforståelse	- Kunnskapsutveksling - Seminarer og workshops - Trening gjennom den visuelle samvirkeanalysen - Evaluering av øvelsen

7.1 Forslag til videre forskning

Denne oppgaven har vært avgrenset til å se på hvordan NB har anvendt samvirke i planlegging og gjennomføring av Cyber22. Det ville vært interessant å studere samvirke i andre sektorer og miljøer. Det for å kunne vurdere om de har samme tolkninger av konseptet, og hvordan andre aktører etterlever samvirke-prinsippet i krisehåndtering. Det trengs også mer forskning på sammenhengen mellom testing av samvirke i øvelser og hvordan samvirkeøvelser gir økt læring. I denne studien har jeg fått innsikt i dimensjonering av beredskapsøvelser. Det ville vært svært interessant å undersøke nærmere hvordan en skal dimensjonere fullskalaøvelser med et cyberscenario for å oppnå læring på alle nivåene i kriseorganisasjonen. Funn fra denne studien viste også betydningen av krisekommunikasjon via media. En interessant vinkling på en fremtidig studie ville vært å undersøke hvilke innvirkning media og kommunikasjon har på situasjonsforståelsen hos ulike aktører i en hendelse.

Litteraturliste

Aasland, T., & Braut, G. S. (2018). Ressursene som finner hverandre: Samvirke – lokal arbeidsform eller sentralt styringsprinsipp? *Heimen (Oslo, Norway), 55*(2), 178-197. https://doi.org/10.18261/issn.1894-3195-2018-02-06

Atkins, S., & Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity, 7*(1). https://doi.org/10.1093/cybsec/tyab024

Backman, S. (2021). Conceptualizing cyber crises. *Journal of contingencies and crisis management, 29*(4), 429-438. https://doi.org/10.1111/1468-5973.12347

Bartnes, M., & Moe, N. B. (2017). Challenges in IT security preparedness exercises: A case study. *Computers & security, 67*, 280-290. https://doi.org/10.1016/j.cose.2016.11.017

Betalingssystemloven. (1999). Lov om betalingssystem (LOV-1999-12-17-95). Hentet fra https://lovdata.no/dokument/NL/lov/1999-12-17-95

Blaikie, & Priest, J. (2019). *Designing social research: the logic of anticipation* (3rd edition.). Polity Press.

Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of contingencies and crisis management, 15*(1), 50-59. https://doi.org/10.1111/j.1468-5973.2007.00504.x

Caspari, C. B. (2021). *Norges forståelse av hybride trusler: Effekten av ulike konseptualiseringer på myndighetenes samarbeid.* [Masteroppgave, Universitetet i Stavanger] https://uis.brage.unit.no/uis-xmlui/handle/11250/2835861

Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public administration review*, *67*, 189-197.

Dalland. (2017). *Metode og oppgaveskriving* (6. utg., p. 267). Gyldendal akademisk

Denzin, N. K. (2012). Triangulation 2.0. *Journal of mixed methods research, 6*(2), 80-88. https://doi.org/10.1177/1558689812437186

Det Norske Akademi for Språk og litteratur. (2022, 14.januar). *Finanssektor.* NAOB. https://naob.no/ordbok/finanssektor

Deloitte. (2022). Ny sikkerhetslov og NIS-direktivet. Hentet 19.januar 2022 fra: https://www2.deloitte.com/no/no/pages/legal/articles/sikkerhetslov-januar-2019.html

Department of Financial Services. (2021, 27. April). *Report on the SolarWinds Cyber Espionage Attack and Institutions' Response.* The New York Department of Financial Services. https://dfs.ny.gov/search/site?search=solarwinds

Departementene. (2019). *Nasjonal strategi for digital sikkerhet*. Regjeringen. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

Direktoratet for samfunnssikkerhet og beredskap (DSB). (u.å.). *Øvelse Digital 2020.* https://www.dsb.no/reportasjearkiv/ovelse-digital-2020/

Direktoratet for samfunnssikkerhet og beredskap (DSB). (2016). Samfunnets kritiske funksjoner. *Hvilken funksjonsevne må samfunnet opprettholde til enhver tid? https://www.dsb.no/rapporter-og-evalueringer/samfunnets-kritiske-funksjoner/*

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity, 5*(1), tyz013.

