Cyber-risiko i den norske finanssektor

Masterstudium i samfunnssikkerhet

Universitetet i Stavanger

Juni 2019

Alvhild Skjelvik

Universitetet
i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i samfunnssikkerhet	Vår 2019 Åpen
Forfatter: Alvhild Skjelvik	Alvhild Skjelvik *(Signatur forfatter)*

Fagansvarlig: Ole Andreas Hegland Engen

Veileder: Odd Einar Falnes Olsen

Tittel på masteroppgaven:

Cyber-risiko i den norske finanssektor

Engelsk tittel:

Cyber Risk in the Norwegian Financial Sector

Studiepoeng: 30

Emneord: Cybersikkerhet, cyber-risiko, cyber-fare, cyber-trusler, cyber-angrep, risiko og sårbarhet, risikostyring, risikoerkjennelse, betalingssystem, finanssektor, risikobilde, trusselbilde, utviklingstrekk, risikotilnærming og organisatoriske faktorer	Sidetall: 94 + vedlegg/annet: 119 Oslo 13. juni 2019

Forside for masteroppgave
Det teknisk-naturvitenskapelige fakultet

Forord

Gjennom denne oppgaven har jeg benyttet muligheten til å knytte samfunnssikkerhet opp mot et svært viktig og omfattende tema, nemlig cybersikkerhet. Kunnskapen jeg har tilegnet meg gjennom masterstudiet i Stavanger, gjør meg godt rustet for å møte en fremtid med nye og dynamiske sikkerhetsutfordringer – jeg gleder meg til å ta fatt på disse utfordringene!

Jeg vil rette en stor takk til alle som har bidratt til at denne oppgaven ble til. Takk til informantene som har bidratt til å gjøre denne oppgaven gjennomførbar. Deres kunnskap har vært uvurderlig. Takk til min fantastiske sjef Arleen Engeset for gode diskusjoner, gode innspill og god støtte gjennom denne hektiske perioden.

Tusen takk til professor og veileder Odd Einar Falnes Olsen for å ha holdt troen på en tidvis forvirret og meget stresset student. Selv om jeg har vært i tvil, har du alltid hatt troen på meg – det har jeg satt utrolig stor pris på.

En stor takk til familie og venner for støtte, oppmuntring og motivasjon gjennom et krevende halvår.

Alvhild Skjelvik, 13. Juni. 2019

Sammendrag

Norge er et av de mest digitaliserte landene i verden. Den teknologiske utviklingen påvirker de fleste samfunnsområder og har bidratt til effektivisering og nyskapning i det norske samfunnet. Samtidig har den teknologiske utviklingen brakt med seg nye utfordringer, nye risikoer og nye sårbarheter. Det har ført til et behov for forståelse og håndtering av cyber-risiko.

I denne oppgaven undersøkes cyber-risiko i finanssektoren og hvorfor den har utviklet seg de siste 10 årene. Dette gjøres gjennom å studere analyser, rapporter og dybdeintervju om risiko og trusselbilde mot den norske finanssektor og mot samfunnet for øvrig. Dokumenter og intervjuer bidrar sammen til å nå oppgavens målsetning. Målet med oppgaven er å øke forståelsen for hvorfor cyber-risiko har utviklet seg i finanssektoren, slik at man enklere kan forstå fremtidige utviklingstrender og best mulig håndtere risikoen.

Gjennom å betrakte finanssektoren som et høyteknologisk system drøftes ulike trusler og farers påvirkning på risiko. Dette gjøres gjennom å benytte teori om normale ulykker og ved å anvende prinsipper fra høy pålitelig organisasjonsteori og IRGC-rammeverket. Trefaktormodellen bidrar til å belyse hvordan ulike perspektiver (*safety* og *security*) påvirker hvordan man tilnærmer seg og forstår risiko.

Undersøkelsen av cyber-trusler, cyber-farer og risikostyring for cyber-risiko demonstrerer at det har skjedd store endringer det siste tiåret. Årsaken for hvorfor cyber-risikoen i finanssektoren har utviklet seg er sammensatte og oppgaven viser at:

- Cyber-domenet gjennomsyrer finanssektoren i 2019, hvilket eksponerer verdier, tjenester og infrastruktur på stadig flere måter.
- Risikoen knyttet til bruk av cyber-domenet må ses i lys av samhandlingen mellom menneske, teknologi og organisasjoner.
- Kompleksitet i finanssektorens system og infrastruktur gjør det utfordrende å holde oversikt over cyber-domenet.
- Cyber-farene som i sin tur utgjør trusler mot sektoren, har stor effekt på cyber-risikoen i sektoren og må forstås som trusler selv om de ikke er tilsiktede.
- Trusselbildet er i kontinuerlig utvikling og trusselaktørene justerer sine metoder etter forsvarsverk og tiltak som blir gjort i sektoren.
- Trusselaktørene har utviklet seg hurtigere enn tiltakene for å forhindre uønskede hendelser.

Det var overraskende at sektoren i stor grad fokuserer på tilsiktede hendelser når risiko forklares og kommuniseres, særlig med tanke på at utilsiktede hendelser utgjør majoriteten av hendelser som påvirker sektoren. Det var også overraskende at sårbarheten i sektoren betraktes som lavere selv om truslene, verdiene og konsekvensene av en uønsket cyber-hendelse er større i 2019 enn i 2009.

Innholdsfortegnelse

Tabeller:

Figurer:

Forkortelser:
APT: Advanced persistant threat
CEO: Chief executive officer
CERT: Computer emergency response team
DDoS: Distributed denial of service attack
DSB: Direktoratet for samfunnssikkerhet og beredskap
HRO: High Reliability Organizations (Høy pålitelige organisasjoner)
HRT: High Reliability Theory
IKT: Informasjons og kommunikasjonsteknologi
NAT: Normal Accident Theory
NSM: Nasjonal sikkerhetsmyndighet
NSR: Næringslivets sikkerhetsråd
PST: Politiets sikkerhets tjeneste
SRA: Society of Risk Analysis

1. Innledning

1.1 Bakgrunn

Den 6. Februar 2019 kom det frem at Visma, et norsk dataselskap, hadde blitt utsatt for et dataangrep hvor trolig kinesisk etterretning sto bak (Halsør, Skille, Olsson, Vartdal & Døvik, 2019). Dette dataangrepet skjedde et par dager etter at Politiets sikkerhetstjenestes (PST) hadde lagt frem sin årlige trusselvurdering, hvor statlig etterretning skisseres som en av hovedtruslene mot Norge (PST, 2019). Selv om Kina fnyser av anklagene mot Visma illustrer angrepet en økende utfordring i Norge, nemlig informasjons- og kommunikasjonsteknologiens (IKT) sikkerhet, også referert til som cybersikkerhet. En drøy måned senere, 19.Mars 2019 ble Norsk Hydro rammet av et løspengevirus som vanskeliggjorde normal drift av tjenester, samt ga store økonomiske konsekvenser. Hydro estimerer at angrepet ga et tap på mellom 300 – 350 millioner kroner (Hydro, 2019). Digitalisering av tjenester bringer med seg en rekke fordeler som at det bidrar til effektivisering av offentlig og privat sektor, samtidig som det utvikler samfunnet og måten verdier skapes på. Solberg-regjeringen la frem en ny nasjonal digital strategi i 2019, hvor de trakk frem at Norge er et av de mest digitaliserte landene i verden (Departementene, 2019). Selv om digitalisering gir oss en rekke muligheter, finnes det også utfordringer knyttet til digitaliseringen av samfunnet samtidig som det medfører et nytt risikobilde, nye trusler og endring i sårbarhetsbildet.

Bare de siste tre årene har det blitt gjennomført en rekke omfattende studier knyttet til cybersikkerhet i finanssektoren. Eling og Wirfs undersøkte i 2016 hvordan cyber-risiko kunne forsikres og hvilke implikasjoner cyber-risiko gir. Deloitte har gitt ut en rapport hvor de undersøker årsaker, sårbarheter og konsekvenser knyttet cyberangrep (2018). Den Europeiske sentralbank ga i 2018 ut en publikasjon som konsentrerte seg om motstandsevne (resiliens) for cyber og utsiktene for finansmarkedets infrastruktur. Friedman (2016) trekker frem hvilke erfaringer man har tilegnet seg fra finansinstitusjoner og hvordan disse erfaringene kan bidra til å bedre risikostyring for cyber-risiko. Kopp, Kaffenberger og Wilson (2017) undersøker hvordan cyber-risiko, svikt i markedet og finansiell stabilitet henger sammen og belyser hvilke effekter cyber-risiko har for markeder. Armour (2017) undersøker hvordan økende antall, kompleksitet og omfanget av cyberangrep har ført til et økt behov for at ledere fokuserer på å cyber-resiliens i sine respektive organisasjoner.

Samtidig er sikkerhet knyttet til teknologi ikke er noe nytt. Allerede i 2000 trakk sårbarhetsutvalget, ledet av Kåre Willoch, frem bekymring tilknyttet den teknologiske utviklingen og særlig den økende avhengigheten av informasjons- og kommunikasjonsteknologi (NOU 2000:24). Siden 2000 har teknologien utviklet seg enormt, og man har gått fra et analogt samfunn til et digitalt samfunn. I tillegg fastslår departementene i Solberg-regjeringen (2019) at teknologien kommer til å endre samfunnet enda mer i årene fremover, gjennom ny teknologi som kunstig intelligens og robotisering (Departementene, 2019). Det vil naturligvis medføre økte bekymringer, slik PST og Nasjonal sikkerhetsmyndighet (NSM) skisserer i sine årlige rapporter om det nasjonale risikobildet for Norge. Den digitale sårbarheten i samfunnet vokser, og infrastruktur og IKT-systemer blir mer komplekse, integrerte og globale (PST 2019; NSM 2018a). Selv om det vil skje store endringer forventes det at risikobildet vil fortsette å bestå av trusler som allerede er kjente i dag, utfordringen ligger i at måten truslene utartes, er i stadig endring. Risikobildet for cyber-hendelser er særlig knyttet til trusler som statlig etterretning, løspengevirus, industrispionasje, sabotasje, utpressing og ID-tyveri for å nevne noen.

I lys av risikobildet for cyber-hendelser, er det enkelte sektorer som har opplevd økende risiko og sårbarhet de seneste årene, samtidig som trusselbildet har vært skiftende. På bakgrunn av et samfunn i rask digital omvelting, er det interessant å utforske en av sektorene som er særlig sårbare for cyber-hendelser, nemlig finanssektoren (Direktoratet for sikkerhet og beredskap, 2019). I Norge er finanssektoren en kritisk samfunnsfunksjon og en del av samfunnets kritiske infrastruktur, og det er både private og offentlige aktører som driver sektoren (DSB, 2016). Dersom for eksempel betalingssystemene brytes ned, kan det gi svært omfattende konsekvenser for næringslivet, privatpersoner og samfunnet som helhet. Det forvaltes også store økonomiske verdier i sektoren, hvilket gjør det til en attraktiv sektor å angripe.

1.2 Problemstilling

Denne oppgaven er en historisk tilnærming til utvikling av cyber-risiko, hvor trusler og farer [1] mot finanssektoren er objekt for studiet. Hensikten med studien er å kartlegge trender og

[1] Fare er vanligvis ikke brukt i litteratur eller fagmiljøet knyttet til cybersikkerhet. Begrepet benyttes i denne avhandlingen da det bidrar til å skille mellom to ulike konsepter. Farer referer til utilsiktede hendelser som kan føre til operasjonelle hendelser som i sin tur påvirker risiko, mens trusler referer til tilsiktede handlinger som kan føre til sikkerhetshendelser som også påvirker risiko. I kapittel 3.1 vil teoretiske definisjoner legges til grunn.

mønstre tilknyttet utviklingen av cyber-risiko i finanssektoren. Det har ikke blitt gjort en historisk utredning av cyber-risiko mot finanssektoren spesifikt, og det har ikke blitt funnet studier som undersøker dette teamet. Problemstillingen som omfatter hele oppgaven er følgende:

Hvorfor har cyber-risiko i finanssektoren utviklet seg de siste 10 årene?

I undersøkelsen av dette spørsmålet er det formulert tre forskningsspørsmål som på hver sin måte bidrar til å belyse problemstillingen. For å forstå hvorfor cyber-risiko har utviklet seg, burde man undersøke eventuelle trusler som kan påvirke risikoen. Dette har ledet til formuleringen av studiets første forskningsspørsmål:

Hvordan har cyber-truslene mot finanssektoren utviklet seg de siste 10 årene?

Videre kan det sies at risiko ikke utelukkende påvirkes av tilsiktede trusler, men også av utilsiktede farer. Det vil være hensiktsmessig å undersøke hvordan farer forstås i sektoren, for så å identifisere hvilke farer som betraktes som potensielle risikofaktorer. Dette har ledet til formuleringen av et annet forskningsspørsmål:

På hvilken måte påvirker cyber-farer finanssektorens cyber-risiko?

Det siste forskningsspørsmålet forsøker å belyse om det har vært endring i risikostyring, som i sin tur bidrar å belyse noen av faktorene for hvorfor cyber-risikoen har fått utviklet seg. Det er gjort en antagelse om at endringer i trusler og farer vil medføre andre endringer. Siste spørsmål er med bakgrunn i dette formulert som følgende:

Hvordan har risikostyring endret seg for cyber-risiko de siste 10 år?

Avgrensning

Problemstilling og forskningsspørsmål nevner finanssektoren som objekt for studien, men det er gjort avgrensninger i gjennomføringen av dette studiet. Finanssektoren i Norge er en stor sektor, bestående av en rekke ulike offentlige og private aktører. Denne oppgaven har ikke som formål å kartlegge utviklingen for en spesifikk virksomhet eller bedrift, men å gi et overordnet bilde av utviklingen av cyber-risiko i finanssektoren. For å avgrense oppgaven ble

det besluttet å undersøke virksomheter knyttet til finansielle transaksjoner, herunder betalingstransaksjoner. Ytterligere ble det under betalingstransaksjoner fokusert på interbanksystem og overføring av penger mellom kundekonti i banker (system for betalingstjenester). Denne avgrensingen bidro til å generere informanter som hadde inngående kompetanse om bank og finans-virksomhetsområde. Hensikt med avgrensingen var å ha muligheten til å gjøre en grundig analyse av en del av sektoren som ikke har blitt undersøkt tidligere. Videre vil funnene, på tross av avgrensingen, være mulige å overføre til andre deler av sektorer med enkelte modifikasjoner.

1.3 Faglig relevans

Samfunnssikkerheten i Norge hevdes å være i endring som følge av digitalisering, derfor er det nyttig å ha en oversikt over hvordan utviklingen har vært de siste årene. Ved å benytte en historisk tilnærming til fenomenet cyber-risiko kan man kartlegge trender og mønstre ved fenomenet, som bidrar til å gjøre oss mer beredt i fremtiden. Det er ofte slik at fortiden kan hjelpe oss å predikere fremtiden, hvilket gjør denne oppgaven relevant både faglig og samfunnsmessig. Dernest er det manglende kartlegging av cyber-trusler og angrep på den norske finanssektoren, hvilket øker relevansen og nytten av denne studien. Det blir gjort flere årlige trussel-, og risikovurderinger for Norge og næringslivet forøvrig, men det finnes få utredninger og rapporter som tar for seg et større tidsperspektiv og som inkluderer finans. Den faglige relevansen blir også demonstrert gjennom bruk av teori fra samfunnssikkerhetsfeltet, særlig i lys av konseptet risiko.

1.4 Tidligere forskning

International Monetary Fund (IMF) beskriver og kartlegger cyber-risiko gjennom sin publikasjon «Cyber Risk for the Finance Sector: a Framework for Quantitative Assesment» (Bouveret, 2018). Gjennom innsamling av data fra internett, herunder medieartikler og nasjonale analyser av dataangrep, har IMF analysert trender og hendelser som har påvirket finanssektoren. Funnene viser at cyber-risikoen for finanssektoren og trenden for cyber-hendelser er økende. IMF karakteriserer cyber-risiko som en internasjonal nøkkeltrussel mot finansiell stabilitet og mot de finansielle institusjonene i verden (Bouveret, 2018). Videre analyseres frekvensen av angrep og hvilke land som opplever størst risiko for cyberangrep. Analysen tar for seg private aktører i finanssektoren, så vell som offentlige aktører som ulike nasjoner sentralbanker (Bouveret, 2018).

Tim Harford (2011) undersøkte i sin artikkel hva finanssektoren kan lære fra kjernekraftreaktorer, på bakgrunn av finanskrisen i 2007-08. I artikkelen trekkes det flere paralleller mellom sikkerheten på et atomkraftverk og finanssystemet, særlig knyttet til menneskelig feil og normale ulykker. James Reason sin holdning til menneskelige feil, samt Charles Perrow sin tilnærming til ulykker er overførbare til finanssektoren hevder Harford (2011). Ved å se finanskrisen opp imot et atomkraftverk belyser Harford (2011) hvordan den stadig økende kompleksiteten i systemet førte til at det brøt sammen. Det gjøres også en sammenligning av Piper Alpha-ulykken opp imot finanssektoren, for å demonstrere hvordan sikkerhetsbarrierer og kompleksitet kan påvirke et system. Finanssektoren sin kompleksitet har økt siden 2008, særlig med tanke på hvordan digitaliseringen skaper avhengigheter og kompleksitet i infrastrukturen i sektoren.

Det internasjonale tidsskriftet *International Finance Law Review* gjorde i 2015 en grundig undersøkelse av cybersikkerhet i finans sektoren. Konklusjonen de trakk etter å ha pratet med ulike aktører på tvers av finanssektoren i USA, Europa og Asia var at «this fight will never be over» (Myles, Lee, Thomas & Meager, 2015, siste avsnitt). Et gjennomgående tema i utredningen er at et felles problem for finansiell stabilitet og finansiell infrastruktur på tvers av verden er cybercrime og de ulike metodene som kan benyttes. Gjennom å intervjue sentrale sikkerhetsaktører kommer det frem at trenden for å svekke tilliten til banker gjennom å målrettede angrep på et systems integritet og systemets brukere, er økende. Videre trekkes det frem at problematikken med cyber-space er at det stadig forekommer en ny kategori for cybercrime (Myles et al., 2015).

Pat Antonacci (2018) diskuterer i det nylig opprettede tidsskriftet *Cyber Security* hvilke og hvordan cyber-trusler kan påvirke finanssektoren. Det belyses gjennom teksten hvordan cyberkriminelle utfordrer sektoren og at finanssektoren er blant de mest digitaliserte virksomhetene, samt har størst investeringer i IT sikkerhetssystemer. Antonacci (2018) gjør en vurdering av sikkerhetstiltakene som SWIFT initierte etter Bangladesh-hendelsen (Se vedlegg 8 for bakgrunn om bangladesh-hendelsen). Initiativet 'Customer Security Programme' (CSP) er et globalt initiativ for å hjelpe finanssektoren til å beskytte seg mot angrep og omfatter SWIFT sin globale kundegruppe. Det oppfordres til et globalt samarbeid, samstyring og føringer legges for at man skal lære, støtte og videreføre ferdigheter og erfaringer knyttet til cyber-trusler.