Dynes, R. R. (1993). Disaster reduction: The importance of adequate assumptions about social organization. *Sociological spectrum, 13*(1), 175-192. https://doi.org/10.1080/02732173.1993.9982022

Edmondson, A. C. (1999). Psychological Safety and Learning Behavior in Work Teams. *Administrative Science Quarterly, 44*(2), 350-383. https://doi.org/10.2307/2666999

Engen O. A., Kruke I. B., Lindøe H. P., Olsen H., K., Olsen E. O., & Pettersen A. K. (2016) *Perspektiver på samfunnssikkerhet.* Cappelen Damm Akademisk.
Eriksen J., Rake L. E., & Sommer M. (2021) *Beredskapsanalyse.* Cappelen Damm Akademisk.
European central bank. (2018). TIBER-EU Framework. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
Finanstilsynet. (2021, 1.mars). *Årsrapport fra Beredskapsutvalget for finansiell infrastruktur 2020.* https://www.finanstilsynet.no/tema/beredskapsutvalget-for-finansiell-infrastruktur- bfi/arsrapporter-fra-bfi/
Finansdepartementet. (2020a, 28.januar). *Beredskap i den finansielle infrastrukturen.* Regjeringen. https://www.regjeringen.no/no/tema/okonomi-og-budsjett/finansmarkedene/beredskap/id2353825/
Finansdepartementet. (2019a). *Norges Bank.* https://www.regjeringen.no/no/dep/fin/org/underliggende_etater/norges-bank/id213276/
Finans Norge. (2019, 21.mars). Nordic Financial CERT: Finansnæringens forsvar mot dataangrep. https://www.finansnorge.no/aktuelt/nyheter/2019/03/nordic-financial-cert-finansnaringens-forsvar-mot-dataangrep/
Flyvbjerg. (2006). Five Misunderstandings About Case-Study Research. *Qualitative Inquiry*, *12*(2), 219–245. https://doi.org/10.1177/1077800405284363
Forsvarsdepartementet. (2016). *Lov om nasjonal sikkerhet (sikkerhetsloven).* (Prop. 135 L (2016-2017)). https://www.regjeringen.no/no/dokumenter/prop.-153-l-2016-2017/id2556988/?ch=1
Garmezy, Norman (1973) Competence and adaptation in adult schizophrenic patients and children at risk. I S.R. Dean (red.) *Schizophrenia: The first ten Dean Award Lectures* (163–204). New York: MSS Information Corp.
Grønmo. (2016). Samfunnsvitenskapelige metoder (2. utg., p. 462). Fagbokforl.
Holling, C. S. (1973) Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, (4): 1–23
IKT-forskriften. (2003). Forskrift om informasjons og kommunikasjonsteknologi (FOR-2015-12- 17-1732). Hentet fra: https://lovdata.no/dokument/SF/forskrift/2003-05-21-630
Jacobsen. (2015). *Hvordan gjennomføre undersøkelser? : innføring i samfunnsvitenskapelig metode* (3. utg., p. 432). Cappelen Damm akademisk.
Johannessen, A., Christoffersen, L. & Tufte, P. A. (2016). *Introduksjon til samfunnsvitenskapelig metode* (5. utg.). Abstrakt.
Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity, 7*(1). https://doi.org/10.1093/cybsec/tyab005
Korolov, M. (2021, 4. februar). Supply chain attacks show why you should be wary of third-party providers. *CSO.* https://www.csoonline.com/article/3191947/supply-chain-attacks- show-why-you-should-be-wary-of-third-party-providers.html
Kristensen, H. (2016, 14.juni). *High reliability organizations i petroleumsindustrien – finner vi teorien igjen i praksis?* [Masteroppgave, Universitetet i Stavanger] https://uis.brage.unit.no/uis-xmlui/handle/11250/2411872
Leveson, N.G. (2011). *Engineering a Safer World*, Mit Press.
Lunde K. I. (2019). *Praktisk krise- og beredskapsledelse*. Universitetsforlaget.

Lysne O. (2020, 14. februar). *Et brutalt urovekkende cyberangrep. Nå haster det!* Aftenposten. https://www.aftenposten.no/meninger/debatt/i/aP44nE/et-brutalt-urovekkende-cyberangrep- naa-haster-det

Mareile Kaufmann. (2013). Cyber-resiliens i EU. *Internasjonal politikk*, *71*(2), 274–283.

Martin, P. (2019). *The rules of security: staying safe in a risky world*. Oxford University Press.