I tidsskriftet *Risk Analysis* utforsker Paté-Cornell, Kuypers, Smith & Keller (2018) cybersikkerhetsstyring for kritisk infrastruktur ved å ta for seg tre ulike cyber relaterte hendelser i ulike sektorer. Det gjøres en kvantifisering av tilgjengelig statistikk for å se utvikling av cyber-angrep og for å se effekten av tiltakene som har blitt gjort for å øke cybersikkerhet. Datamaterialet som blir brukt og påfølgende funn reflekterer fortiden, men kan sammen med tilleggsinformasjon bli brukt for å kartlegge frekvensen og påvirkningen av liknende hendelser i fremtiden. Funnene demonstrerer at mye penger blir dedikert til å styre cyber-risiko, men at det finnes lite informasjon om effektiviteten tilknyttet de ulike tiltakene. Det trekkes frem at industri, nasjoner og privatpersoner ser på cyber-risiko som bekymringsverdig da konsekvensene kan være vanskelige å forutse, samtidig som det spås at de kan være katastrofale (Paté-Cornell et al., 2018). Funnene fra denne artikkelen, er interessante opp imot hvorfor cyber-risiko har utviklet seg i finanssektoren, da finanssektoren utgjør en kritisk samfunnsfunksjon i Norge og i lys av ressursene som blir brukt på cybersikkerhet.

1.5 Oppgavens struktur

I denne oppgaven vil flere sentrale temaer for forskning gjennomgås. I kapittel 1 introduseres temaet, problemstilling og forskningsspørsmål, og avgrensningen av oppgaven.

Kapittel 2 gjengir konteksten til oppgaven, hvor rammene for studiet settes. I dette kapittelet vil digitaliseringsprosessen av Norge og finanssektoren bli kort redegjort for, samt krav og lovverk som er relevant for finanssektoren.

Kapittel 3 redegjør for teorien som blir brukt i oppgavens drøfting. I kapittel 4 utdypes metode, samt hvilke valg som har blitt tatt gjennom forskningsprosessen. Videre vil kapittelet drøfte forskerrollen og kvaliteten av datamaterialet.

Kapittel 5 presenterer funn og empiri, som vil bli diskutert i lys av teori i kapittel 6. Avslutningsvis vil kapittel 7 oppsummere hovedfunn og svare på oppgavens problemstilling. Til slutt vil det bli gitt forslag til videre forskning.

2. Kontekst

Digitaliseringen av Norge er og har vært en omfattende prosess. I dette kapittelet vil digitaliseringen av finanssektoren bli kort redegjort for, før sentrale begrep innenfor cybersikkerhet vil bli forklart. Deretter trekkes det frem hvilke aktører som opererer innenfor finansielle transaksjoner. Avslutningsvis vil lovverk og krav for finanssektoren bli trukket frem, det gjelder også krav til cybersikkerhet.

2.1 Digitalisering i finanssektoren

Innledningsvis ble det nevnt at Norge er et digitalisert samfunn, faktisk er Norge sammen med Sverige de mest digitaliserte landene i verden (NOU 2018:14). Nordmenn er flinke til å ta i bruk ny teknologi, og man har funnet opp innovative løsninger gjennom å bruke teknologien i utviklingen av samfunnet. Hannemyr (2015) deler digitaliseringen inn i tre faser, som har gitt ulike konsekvenser for industrien, særlig handels- og næringsindustrien.

Fase 1 startet med Steve Jobs og Apple sin utvikling av datamaskiner, som både var mer brukervennlige og funksjonelle enn tidligere oppfinnelser. Steve Jobs sitt fokus var å tenke på hva sluttbrukeren trengte og hvordan datamaskiner ble brukt, for så å tilpasse teknologien der etter. Denne tilnærmingen til teknologien førte til at stadig flere kunne ta i bruk datamaskiner i hverdagen. Fase 2 kjennetegnes av Internett, som revolusjonerte måten man kommuniserer og sprer informasjon på starten av 1990-tallet. Selv om et stort antall forskere spådde at internett ikke ville bli et vedvarende fenomen i samfunnet, har det blitt en del av samfunnet slik vi kjenner det i dag. Internett hadde en ekstrem vekst i antall brukere på kort tid, og man anslår at omtrent 55.1% av verdens befolkning bruker Internett i dag (Statista, 2019). Den siste fasen som Hannemyr (2015) nevner kjennetegnes av mobiltelefoner. Mobiltelefoner er ikke lenger kun et kommunikasjonsverktøy gjennom tale og SMS, men har utviklet seg til små datamaskiner med Internettilgang.

De tre fasene har endret måten finanssektoren opererer på, da sektoren må holde tritt med utviklingen i digitaliseringen. Det har tvunget sektoren til å være innovative i møte med teknologi og digitalisering. Et godt eksempel på innovasjon i finanssektoren er DNB sin utvikling av betalings- og overføringstjenesten VIPPS (Vipps, 2019). Tjenesten har utviklet seg fra en betalingstjeneste mellom privatpersoner til å bli en av de viktigste finansielle infrastrukturene i Norge. Vipps er også en god representasjon for World Economic Forum

(WEF) sine prediksjoner om hvordan bortgangen fra kontanter skaper et nytt press på banker (WEF, 2015). Presset kommer fra at banken i større grad må finne opp og levere nye former for tjenester og moderne banktjenester. Det kontantløse samfunnet er en trend man i større grad ser i Norge, og tjenester som Vipps gjør det lettere for forbrukere å gå bort ifra kontanter. Eksperter mener at Norge er et av landene som blir kontantløse først, og i 2018 utgjorde kontanter under 11 prosent av alle transaksjoner som ble utført i Norge (Norges Bank, 2018a).

På global skala har det vært flere uønskede hendelser som har rammet bank- og finanssektoren. Bortfall av nettbanktjenester plaget DNB i 2017, hvilket de mottok sterk kritikk for av finanstilsynet. DNB er ikke den eneste som har blitt utsatt for uønskede hendelser, eksempelvis ble Norges Bank sine hjemmesider utsatt for et tjenestenektangrep (DDoS-angrep) i 2014, som førte til at deres hjemmeside krasjet (Havnes, 2014). Videre ble sentralbanken i Bangladesh rammet av et alvorlig cyber-angrep gjennom SWIFT i 2016 (se vedlegg 8 for beskrivelse). Andre kjente hendelser i det digitale domenet det siste tiåret som har rammet sektorer utenfor finanssektoren er kryptoorm viruset WannaCry i 2017 og løspengevirus og malware angrepet NotPetya i 2016 og 2017 (se vedlegg 8 for beskrivelse). Wannacry rammet helsesektoren særlig hardt, hvor helse Midt-Norge ble berørt. Britiske sykehus ble også hardt rammet av dette viruset, og tusenvis av pasienter fikk sine journaler kompromittert. Det siste halvåret har flere norske virksomheter opplevd omfattende cyber-angrep, og innledningsvis ble angrepet på Visma i februar nevnt. Et annet alvorlig angrep som har blitt nevnt er løspengeviruset mot Hydro i Mars 2019.

Disse hendelsene demonstrerer utfordringene som ble påpekt allerede for 20 år siden, nemlig at digitalisering kan gi uforutsigbare konsekvenser og utfordringer for samfunnet. Selv om teknologi og digitalisering gir samfunnet ekstremt mange goder, burde man i aller høyeste grad sørge for å forstå de samfunnsmessige implikasjonene når de integreres i samfunnet (NOU 2018:14; Departementene, 2019).

2.2 IKT og Cyber

I denne oppgaven vil begrepet cybersikkerhet bli brukt som et synonym til IKT-sikkerhet. Det er ulike sikkerhetsmål i ivaretakelse av cybersikkerhet, og de tre vanligste knyttes mot integritet, konfidensialitet og tilgjengelighet (NOU 2015:13).

Konfidensialitetsproblemer forekommer når privat informasjon innad i et firma blir tilgjengelig for utenforstående, som gjennom databrudd. Integritetsproblematikk kan relateres til misbruk av systemene, slik som under svindel. Mens tilgjengelighetsproblemer er tilknyttet til forretningsforstyrrelser (NOU 2015:13). De tre ulike typene for kompromittering har ulik innvirkning på de som blir utsatt. Forretningsforstyrrelser forhindrer firmaer i å opprettholde tjenesteleveranser som kan forsake inntekter, svindel fører til direkte økonomiske tap, mens et datainnbrudd tar mer tid til å materialisere, ofte gjennom omdømmepåvirkning og saksomkostninger. Mer generelt er risikoen for å tape tillit som følge av et cyber-angrep svært alvorlig for finanssektoren, særlig ettersom finansielle institusjoner er avhengige av tilliten fra sine kunder.

Skuterud (2003) referer til *logisk* og *fysisk* sikring i arbeidet med IKT-sikkerhet og informasjonssikkerhet. IKT-sikkerhet omfatter sikring av informasjon, men må ikke forveksles med informasjonssikkerhet. IKT-sikkerhet innsnevres til informasjon som kun er i elektronisk form og ved at det omfatter infrastruktur (Solhaug, 2014). Logisk sikring har som overordnet mål å tilrettelegge for tiltak som reduserer risikobildet for hva ledelse oppfatter som et akseptabelt sikkerhetsnivå. Dernest handler det om å beskytte mot farer, slik at sannsynlighet reduseres og konsekvenser av hendelser minimeres. Informasjon, systemer og tjenester skal beskyttes mot kriminelle handlinger, uhell og manipulering. Fysisk sikkerhet er sikring av IT-systemer og informasjon mot fysisk tilgang fra utenforstående personer eller mot naturkatastrofer. I finanssektoren er det viktig for både virksomheter og privatpersoner at sikkerheten for konfidensialitet, tilgjengelighet og integritet er på et tilfredsstillende nivå, samt at virksomheten opprettholder krav til fysisk sikring av systemer og verdier (Skuterud, 2003). Det er viktig at finanssektoren forstår sammenhengen mellom logisk og fysisk sikring, for dersom man ikke har god nok fysisk sikring av for eksempel et bygg, kan uvedkommende skaffe tilgang til sikkerhetstekniske system som kan lede til uønskede IKT-hendelser (Skuterud, 2003). Likeså dersom den logiske sikringen ikke er ivaretatt kan det føre til svikt i fysiske sikringstiltak – som i sin tur kan gi uønskede konsekvenser.

2.3 Aktører

Det har blitt nevnt tidligere i oppgaven at finanssektoren består offentlige og private aktører. Samtidig er det ulike aktører som representerer en trussel mot finanssektoren. Videre er det

ulike aktører som arbeider med å håndtere truslene som møter finanssektoren. Nordic Financial Computer Emergency Response Team (NF CERT) er et eksempel på en viktig aktør i håndteringen av truslene som møter finanssektoren, og som daglig jobber med hendelseshåndtering av digitale angrep. Videre spiller NSM og NorCERT en sentral rolle i rådgiving og støtte i arbeidet med cyber-trusler og cyber-angrep. I dette studiet gjøres en logisk avgrensing til aktører som er involvert i finansielle transaksjoner. Under finansielle transaksjoner finnes interbanksystemer, system for bankoppgjør og elektronisk ID (Lov om betalingssystemer, 1999).

Aktører som er involvert i finansielle transaksjoner er tilsynsmyndigheter, driftsleverandører og systemeiere. En tilsynsmyndighet har ansvar for å føre tilsyn og kontrollere at virksomheter som driver med finansielle transaksjoner overholder lov- og regelverk i henhold til betalingssystemloven. Driftsleverandør er leverandør og forvalter av IKT-drift, IKT-systemer og IKT-infrastruktur, mens systemeier refererer til ansvarlig eier av et gitt system. Eksempelvis er DNB Bank ASA ansvarlig for DNBs nettbanksystemer i kraft av deres rolle som systemeier, mens Evry svarer til DNB som deres driftsleverandør og er ansvarlig for at driften er problemfri på vegne av DNB. Finanstilsynet er tilsynsmyndigheten som fører tilsyn med DNB for å forsikre at IKT-forskriften blir overholdt. Avgrensningen for valg av informanter vil bli nærmere redegjort for i kapitel 4.2. Aktørene er fremstilt i tabell 6, vedlegg 2.

2.4 Lovverk og krav

Betalingssystemloven

Betalingssystemloven (1999) omfatter betalingssystem og verdipapiroppgjør. Det stilles gjennom lovverket særskilte retningslinjer og krav for aktører som er omfattet av lovverket. Lovbestemmelsene retter seg mot hvordan interbanksystemer og system for betalingstjenester skal drives, hvem som har tilsyn, konsesjonsrett og adgang, samt at den gir ulike systemkrav. Loven definerer internbanksystemet som de systemer som baseres på felles regler for avregning, oppgjør eller overføring av penger mellom kredittinstitusjoner, mens system for betalingstjenester forklares som «systemer basert på standardvilkår for overføring av penger fra eller mellom kundekonti i banker eller andre som kan yte betalingstjenester etter finansieringsvirksomhetsloven § 4b-1 første ledd når overføringene bygger på bruk av betalingskort, tallkoder eller annen form for selvstendig bruker legitimasjon utstedt til en

ubestemt krets» (Betalingssystemloven, 1999). Det knyttes dermed opp mot nettbanktjenester som for eksempel eies av DNB Bank ASA, i kraft av at de er systemeiere.

Formålet for bestemmelsene for interbanksystem er gitt i § 2.1 «formålet med bestemmelsene i dette kapittelet er å bidra til at interbanksystemer organiseres slik at hensynet til finansiell stabilitet blir ivaretatt» (Betalingssystemloven, 1999). Det skal særlig legges vekt på å motvirke risiko som følge av likviditets- eller soliditetssvikt hos deltakere i slike systemer. Videre er formålet for system for betalingstjenester gitt i § 3-1 «formålet med bestemmelsene i dette kapittelet er å bidra til at systemer for betalingstjenester innrettes og drives slik at hensynet til sikker og effektiv betaling og til rasjonell og samordnet utførelse av betalingstjenester ivaretas» (Betalingssystemloven, 1999). Slik som paragrafen leses skal det tas hensyn til sikkerhet i banktjenestene. Sikkerheten for betaling og ivaretakelse av betalingstjenester er i stor grad avhengig av at det er tilstrekkelig sikkerhetsstyring i virksomhetene som er omfattet av lovverket. For eksempel skal Norges Bank som landets sentralbank ha en tilfredsstillende sikring av sine systemer, slik at effektive og robuste betalingssystemer ivaretas.

IKT-forskriften

IKT-forskriften (2003) stiller spesifikke krav til finansnæringen angående bruk av informasjons og kommunikasjonsteknologi, og gjelder for den norske finanssektoren. Finanstilsynet har som ansvar å føre tilsyn med finansforetak, for å sørge for etterlevelse av lovverk og hjemler gjeldende for det norske betalingssystemet (Finanstilsynet, 2017b). Gjennom forskriften stilles det krav til regelmessige risikoanalyser og krav til sikkerhetsnivå for IKT-systemer, tjenester og drift. Dersom det er eksterne som drifter en virksomhets IKT-systemer skal avtalene sikre at forskriftens krav overholdes, særlig bestemmelser rettet til sikkerhet og dokumentasjon (IKT-forskriften, 2003). Videre stiller forskriften også krav til avvikshåndtering og rapporteringskrav til finanstilsynet, dette gjelder både for operasjonelle og sikkerhetshendelser som vurderes som alvorlig til kritisk av den rammede virksomheten. IKT-forskriften er et virkemiddel i en helhetlig sikkerhetsstyring for sektoren, og ved brudd på IKT-forskriften kan finanstilsynet gi bøter og i verste fall trekke tilbake konsesjonsretten til en virksomhet.

NIS-direktivet

EU vedtok NIS-direktivet i 2016 og pålegger medlemmer i EU og EØS om å ivareta og sørge for et samordnet nivå for IKT-sikkerhet. Dette skal oppnås gjennom utarbeidelse av «strategier for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) og pålegge operatører og leverandører av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser» (Justis- og beredskapsdepartementet, 2016). Bakgrunnen for direktivet er EU sin strategi for cybersikkerhet som ble publisert i 2013. Innholdet retter seg mot nasjoner i sin helhet, hvor det skal også gis anbefalinger om å etablere sektorspesifikke CERT-team, her er finansmarkedsinfrastruktur inkludert da den er leverandør av essensielle tjenester. Finanstilsynet belyste i sitt høringssvar på NIS-direktivet at IKT-forskriften som hovedtrekk var «dekkende for NIS-direktivets bestemmelser» (Justis- og beredskapsdepartementet, 2016). NIS-direktivet er et viktig steg i å samordne responsen på cyberangrep og mitigering av cyber-risiko på tvers av EU. Videre oppfordrer det til transnasjonalt samarbeid for å motstå risiko, trusler og angrep knyttet til cyber-domenet.

PSD2

EU fremmet et nytt betalingsdirektiv som skal implementeres i løpet av 2019. Dette vil medføre en endring i aktører som kan tilby betalingstjenester, og hvilke aktører som har tilgang til kunders kortinformasjon (Regjeringen, 2019). Bankene har hatt monopol på betalingsformidlingstjenester som nå vil forsvinne. Dette muliggjør bruken av tredjepartsleverandører og vil medføre økt konkurranse for betalingstjenester og om kundene. Videre åpner det opp for at tredjepartsleverandører får tilgang til kunders informasjon, da direktivet muliggjør at nye selskaper, også utenfor bankvesenet, kan benytte seg av informasjonen bankene har.

PSD2 åpner altså opp for at tunge aktører som Facebook, Google og Amazon kan delta på betalingstjeneste markedet, men åpner også døren for start-ups og ny innovasjon for betalingsformidlingen.

Sikkerhetsloven

Lov om nasjonal sikkerhet (sikkerhetsloven) ble fornyet ved inngangen til 2019. Hovedvirkeområdet til lovverket er offentlig forvaltning, men ettersom samfunnets risikoer og sårbarheter har utviklet seg, har loven blitt utvidet. For å sørge for at virksomhetene er

beredt til å møte et endret trusselbilde stiller loven blant annet krav om alle virksomheter som er omfattet av loven må ha på plass et styringssystem for sikkerhet. Oppdateringen av lovverket går fra beskyttelse og bruk av sikkerhetsgradert informasjon til også å regulere tjenester og infrastruktur som er av samfunnskritisk betydning.