Meld. St. 31 (2020-2021). *Finansmarkedsmeldingen 2021.* Finansdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-31-20202021/id2845705/?ch=1

Meld. St. 5 (2020-2021). *Samfunnssikkerhet i en usikker verden.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-5-20202021/id2770928/

Meld. St. 10 (2016-2017). Risiko i et trygt samfunn. *Samfunnssikkerhet.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/

Meld. St. 38. (2016 - 2017). *IKT-sikkerhet - Et felles ansvar.* Det kongelige Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/?ch=1

Meld. St. 29 (2011-2012). *Samfunnssikkerhet.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld-st-29-20112012/id685578/?ch=1

Meld. St..7 (2001–2002). *Om helse, miljø og sikkerhet i petroleumsvirksomheten.* Arbeids- og inkluderingsdepartementet. https://www.regjeringen.no/no/dokumenter/stmeld-nr-7-2001-2002-/id134387/sec9?q=

Nasjonal Sikkerhetsmyndighet. (2022) *Risiko 2022. Økt risiko krever økt årvåkenhet*. https://nsm.no/regelverk-og-hjelp/rapporter/

Nasjonal Sikkerhetsmyndighet. (2021). *Risiko 2021: Helhetlig sikring mot sammensatte trusler.* Hentet fra: https://nsm.no/aktuelt/risiko-2021-helhetlig-sikring-mot-sammensatte- trusler

Nasjonal Sikkerhetsmyndighet. (2018). *Et sikkert digitalt Norge – IKT-risikobilde 2018*. Hentet fra https://www.nsm.stat.no/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf

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

Norges Bank. (2021a). Strategi 2022. *https://www.norges-bank.no/tema/Om-Norges-Bank/samfunnsoppdrag/*

Norges Bank. (2021b). Finansiell stabilitet 2021: *Sårbarhet og risiko*. https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Finansiell-stabilitet---rapport/?tab=null&newstype=0&year=0

Norges Bank. (2021c). Det norske finansielle system 2021 *– en oversikt.* https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/det-norske-finansielle-systemet/2021-dnfs/

Norges Bank. (2021d). Finansiell infrastruktur 2021. https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Finansiell-infrastruktur---rapport/finansiell-infrastruktur-2021/

Norges Bank. (2020a). *Finansiell infrastruktur.* (ISSN 1894-8316). https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Finansiell-infrastruktur---rapport/finansiell-infrastruktur-2020/

Norges Bank. (2020b). *Årsrapport NBO 2020.* https://www.norges-bank.no/tema/Norges- Banks-oppgjorssystem/Arsrapporter-NBO/
Norges Bank. (2020c). Finansiell stabilitet 2020: *Sårbarhet og risiko* https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Finansiell-stabilitet---rapport/?tab=null&newstype=0&year=0
Norges Bank. (2020d). Norges Banks oppgjørssystem. *Egenvurdering mot internasjonale prinsipper for finansiell infrastruktur.*
Norges Bank. (2019a). Finansiell stabilitet 2019: *Sårbarhet og risiko*. https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Finansiell-stabilitet---rapport/?tab=null&newstype=0&year=0
Norges Bank. (2018). Finansiell stabilitet 2018: *Sårbarhet og risiko*. https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Finansiell-stabilitet---rapport/?tab=null&newstype=0&year=0
Norges Bank. (2017). Finansiell stabilitet 2017: *Sårbarhet og risiko*. https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Finansiell-stabilitet---rapport/?tab=null&newstype=0&year=0
Norges Bank. (2009, 4.mai). *Oppgjørssystemet – hovedfunksjoner.* https://www.norges-bank.no/tema/Norges-Banks-oppgjorssystem/Hovedfunksjoner-i-NBO/
NOU 2019: 13. (2019). *Når krisen inntreffer.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2019-13/id2654109/?ch=1
NOU 2018: 14. (2018). *IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/
NOU 2016: 19. (2016). Samhandling for sikkerhet — Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid. Forsvarsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/?ch=1
NOU 2015: 13. (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/
NOU 2012: 14. (2012). *Rapport fra 22.juli-kommisjonen.* Statsministerens kontor. https://www.regjeringen.no/no/dokumenter/nou-2012-14/id697260/?ch=1
Oxford Academic. (2022). Journal of Cybersecurity – About the journal. Hentet 18.februar 2022: https://academic.oup.com/cybersecurity/pages/About
Perrow, C. (1999). Normal accidents: Living with high-risk technologies. Princeton University Press.
Perry, R. W., & Lindell, M. K. (2003). Preparedness for emergency response: Guidelines for the emergency planning process. Disasters, 27(4), 336–350. Politiets sikkerhetstjeneste. (2022). *Nasjonal trusselvurdering 2022*. https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2022/
Phillips, & Austad. (2021). *Politiets rolle i deteksjonen av sammensatte trusler*. Politihøgskolen. https://hdl.handle.net/11250/2780592
Politidirektoratet. (2020). PBS I. Politiets beredskapssystem del I. *Retningslinjer for politiets beredskap.* https://www.politiet.no/rad/beredskap/
Regjeringen. (2020, 10.desember). Forslag til forordning om digital operasjonell motstandsdyktighet i finanssektoren. *https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2020/des/forslag-til-forordning-om-digital-operasjonell-motstandsdyktighet-i-finanssektoren/id2791266/*

Sagabraaten, M.O. (2019). «Den tryggheten er alfa omega. Alt for å kunne lykkes med noe.» *En kvalitativ studie om psykologisk trygghet og teamlæring.* Universitetet i Oslo. https://www.duo.uio.no/handle/10852/70094

Sentralbankloven. (2019). Lov om Norges Bank og pengevesenet mv. (LOV-2019-06-21-31). Hentet fra: https://lovdata.no/dokument/NL/lov/2019-06-21-31?q=sentralbankloven

Sikkerhetsloven. (2019). Lov om nasjonal sikkerhet (LOV-2018-06-01-24). https://lovdata.no/dokument/NL/lov/2018-06-01-24

Sommer, M., Pollestad, B., & Steinnes, T. (2020). *Beredskapsøving og -læring* (1. utgave. ed.). Fagbokforlaget. Stortinget. (2021, 21.januar). *Forslag til nytt cybersikkerhetsdirektiv.* https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/EU-EOS-informasjon/EU-EOS-nytt/2021/eueos-nytt---21.-januar-2021/forslag-til-nytt-cybersikkerhetsdirektiv/

Thagaard, T. (2018). *Systematikk og innlevelse : en innføring i kvalitative metoder* (5. utg. ed.). Fagbokforl.

Tierney, K., Lindell, M. K., & Perry, R. W. (2001). Facing the unexpected: Disaster preparedness and response in the United States. Washington, D.C.: Joseph Henry Press.

Tisdale, SM. Cybersecurity: challenges from a systems, complexity, knowledge management and business intelligence perspective. Issues Infor Syst 2015; 16:191–8.

Trimintzios, P., Holfeldt, R., Koraeus, M., Uckan, B., Gavrila, R., & Makrodimitris, G. (2014). *Report on Cyber Crisis Cooperation and Management: Comparative study on the cyber crisis management and the general crisis management*. https://doi.org/10.2824/34669

Tora, A., & Geir Sverre, B. (2018). Ressursene som finner hverandre. *Heimen (Oslo, Norway)* (2), 178-197. https://doi.org/10.18261/issn.1894-3195-2018-02-06

Rosenthal, U., Charles, M. M., & 't Hart, P. (Eds.) (1989). Coping with crises: The management of disasters, riots and terrorism. Charles C. Thomas.

Von Bertalanffy, L. (2010). General Systems Theory. *The Science of Synthesis: Exploring the Social Implications of General Systems Theory, 103*.

Weick, K. E. & Sutcliffe, K. M. (2007). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. (2. utg.). John Wiley & Sons, Inc. https://www-researchgate-net.ezproxy.uis.no/publication/265106124_Managing_the_Unexpected_Resilient_Performance_in_an_Age_of_Uncertainty

Yin. (2013). Validity and generalization in future case study evaluations. *Evaluation (London, England. 1995)*, *19*(3), 321–332. https://doi.org/10.1177/1356389013497081

Young, W., & Leveson, N. G. (2014). Inside Risks An Integrated Approach to Safety and Security Based on Systems Theory. *Communications of the ACM*, *57*(2), 31–35. https://doi.org/10.1145/2556938

Young, W., & Leveson, N. G. (2013, December). Systems thinking for safety and security. In *Proceedings of the 29th Annual Computer Security Applications Conference* (pp. 1-8).