I §1 utdypes lovens formål *«loven skal bidra til a) å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser, b) å forebygge, avdekke og motvirke sikkerhetstruende virksomhet, c) at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn»* (Sikkerhetsloven, 2019). Videre introduseres begrepet «grunnleggende nasjonale funksjoner» (GNF) som defineres som følgende «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser». I henhold til nasjonale sikkerhetsinteresser inkluderes økonomisk stabilitet og handlefrihet, og derav er flere aktører i finanssektoren omfattet av dette lovverket. Høringen om sikkerhetsloven omfattet tre forskrifter: myndighets-, klarerings-, og virksomhetsforskriften. Forskriftene er ikke delt etter fagområder, og et av hovedmålene ved den nye forskriftsstrukturen er å legge til rette for at både myndigheter og virksomheter ser det forebyggende sikkerhetsarbeidet i sammenheng, og jobber tverrfaglig og helhetlig med sikkerhet. Gjennom forskriftene er det stilt krav om et forsvarlig sikkerhetsnivå. Det kreves at dette skal oppnås gjennom en kombinasjon av menneskelige, elektroniske, fysiske og organisatoriske tiltak, hvilket fordrer en helhetlig og tverrfaglig tilnærming. (Deloitte, 2019).

3. Relevant teori

Dette kapittelet utdyper relevante begreper og redegjør for oppgavens teori. Det blir tatt i bruk flere generiske begreper som risiko, trussel og sårbarhet – disse med flere forklares og knyttes opp mot problemstillingen i første del av teorikapittelet. I lys av begrepet risiko, vil «safety» og «security»-perspektivene forklares. I andre del vil Charles Perrow (1984) sin teori om Normal Accidents (NAT) bli redegjort for. Dernest forklares High Reliability Theory som fokuserer på høy pålitelige organisasjoner (HRO) (Weick & Sutcliffe, 2007; Sutcliffe & Vogus, 2007; Rosness, Guttormsen, Steiro, Tinmannsvik & Herrera, 2004; LaPorte & Consolini,1991; Hollnagl, Woods & Levenson, 2006). Til slutt blir IRGC-rammeverket bli presentert (Renn, 2008: IRGC, 2017).

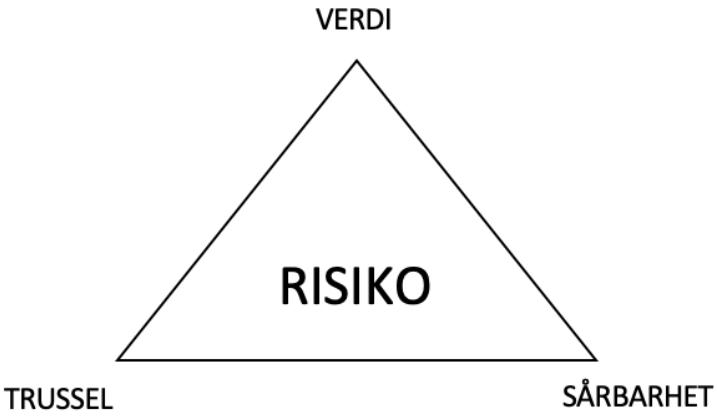
3.1 Begrepsavklaring

3.1.1 Risiko

I finanssektoren og samfunnet forøvrig er det risiko tilknyttet digitaliseringsprosessen. Det er en risiko da konsekvensene av utilsiktede og tilsiktede hendelser kan være svært omfattende og skadelige, og sannsynligheten for at slike hendelser inntreffer er økende. I den internasjonale standarden for risikostyring av informasjonsteknologi (ISO 27005:2018) defineres risiko som «potensialet for at en gitt trussel vil utnytte sårbarhetene til et sett av verdier og derigjennom forårsake skade» (ISO 27005:2018, s.33). I denne oppgaven vil tilnærming til risikobegrepet være knyttet opp til blant annet Aven (2015) sin forståelse av begrepet og tre-faktormodellen (NS 5832:2014; Budmundrud, Maal, Kiran & Endregard, 2015). Konseptualiseringen av risikobegrepet vil bli forklart i det følgende.

Risiko kan ses på som en kombinasjon av trussel, sårbarhet og verdi – og det endrede trusselbilde gir nye sårbarheter med kjente og ukjente konsekvenser er en betydelig risiko for finanssektoren (Engen et al., 2016). Risiko kan forstås som kombinasjonen av sannsynlighet og konsekvens, beheftet med en viss form for usikkerhet (Aven, 2015). Risikoen som det henvises til i denne oppgaven er cyber-risiko, altså risikoen for at informasjons- og kommunikasjonsteknologi og tilhørende systemer, infrastrukturer og prosesser blir utsatt for uønskede hendelser med ulikt konsekvenspotensial. Cyber-risiko forstås i finanssektoren som operasjonell risiko i forhold til de verdier som befinner seg på, eller man kan få tilgang til gjennom informasjon-og kommunikasjonsteknologien (Cebula & Young, 2010). Dette kan i sin tur kan påvirke konfidensialitet, tilgjengelighet og integritet.

3.1.2 Trefaktormodellen



Figur 1: Trefaktormodellen

VERDI

I finanssektoren finnes det ulike verdier, og de kan bestemmes ut ifra deres betydning med hensyn til hvilke beslutninger, vurderinger og tiltak som gjøres for å beskytte og sikre dem. Standard Norge (2012) definerer en verdi som «hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen» (NS5830:2012, s.4). Videre forklares uønsket påvirkning som ødeleggelse, kompromittering eller forstyrrelse. Verdier er blant annet bygninger, servere, mennesker og kompetanse. I dette studiet henvises det til særlig to verdier, den første er penger, mens den andre er data/informasjon. Ettersom finanssektoren er forvalter av store økonomiske verdier er verdivurderingene som gjøres for å være innforstått med farene mot denne verdien særlig viktig.

TRUSSEL

I finanssektoren spenner trusselbildet bredt, og det er ulike aktører med ulike intensjoner som potensielt kan gjennomføre angrep. Truslene som fokuseres på i denne oppgaven er både tilsiktede trusler og utilsiktede trusler som forstås som farer.

Trussel forstås på ulike måter, men defineres ofte som en mulig årsak til en uønsket hendelse (Budmundrud et al., 2015). Begrepet trussel belyser hvilke kapasiteter og intensjoner trusselen har for å gjennomføre skadelige handlinger. Trussel kan i enkelte sammenhenger forveksles med fare. En trussel referer til tilsiktede handlinger som har som formål å føre til

uønskede hendelser, mens fare beskrives som utilsiktede forhold eller handling som fører til uønskede hendelser (NS5814:2008). Faren knyttes opp til risiko dersom potensielle konsekvenser fører til skade (Society of Risk Analysis, 2018).

Det finnes ulike trusselaktører på cyber-domenet. En trusselaktør defineres som «entitet som forbindes med trussel» (NS5830:2012). Trusselaktører har dermed som formål å forårsake uønskede hendelser. En faktor som skiller disse aktørene fra hverandre ligger særlig i motivasjonen for å gjennomføre angrep. Dernest er kompleksitet, formål og ressurser faktorer som skiller aktørene (Langø & Sandvik, 2013). Trusselaktører mot finanssektoren vil bli gjengitt i kapittel 5.2, ettersom funn fra studiet bidrar til å belyse de relevante aktørene.

SÅRBARHET

Sårbarhet har i likhet med risiko-begrepet ulike tilnærminger. I NS5814:2008 defineres sårbarhet som et systems «manglende evne (...) til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin opprinnelige tilstand eller funksjon etter hendelsen». Det motsatte av sårbarhet er robusthet, som referer til «et system evne til å stå imot og opprettholde sin funksjon under ulike former for ytre påkjenninger» (Aven et al., 2004, s.124). Systemet som undersøkes i denne oppgaven er finanssektoren hvor sårbarheten kan knyttes til cyber-domenet. Sårbarheten som avdekkes er digital sårbarhet gjennom kompromittering av konfidensialitet, tilgjengelighet og integritet. Sårbarheten handler med andre ord om alt som er koblet til, eller er avhengig av informasjons- og kommunikasjonsteknologi, og IKT-sikkerhet søker å beskytte alt dette. Det inkluderer ulike former for sikringstiltak, både tekniske, organisatoriske og administrative, for å sikre system og informasjon (Justis- og beredskapsdepartementet, 2017). Videre handler det om å implementere risikoreduserende tiltak og barrierer for å unngå at uønskede hendelser utvikler seg og gir store konsekvenser.

3.1.3 «Safety» og «Security»

Definisjonen av risiko i henhold til trefaktormodellen er en tilnærming til risiko som er i tråd med et security-perspektiv, men det kan også omsettes i et safety-perspektiv (Engen et al., 2016). Det har vært store teoretiske diskusjoner om hvordan sikkerhet skal beskrives, og en distinksjon er gjort mellom «safety» og «security». I det norske språket har man kun et ord for sikkerhet, mens i det engelske språk har de flere, «safety» og «security» henviser til to ulike måter å beskrive sikkerhet (Budmundrud et al., 2015). «Safety» kan forstås som trygghet, og

begrepet benyttes om sikkerhet mot uønskede hendelser som et resultat av tilfeldigheter og uhell. Det referer dermed til uønskede, *ikke-tilsiktede* hendelser. «Security» referer til *tilsiktede* hendelser, og omhandler sikkerhet mot uønskede hendelser som et resultat av hensikt. Sikring blir vanligvis forbundet med «security» begrepet, og taler til beskrivelse av handlinger som har som formål å føre til skade. Trefaktormodellen kan omsettes både i et «safety» og «security»-perspektiv når man undersøker hvilke trusler som har potensiale til å true viktige verdier (Boholm, Möller og Hansson, 2016). Ved å anvende et «security»-perseptiv vil trusler da være tilsiktede hendelser, men fra et «safety»-perspektiv kan trusler forstås som utilsiktede hendelser – altså farer.