Vedlegg

Vedlegg 1: Intervjuguide

Intervjuguide

Del 1: Introduksjonsspørsmål

1. Kan du fortelle om din funksjon i det daglige, funksjon i planlegging av øvelsen og funksjon under øvelsen?

Del 2: Samvirke og cybersikkerhet

1. Hva legger du i begrepet/konseptet cybersikkerhet?
2. Kan du fortelle om hvordan man jobber med cybersikkerhet i førkrisefasen?
3. Hva legger du i begrepet/konseptet samvirke?
4. Finnes det noen kriterier for et godt samvirke?
5. Hva tenker du kjennetegner et godt samvirke under håndtering av en cyberhendelse?

Del 3: Planprosess

1. Kan du beskrive planprosessen for Cyber22?
2. Hvordan ble/blir kriterier for samvirke inkludert i planprosessen og øvelsen Cyber22?
3. Hvordan har man involvert andre relevante aktører i planprosessen?
4. Hva kan andre aktører tilby av ressurser som er relevante for å håndtere en cyberhendelse?

Del 4: Øvelsen Cyber22

1. Hva innebærer en beredskapsøvelse for cyberangrep i finanssektoren?
2. Kan du forsøke å beskrive ansvarsforholdene til de ulike deltakerne i øvelsen, slik det fremstår før øvelsen?
3. I hvilken grad og hvordan blir samvirke testet under øvelse Cyber22?
4. Hva skiller samhandling under beredskapsøvelser for cyberangrep fra samhandling under andre typer beredskapsøvelser?
5. Hvilke erfaringer har man med samhandling fra tidligere cyberøvelser i finanssektoren?
6. På hvilken måte kan øvelse Cyber22 og evaluering etter øvelsen forbedre samvirke og beredskapen i sektoren?

Vedlegg 2: Meldeskjema for behandling av personopplysninger

742841

Cybersikkerhet i finanssektoren: En studie av samvirke i planlegging og gjennomføring av beredskapsøvelsen Cyber22.

Universitetet i Stavanger / Det teknisk- naturvitenskapelige fakultet / Institutt for sikkerheit, økonomi og planlegging

Henrik Bjelland

Ingrid Høiland

01.01.2022 - 01.08.2022

Meldeskjema

19.01.2022 Standard

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 19.01.2022. Behandlingen kan starte.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 01.08.2022.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake.

Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
Personverntjenester vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

• lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
• formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
• dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
• lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), og dataportabilitet (art. 20).

Personverntjenester vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.
Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER

Vedlegg 3: Informasjonsskriv med samtykkeerklæring for intervju

Forespørsel om deltakelse i forskningsprosjekt

«Operasjonalisering av samvirke i beredskapsøvelsen Cyber22»

Bakgrunn

Jeg er masterstudent ved Universitet i Stavanger og holder på med den avsluttende masteroppgaven av mitt studie innen samfunnssikkerhet. I denne forbindelsen ønsker jeg å undersøke hvordan samhandling operasjonaliseres i tilknytning til øvelsen Cyber22.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Stavanger er ansvarlig for prosjektet.

Hva innebærer deltakelse i studien?

Jeg ønsker å intervjue aktører som er deltakende og involvert i både planprosessen og utførelse av øvelsen. Formålet er å bidra til mer kunnskap om betydningen av et godt samvirke, hvordan samhandling fungerer i gjennomføring av en praktisk øvelse og hvordan øvelsen er dimensjonert til å kunne gi relevant øving på samvirke for aktører i finanssektoren.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Alle opplysninger vil bli behandlet konfidensielt. Datamaterialet vil kun være tilgjengelig for student og veileder. Foretak og øvelsen som studeres vil bli presentert innledningsvis i oppgaven. I fremstillingen av observasjonsresultatene vil alle opplysninger bli anonymisert. For å sikre konfidensialitet vil deltakerne videre i oppgaven bli omtalt med koder som for eksempel «Foretak 1» eller «Informant 1». På denne måten sikres det at alle opplysninger bli behandlet anonymt. Prosjektet avsluttes 15.juni 2022, og da vil også alle observasjonsnotater bli slettet og makulert.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra *Universitetet i Stavanger* har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Universitetet i Stavanger ved Henrik Bjelland, e-post: henrik.bjelland@uis.no.

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 53 21 15 00.

Frivillig deltakelse

Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi grunn. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller velger å trekke deg. Dersom du har spørsmål til studien, ta kontakt med meg, Ingrid Høiland, på tlf. 97415811 eller 233995@uis.no / Ingr.hoiland@stud.uis.no.

Vedlegg 4: Beskrivelse av lovkrav og rammeverk

Hovedprinsipper i beredskapsarbeid

I Norge har man etablert fire grunnprinsipper i arbeidet med samfunnssikkerhet (Meld. St. 10, 2016-2017, s. 20).

1. *Ansvarsprinsippet som innebærer at den organisasjonen som har ansvar for et fagområde i en normalsituasjon, og har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området.*
2. *Likhetsprinsippet som betyr at den organisasjonen man operer med under kriser i utgangspunktet skal være mest lik den organisasjonen man har til daglig.*
3. *Nærhetsprinsippet som betyr at kriser organisatorisk skal håndteres på lavest mulig nivå.*
4. *Samvirkeprinsippet som betyr at myndigheter, virksomheter eller etater har et selvstendig ansvar for å sikre best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering.*
   (Meld. St. 10, 2016-2017, s. 20).

Som nevnt tidligere i oppgaven så søkes det i sikkerhetsloven å balansere ansvar- og samvirkeprinsippet. Dette ved at loven fastslår både behovet for et sentralt og tverrsektorielt samarbeid samtidig som ansvarsprinsippet for enhver sektor lovfestes. Videre sikrer loven at NSM (Nasjonal sikkerhetsmyndighet) har ansvaret for koordineringsoppgaver som for eksempel innebærer å legge til rette for informasjonsdeling (NOU 2018: 14, s. 34).

Sikkerhetsloven

I inngangen av 2019 tredde ny sikkerhetslov i kraft og opphevet med det sikkerhetsloven fra 1998. Det med bakgrunn i det endrede risiko og trusselbilde var det et behov for å utvide lovens virkeområde. Der den nå regulerer tjenester og infrastruktur av samfunnskritisk betydning (Deloitte, 2022). Formålet til loven er beskrevet i § 1-1 der det blant annet etter bokstav b sies at loven skal bidra til å forebygge, avdekke og motvirke sikkerhetstruende virksomhet (Sikkerhetsloven, 2019). Loven dekker dermed tilsiktede handlinger, men tar ikke for seg utilsiktede handlinger. I henhold til den opphevete sikkerhetslov var NBO innmeldt av Finansdepartementet som et skjermings objekt til Nasjonal

sikkerhetsmyndighet. Følge av ny sikkerhetslov skal et hvert departement for sitt område utpeke skjermingsverdige objekter og infrastruktur jf. § 7-1, andre ledd. Det antas dermed at NBO vil falle under ny sikkerhetslov (Norges Bank, 2020d, s. 7).

Sentralbankloven

Sentralbankloven (2019) regulerer NBs rolle og ansvar i den finansielle infrastrukturen. Formålet med loven er at sentralbankvirksomheten skal opprettholde en stabil pengeverdi, fremme stabilitet i det finansielle systemet og sikre et effektivt og sikkert betalingssystem jf. § 1-2, Sentralbankloven. Dette skal de gjøre ved å legge til rette for et stabilt og effektivt system for betaling, avregning og oppgjør mellom foretak med konto i banken. De skal også overvåke betalingssystemet og annen finansiell infrastruktur og bidra til beredskapsløsninger jf. § 3-3 pkt. 1 og 2 (Sentralbankloven, 2019).

Betalingssystemloven

Loven bygger på at finanssektoren har et ansvar for å dimensjonere robuste systemer, og at aktørene selv har ansvar for å ta hensyn til risiko og effektivitet ved drift av interbanksystemer (Direktoratet for samfunnssikkerhet og beredskap, 2016, s. 84). Etter betalingssystemloven (1999) har Finanstilsynet ansvar for tilsyn knyttet til de systemer for kunderettede betalingstjenester og systemer for verdipapiroppgjør, mens NB har konsesjons- og tilsynsmyndighet med interbanksystemene (Norges Bank, 2021d, s. 10). Etter § 1-1 defineres betalingssystemer som *«systemer for overføring av midler med formelle og standardiserte ordninger og felles regler for behandling, avregning eller oppgjør av betalingstransaksjoner»* (Betalingssystemloven, 1999). I et slikt system inngår interbanksystem eller systemer for betalingstjenester.