I kapittel 6 vil begrepene «safety» og «security» bli brukt som to ulike beskrivelser av risiko og vil representere to ulike perspektiver på sikkerhet. Henholdsvis vil referansen til cyber-farer befinne seg i et «safety»-perspektiv, mens cyber-trusler må forstås fra et «security»-perspektiv. Fra et «safety»-perspektiv kan man trekke inn operasjonell risiko, som forklares som feil i IT-systemer, regelbrudd, prosedyresvikt, og dette kan knyttes til både kontrollsystemer og menneskelige feil (Det Norske Veritas, 2009). Pietre, Cambacédès & Chaudet (2010) hevder det er hensiktsmessig å skille mellom «security» og «safety» når man skal håndtere risiko, da det krever ulike tiltak for å håndtere risiko knyttet til for eksempel terrorisme og risiko knyttet til naturfarer. Selv om det finnes uenigheter omkring forskjellen mellom begrepene vil hovedforskjellen handle om intensjonen bak handlingen.

3.1.4 Risikostyring

Risikostyring er en viktig oppgave i finanssektoren. Det handler om den målrettede aktivitet for å identifisere, estimere og kontrollere hendelser som kan påvirke måloppnåelse negativt (Aven, 2015; Aven et al., 2017). Hensikten er å unngå alvorlige konsekvenser og minimere eventuelle tap. Risikostyring, også referert til som sikkerhetsstyring, beskrives av Aven et al. (2004, s. 67) som «alle tiltak som iverksettes for å oppnå, opprettholde og videreutvikle et sikkerhetsnivå i overensstemmelse med definerte mål». James Reason (1997) skriver at det viktigste målet for sikkerhetsstyring ikke bør være å redusere antall uønskede hendelser til null. I stedet bør man fokusere på å øke robustheten for å kunne forsvare seg mot all fare. For å styre risiko er det en forutsetning at man har en felles forståelse av risiko (Dahl, 2000).

Aven og Krohn (2013) belyser at det er ulike tilnærminger til hvordan man forstår, vurderer og styrer risiko og fremtidsrettet aktivitet. I finanssektoren vil ulike virksomheter ha ulik

tilnærming til risikostyring, også avhengig av hvilke risikoer de møter. Dette vil naturligvis variere mellom små, mellomstore og store virksomheter.

Risiko- og sårbarhetsanalyse

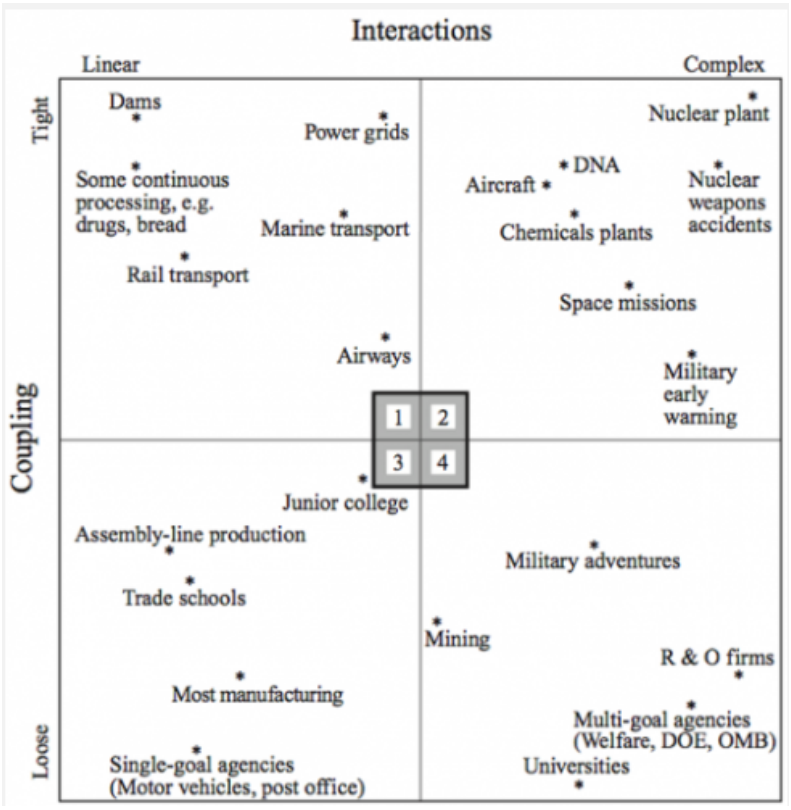
I en risiko- og sårbarhetsanalyse (ROS-analyse) skal man identifisere og kategorisere ulike risikoer og sårbarheter som møter systemet, for så å kartlegge mulighet for styring, tiltak og ulike virkemidler for å oppnå definerte mål (Aven et al., 2017). Analysen identifiserer trusler og farer, og tilbyr veiledning for hvordan de kan forebygges. ROS-analyser er beheftet med en viss grad av usikkerhet ved at man ikke kan predikere alle former for risikoer, og dermed heller ikke alle konsekvenser. Det gjelder særlig når man analyserer og styrer fremtidsrettet aktivitet, hvor man ikke har tilstrekkelig kunnskap og informasjon om aktiviteten som analyseres (Aven et al., 2017).

3.2 Normal Accident Theory (NAT)

Charles Perrow (1984) har studert ulykker i høyteknologiske systemer, og har identifisert sammenhenger som øker risikoen for ulykker. I stedet for å betrakte ulykker som noe man kan sikre seg mot, mener Perrow at ulykker vil forekomme i høyteknologiske systemer før eller senere – de er på et vis uunngåelige. Man kan skille mellom ulike typer ulykker, og dette gjør Perrow ved å karakterisere en type ulykke for komponentfeil-ulykke der en eller flere komponenter i et system feiler. Den andre karakteriseringen er systemulykke som kjennetegnes ved at flere komponenter feiler samtidig som i sin tur fører til uventede interaksjoner. En systemulykke er vanskeligere å predikere, da sekvensene oppstår i nye og ukjente interaksjoner, mens komponentfeil-ulykker forplanter seg i forventede sekvenser. Det stilles noen forutsetninger for disse ulykkene, det er at systemet som de oppstår i er komplekst, tett koblet og har et stort katastrofepotensial.

Et systems kompleksitet kjennetegnes av hvordan det er koblet og egenskaper ved interaksjoner i systemet. Perrow skiller mellom tette og løse koblinger, og mellom lineære og komplekse interaksjoner. Et system som er løst koblet med lineære interaksjoner vil vanligvis ikke medføre alvorlige systemulykker, da det er liten tidsavhengighet og uforutsigbarhet i systemet som muliggjør at eventuelle komponentfeil kan bli håndtert. Derimot vil et system som har komplekse interaksjoner samtidig som det er tett koblet kunne medføre mer alvorlige hendelser, eller systemulykker som Perrow referer til.

Høyrisikosystemene som omsettes i teorien er eksempelvis atomkraftverk og flytransport-trafikk, men teorien er lett omsettelig til andre komplekse høyteknologiske systemer. Ved å bygge inn sikkerhetsmekanismer som redundante løsninger, vil kompleksiteten i et system øke. Økt kompleksitet vil i sin tur øke sannsynligheten for en ulykke ettersom interaksjonene blir for komplekse i tett koblede systemer. Kun gjennom å redusere kompleksiteten i systemet og løse opp de tette koblingene vil man gjøre systemet mindre sårbart for ulykker, hevder Perrow (1984). Et annet interessant aspekt ved Perrow sin teori er at ulykkene er uunngåelige og ikke kan designes bort ved å øke redundansen i ett system. Ulykker skyldes ikke kun teknologi eller system, men kan relateres til organisasjonen, ledelsen og menneskene som opererer i det.



Figur 2: Interaksjon/koblingskart (Perrow, 1984)

Figur 2 bidrar til å demonstrere Perrow sin kategorisering av ulike systemer. Finanssektoren er som sådan ikke et høyteknologisk system på samme måte som et atomkraftverk. Likevel finnes det flere likhetstrekk i hvordan systemiske, organisatoriske og menneskelige feil kan forplante seg i systemet og føre til at system ikke fungerer. Videre vil trolig ikke konsekvensene knyttet til ulykker i finanssektoren være like katastrofale i forhold til liv og helse som et atomkraftverk.

3.3 High Reliability Organisations (HRO)

I teorien om HRO tar man utgangspunkt i at ulykker i høyteknologiske systemer kan forebygges og at det er mulig å ha et pålitelig system basert på upålitelige komponenter (Aven et al., 2004). Teorien undersøker hvordan organisasjoner kan organisere seg for å oppnå høy ytelse under forhold hvor feil kan få svært alvorlige konsekvenser – som krever at man har pålitelige systemer. Organiseringen kan på et vis kompensere for menneskelige feil og teknologiske svakheter. Weick og Sutcliffe (2007) hevder at små hendelser kan være grunnlaget for store ulykker, og at man derfor må være årvåkne for å oppfatte små hendelser før de materialiserer seg til ulykker. Det er særlig tre egenskaper en organisasjon må besitte for å karakteriseres som en høy pålitelig organisasjon, det er:

1. Organisatorisk redundans
2. Spontan omstilling (desentralisering og sentralisering)
3. Årvåkenhet (mindfullness)

Rosness et al. (2004) hevder at organisatorisk redundans kan ses fra en strukturell og en kulturell dimensjon. Den strukturelle dimensjonen fokuserer på utvikling av kompetanse og mulighet for kommunikasjon, mens den kulturelle dimensjonen handler om å ha en kultur (eksempelvis) for rapportering av feil og deling av informasjon. James Reason (1997) er også kjent for sitt fokus på kultur, og han hevder at en forutsetning for høy pålitelige organisasjoner er at man har en informert kultur. En informert kultur forutsetter at man har en rapporterende, rettferdig, lærende og fleksibel kultur. LaPorte og Consolini (1991) nevner i likhet med Rosness et al. (2004) redundans som et viktig element for å ha en høy pålitelig organisasjon (HRO). Det handler om å ha flere lag med sikkerhet, for eksempel ved å ha overlappende kompetanse blant personell, eller overlappende funksjoner i et system. Det betyr at dersom en person eller en funksjon skulle bli satt ut av spill, besitter en annen person kompetansen og kan tre inn, eller en annen komponent tar over funksjonen i et system.