Gjennom lovverket stilles det krav til de aktører og deltakere som loven omfattes av etter § 1-3. Formålet beskrevet i § 2-1 er *«å bidra til at interbanksystemer organiseres slik at hensynet til finansiell stabilitet blir ivaretatt»*. Følgelig legges det vekt på *«å motvirke risiko som følge av likviditets- eller soliditetssvikt hos deltakere i slike systemer»* (Betalingssystemloven, 1999). NB omfattes ikke av kapittel 2, men legger likevel vekt på å følge de bestemmelsene som er relevante for NBO (Norges Bank, 2020d, s. 7). Loven tar videre for seg konsesjon, adgang, tilsyn og alminnelige systemkrav. Loven har som funksjon å sikre betalingssystemene og setter krav til brukere og operatør av systemene.

IKT-forskriften

IKT-forskriften (2003) er supplerende til betalingssystemloven og er en viktig del av sikkerhetsstyringen av finanssektoren. Finanstilsynet har med hjemmel i lov tilsynsansvar av finansinstitusjoner. Denne forskriften er gjeldende for alle norske finans- og bankvirksomheter i finanssektoren samt IKT-systemer som har betydning for foretakets virksomhet. Bestemmelsen i forskriften påser at virksomheter gjennomfører risikoanalyser og fastsetter kriterier for akseptabel risiko i forbindelse med bruk av IKT-systemene jf. § 3 (IKT-forskriften, 2003). I bestemmelsen § 5 *sikkerhet* skal virksomhetene utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon (IKT-forskriften, 2003). Videre stilles det krav til «skriftlige prosedyrer for anskaffelse, utvikling, videreutvikling og testing av IKT-systemer» jf. § 6 (IKT-forskriften, 2003). Det stilles også krav til hvordan IKT-systemene skal driftes, samt hvordan man skal håndtere avvik og hendelser i tilknytning til driften av IKT-systemene. Operasjonelle hendelser eller sikkerhetshendelser som medfører brudd på sikring av IKT-systemet skal rapporteres inn til finanstilsynet jf. § 9, 3.ledd (IKT-forskriften, 2003). NB omfattes heller ikke av denne forskriften, men følger også denne loven i tråd med god praksis for viktige IKT-systemer (Norges Bank, 2019d, s. 8).

TIBER-NO-rammeverket

I 2018 publiserte European central bank (ECB) rammeverket «Threat Intelligence-based Ethical Red Teaming (TIBER-EU). Rammeverket er utarbeidet for europeiske og andre nasjonaliteter for å kunne teste og forbedre finansiell infrastrukturs cyber-resiliens (European Central bank, s. 2). NB og Finanstilsynet har med utgangspunkt i dette rammeverket utarbeidet et forslag til rammeverk for å teste cybersikkerhet i bank- og betalingssystemer i Norge. Videre skal NB med et bemannet «TIBER Cyber Team» (TCT-NO) forvalte og operasjonalisere rammeverket. Dette innebærer et ansvar i å følge opp at kritiske funksjoner i at det finansielle systemet testes, og at testingen følger kravene til TIBER-NO. Rammeverket stiller krav til systematisk testing og innebærer testing av it-systemer, prosesser, beredskapsplaner og kompetanse. Det er kun noen få i foretaket som kjenner til testen, og testen skal dermed oppfattes som et reelt angrep (Norges Bank, 2021d, s. 19-20). 24.september 2020 ble det lagt inn forslag fra EU-kommisjonen angående ny lovgiving for digital operasjonell motstandsdyktighet (Digital Operational Resilience Act, DORA). Forslaget innebærer at man setter krav om nødvendige tiltak for å redusere