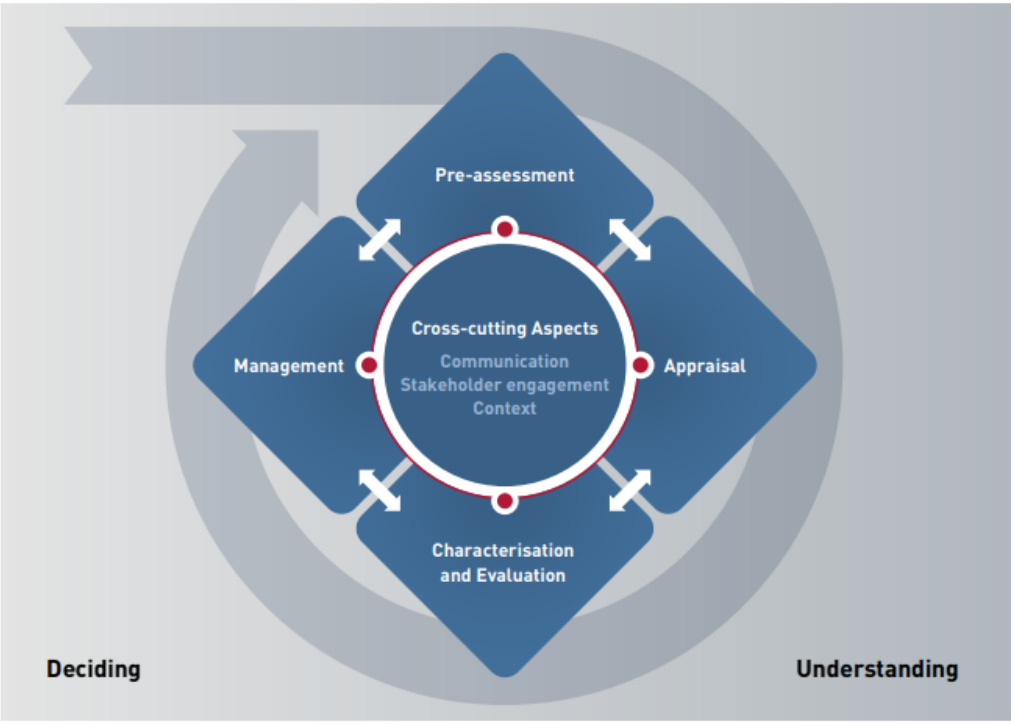
Spontan omstilling handler om at en organisasjon kan omstille seg når hendelser eller situasjonen endrer seg eller krever det. For eksempel kan dette knyttes opp mot desentralisering av beslutninger, ettersom enkelte hendelser kan kreve at beslutninger tas hos operatører heller enn i en ledergruppe. Samtidig kan det også bety at beslutningsmyndigheten må sentraliseres dersom det er snakk om strategiske og langsiktige beslutninger. Mindfullness

handler om å ha evnen til å oppdage og håndtere uventede hendelser som kan oppstå ulike steder i organisasjonen (Weick & Sutcliffe, 2007). Mindfullness kan i denne sammenheng forstås som årvåkenhet, som krever at man er oppmerksomme på omgivelsene og systemet man har.

Hollnagl, Woods og Leveson (2006) hevdet at høy pålitelige organisasjoner må være resiliente. Resiliens referer til en organisasjons evne til å takle motgang, og kan omsettes til hvilken evne et system har til å fortsette å eksistere i møte med omfattende endringer (Hollnagl et al., 2006). Sutcliffe og Vogus (2007) trekker resiliens mot proaktivitet, der resiliens handler om å tilpasse seg skiftende og utfordrende forhold uten at organisasjonen opphører, og at dette bidrar til å styrke organisasjonen i ettertid. Ved å ha en proaktiv tilnærming til utfordrende forhold og situasjoner økes organisasjonens resiliens da en slik tilnærming søker å definere sine egne omgivelser og være beredt, heller en å reagere (reaktivt) når omgivelsene plutselig endrer seg. Weick og Sutcliffe (2007) hevder at organisasjoner øker sin resiliens ved å utvikle sine egenskaper og skriver i den forbindelse «to detect, contain and bounce back from those inevetable errors that are part of an interminate world» (Weick & Sutcliffe, 2007, s.14). For å være resiliente må dermed organisasjoner ikke bare håndtere, men også oppdage feil.

3.4 IRGC rammeverket

IRGC-rammeverket fremmer en helhetlig tilnærming til risiko og risikostyring (International Risk Governance Council, 2017). 'Risk Governance' defineres som «å anvende samstyringsprinsipper under identifikasjon, vurdering, styring og kommunikasjon av risiko» (SRA, 2018, s.8). Rammeverket inkluderer en multidisiplinær forståelse, samtidig som det inkluderer en rekke ulike aktører og interessenter i risikostyringsprosessen. Det er et rammeverk som forsøker å bedre håndteringen av risiko knyttet til systemer og situasjoner som er preget av kompleksitet, usikkerhet og tvetydighet (SRA, 2018). Videre bidrar rammeverket til tidlig identifisering og håndtering av risiko, på tvers av interessenter. Det som er unikt med dette rammeverket er at det inkluderer de aspektene som er nødvendige for å forstå risiko, men også for å ta avgjørelser for å håndtere risiko. Den tilbyr altså å generere og evaluere kunnskap, samtidig som den muliggjør beslutningstaking og styring (Renn, 2008).



Figur 3: IRGC-modellen (IRGC, 2017)

Modellen skisserer 5 aspekter knyttet til risiko, som alle på en eller annen måte henger sammen og bygger videre på hverandre. Man jobber ofte frem og tilbake mellom de ulike aspektene for å skape en kontinuerlig prosess i tråd med utviklingen av risiko.
For finanssektoren er rammeverket institusjonalisert i praksisen som gjennomføres ved at man skal ha en risikobasert tilnærming til måten man driver virksomheten på. Særlig knyttet til risikovurdering og risikostyring gir IRGC rammeverket noen interessante elementer som kan omsettes til cyber-risiko i finanssektoren. Risikovurdering handler i korte trekk om å vurdere hvilke implikasjoner en risiko kan ha for virksomheten og dens verdier, i samråd med ulike interessenter.

Risikostyring er den prosessen hvor risikovurderingen inkluderes, der man forsøker å styre risiko. Renn (2008) belyser at det finnes ulike strategier for risikostyring, og at virksomheter burde søke å ha en bred beslutningstaking om hvilke tiltak som skal innføres for å redusere, håndtere og respondere på eventuelle risikoer. I finanssektoren er det flere interessenter og regulerende myndigheter som bidrar til å styre cyber-risiko. IKT-forskriften er et godt eksempel på hvordan samstyring (*governance*) har bidratt til å styre cyber-risiko, og hvordan denne skal reguleres.

3.5 Oppsummering av teori

I dette kapittelet er det teoretiske fundamentet i oppgaven redegjort for. Ettersom det blir brukt mer enn én teori for å besvare oppgavens problemstilling, vil de ulike teoriene sammen bidra til å belyse problemstilling og tilhørende forskningsspørsmål. Begreper knyttet til risiko vil bli brukt i kapittel 6 sammen med hvordan distinksjonen mellom «safety» og «security» påvirker forståelse og tilnærming til cyber-risiko, -trusler og -farer. Risiko- og sårbarhetsanalyse er definert slik at leser skal være innforstått med hva det innebærer, ettersom oppgaven i stor grad bygger på studie av ROS-analyser.

Risikostyring, eller sikkerhetsstyring slik som Aven et al (2017) referer til, er sentralt i hele oppgaven da det innebærer ulike forståelser og prosesser knyttet til styringen av cyber-risiko. Charles Perrow (1984) sin teori om normale ulykker særlig knyttet opp mot kompleksitet, i tillegg til high reliability theory sitt fokus på pålitelige organisasjoner, årvåkenhet og organisatorisk resiliens, vil bli brukt om hverandre i drøftingskapittelet. De ulike tilnærmingene vil bli diskutert om hverandre da de på hver sin måte belyser funnene i oppgaven. IRGC-rammeverket vil bli anvendt i undersøkelsen av risikostyring, og i forhold til hvordan risikostyring har endret seg. Det vil særlig bli lagt vekt på de ulike prosessene knyttet til risikostyring – da det i denne oppgaven forstås som en kontinuerlig og dynamisk prosess. Gjennom kapittel 6 vil teorien bli drøftet opp mot funnene som blir presentert i kapittel 5.