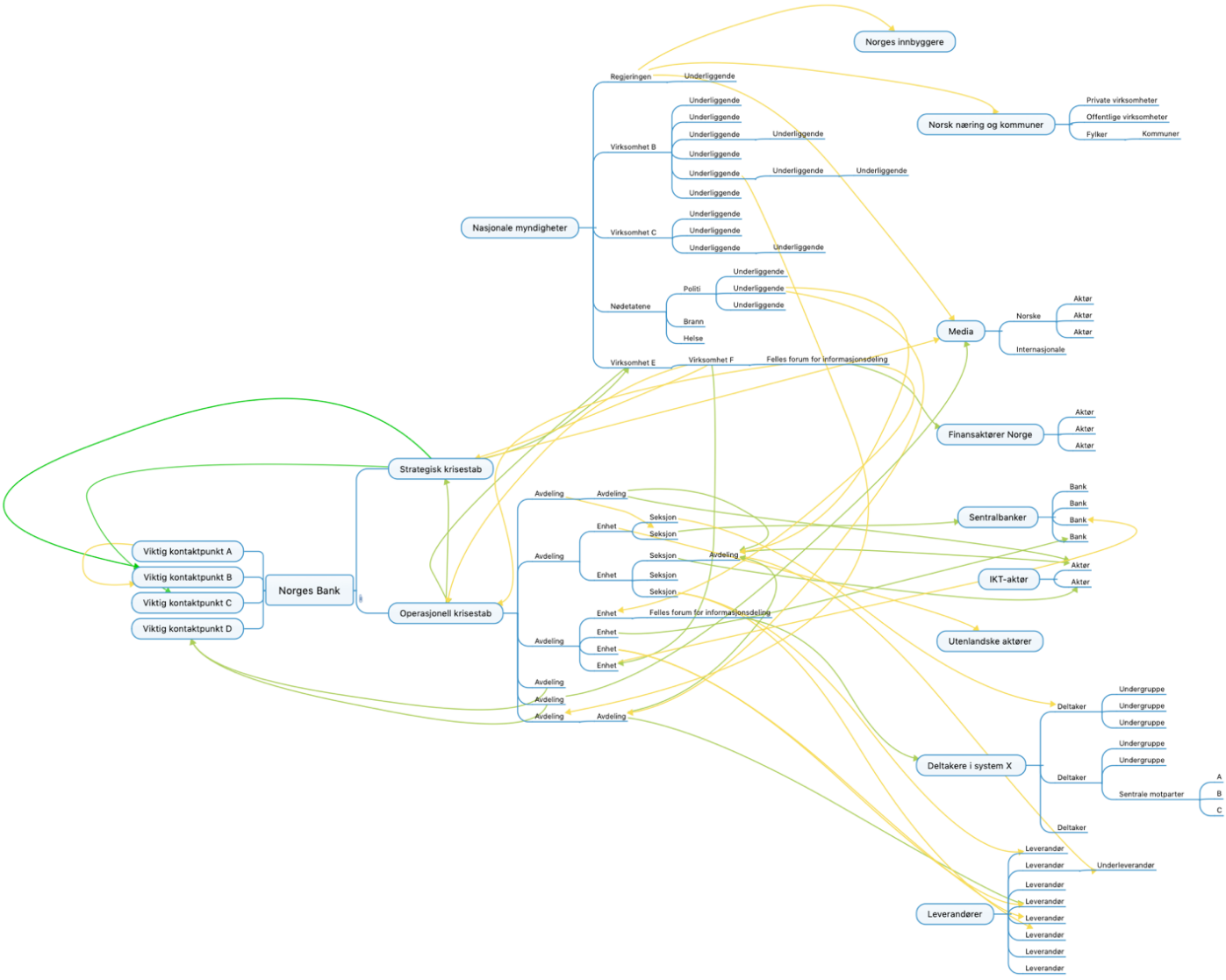
cyberangrep og andre risikoer for aktører og deltakere i det finansielle system. Det vil være krav om at alle foretak skal kunne håndtere alle type IKT-relaterte forstyrrelser og trusler. Som følge av DORA vil det også kunne komme endringer i TIBER-NO-rammeverket (Regjeringen, 2020; Norges Bank, 2021d, s. 21).

NIS 2-direktivet

Europakommisjonen foreslo i desember 2020 en revidert versjon av EUs cybersikkerhetsregler for kritiske sektorer og en ny cybersikkerhetsstrategi. Forslaget er en del av en styrket innsats for å hindre større datasikkerhetsbrudd og angrep fra aktører med støtte fra fremmede stater (Stortinget, 2021). Bakgrunnen i etablering av NIS-direktivet fra 2016 var at innen EU var det mangel på tilstrekkelig og helthetlige beskyttelsestiltak for å oppnå god cybersikkerhet i nettverk- og informasjonssystemer. Kravene er rettet mot virksomheter som leverer tjenester som er viktige for det indre markeds samfunnsmessige og økonomiske aktiviteter. Deriblant gjelder kravet for tilbydere av samfunnsviktige tjenester innen finanssektoren som bank, finansmarkedsinfrastruktur og digital infrastruktur (Meld. St. 5, 2020-2021, s. 86).

Vedlegg 5: Illustrasjon av den visuelle samvirkeanalyse

Figur 8 viser et illustrert eksempel av den visuelle samvirkeanalysen. Samhandlingslinjene i eksempelet er fiktive.



Figur 8: Den visuelle samvirkeanalysen av Norges Bank og Proactima.