4. Forskningsmetode

Dette kapittelet beskriver valg av metode og hvilke avgjørelser som er tatt gjennom forskningsprosessen for å belyse problemstilling og forskningsspørsmål. Valget av metode, innsamling og bearbeiding av data vil bli redegjort for i dette kapittelet. Dernest redegjøres det for kvalitetskriteriene reliabilitet, validitet og overførbarhet. Til slutt vil styrker og svakheter ved metoden belyses.

4.1 Metodisk tilnærming

4.1.1 Forskningsdesign

Forskningsdesignet som anvendes i denne oppgaven er et sted mellom induksjon og deduksjon, nemlig en abduktiv tilnærming. Induksjon vil ofte være knyttet til kvalitative metoder ved å fortolke empiri, mens deduksjon søker å bekrefte hypoteser og teorier som allerede eksisterer – og sammenfaller med kvantitativ metode. Abduksjon bygger på en stegvis-deduktiv-induktiv metode, som kontinuerlig arbeider mellom induksjon og deduksjon. Denne tilnærmingen ble valgt ettersom jeg ønsket at empiri og teori begge skulle bidra til å besvare problemstillingen, samtidig som jeg ikke ønsket å låse mitt metodiske utgangspunkt til ren induksjon eller deduksjon. Jeg ønsket å være åpen for å la innsamlet empiri lede forskningsarbeidet. Tjora (2012) skriver at man med en abduktiv tilnærming starter fra empirien, og vil i løpet av forskningsprosessen ta nytte av teorier og perspektiver som hjelper å forstå det genererte datamaterialet (Tjora, 2012). Det betraktes som et eksplorerende design hvor problemstillingene har vært flytende, for å øke innsikten og forståelse underveis. Tjora sin (2012) fremstilling av abduktiv metode sammenfaller med hvilken tilnærming jeg har hatt gjennom forskningsprosessen, helt fra start til slutt.

4.1.2 Kvalitativ forskningsmetode

I denne oppgaven er det valgt å ta i bruk kvalitativ metode, for å øke innsikt og skape forståelse for temaet som undersøkes. Gjennom søk etter informasjon i dokumenter og samtale med informanter har det blitt samlet inn data for å skape en god forståelse for temaet. I samfunnsvitenskapelig forskningsmetode skilles det mellom to metoder, kvalitativ og kvantitativ metode. Skillet mellom metodene handler om hvordan jeg har samlet inn og analysert data. Med kvantitativ metode vil det vanligvis tas i bruk tall for å generere statistikk, mens jeg har gjennom kvalitativ metode forsøkt å skape forståelse for temaet gjennom

samtale og dialog (Johannessen et al., 2011). Et annet skille mellom kvantitativ og kvalitativ metode er at man i kvantitativ metode samler inn data, mens man i kvalitativ metode både genererer og samler inn data (Tjora, 2012). Når man beskriver hva sosiale aktører mener og fortolker, er det nyttig å være kjent med begrepene ontologi, epistemologi og metodologi.

4.1.2.1 Ontologi, epistemologi og metodologi

I dette studiet har forsker og informanter ulike ontologier knyttet til temaet i oppgaven. Ontologi, epistemologi og metodologi er tett sammenvevde begreper, og de tre begrepene vil gjerne være lettere å forstå dersom de sees i sammenheng med hverandre. Ontologi referer til den virkelighetsoppfatningen man har, og beskrives som læren om hvordan verden faktisk ser ut. Det er sentralt at man som forsker og leser er bevisste over hvordan ulike ontologier påvirker informanters forståelse for temaet som utforskes. Det er vanskelig å gi en universell forklaring på hva verden er, da det er ulike ontologier i forståelsen av verden. En ontologi kan så beskrives som et element som gir ulike forutsetninger for menneske og samfunn når de skaper et bilde av virkeligheten. Forutsetninger og antakelser kan ha stor betydning for hvordan man tolker resultater og hvilke konklusjoner man trekker, og derfor er det viktig å tydeliggjøre og begrunne dem (Johannessen et al., 2011).

Epistemologi beskrives som læren om å lære, altså læren om kunnskap. Ettersom mennesker og samfunn har ulike ontologier, finnes det uenighet om hvordan man samler kunnskap om verden, og i hvilken grad det faktisk er mulig å tilegne seg en objektiv virkelighetsforståelse. Hva er egentlig kunnskap om verden, og hva er ikke? Metodologi handler om hvilke metoder som anvendes for å samle inn kunnskap om verden (Tjora, 2012). Metoden for å kartlegge virkeligheten, vil så være avhengig av hvilket syn man har på virkeligheten som man ønsker å belyse. Årsaken til at man må være kjent med disse begrepene, er at det bidrar til å belyse hvordan samspillet mellom virkelighetsforståelse, kunnskap og metode påvirker forskningsprosjekter mer eller mindre ubevisst. Analyse av dokumenter vil i stor grad være preget av min ontologi, mens dybdeintervjuer har bidratt til informantenes egen ontologi kommer frem, basert på deres oppfattelse og forståelse av temaet.

4.1.3 Valg av forskningsstrategi

Blakie (2010) skriver at en forskningsstrategi handler om prosedyrene som foreligger for å besvare problemstilling og forskningsspørsmål. Forskningsprosessen består av ulike trinn og

kan betraktes som en læringsprosess. Basert på dialog med informanter og analyse av dokumenter er det mulig å presentere en forståelse av hvordan trusler har utviklet seg, på hvilken måte farer påvirker risiko og hvordan risikostyring har utviklet seg. Samlet bidrar dette til å besvare målet med oppgaven, nemlig forståelsen for hvorfor cyber-risiko i finanssektoren har endret seg de siste 10 årene. Gjennomføringen av forskningsstrategien er presentert i tabell 1.

Når	Hva ble gjort	Hensikt	Oppnådd resultat
Januar	Utarbeidet problemstilling og forskningsspørsmål rettet mot beredskap for cyber-hendelser i samråd med arbeidsgiver. Utarbeidet skisse med innledning, kontekst, systembeskrivelse av arbeidsgiver, oppbygning av organisasjon og skissering av intervjuguide. Lette etter relevante dokumenter om beredskap og cybersikkerhet i finanssektoren, samt undersøkelse av nasjonale rapporter om risiko og trusselbilde mot Norge.	Ønsket å komme i gang med oppgaven så fort som mulig for å være tidlig ute dersom det oppsto problemer i forhold til samarbeid med arbeidsgiver. Skisseringen av intervjuguide ble gjort for å forsikre meg om at spørsmål kunne besvares uten at informanter brøt sin taushetsplikt. Ville lese meg opp på foreliggende dokumentasjon for å generere og moderere intervjuguide, samt øke min egen kunnskap for temaet og systemet jeg ønsket å undersøke.	Fikk kontakt med relevante personer hos min arbeidsgiver, og fant dermed aktuelle kandidater til intervju. Førsteutkast ble utarbeidet og var klar til levering frem til arbeidsgiver og jeg innså at oppgaven undersøkte et tema hvor funn kunne gi potensielle sårbarheter for virksomheten. 1. Februar ble den opprinnelige oppgaven trukket av arbeidsgiver.
Februar	Startet på ny og forsøkte å finne et nytt tema og tilhørende problemstilling for ny oppgave. På bakgrunn av veiledning ble det bestemt å holde temaet på cyber innenfor finanssektoren. Gjennomførte litteratursøk for å finne flere tilgjengelige dokumenter, rapporter og utredninger. Modererte metodevalg, teori og søkte etter nye informanter for intervju. Laget derfor en liste med aktuelle informanter. Startet med innledning og kontekstkapittel.	Utarbeide en problemstilling og et tema som var gjennomførbart uten at mine funn ville medføre sårbarhet for finanssektor eller systemene jeg ønsket å undersøke. Utvalgt litteratur ville bidra til å spisse problemstilling, øke min kompetanse og forståelse for finanssektoren. Samtidig ville dokumenter være nyttige i utarbeidelse av ny intervjuguide. Fullførte intervjuguide. Listen over potensielle informanter ble brukt som et logisk utgangspunkt for videre arbeid. Startet på innlednings- og kontekstkapittel for å komme i gang med skriveprosessen.	Et nytt utgangspunkt for oppgaven ble etablert. Dokumentene bidro til å generere kategorier for intervjuguide, samtidig som analysen av dokumentene ga interessante funn som belyste temaet jeg undersøkte. Intervjuguide ble ferdigstilt med rom for senere modifikasjoner, og aktuelle intervjuobjekter ble identifisert. Etablerte kontakt med potensielle informanter. Innledning og kontekstkapittelet bidro til å «få i gang» oppgaven og tankeprosessen.

Når	Hva ble gjort	Hensikt	Oppnådd resultat
Mars	Fortsatt skrivingen av innledning og kontekstkapittel, for å bygge videre mot teori og metode-kapittel. Gjennomførte 5 intervju med informanter som defineres som tilsynsmyndighet og systemeier. Transkriberte intervjuene etter hvert intervju for å forbedre intervjuguide. Kontaktet nøkkelinformanter utenfor den logiske defineringen av utvalg, da det var vanskelig å komme i kontakt og få svar fra informanter. Skrev videre på metode og startet på empirikapittel.	Ønsket å ferdigstille det jeg hadde mulighet til å ferdigstille, slik at jeg kunne få tilbakemelding på arbeidet. Intervjuene ble gjort for å samle inn data om temaet, samt øke min forståelse og peke retning for videre teorivalg. Ønsket å skrive ut intervju for å finne kategorier samt forbedre intervjuguide og egen opptreden under intervju. Nøkkelinformanter ble inkludert på bakgrunn av utfordring med å etablere kontakt og ved at temaet gikk utenfor finansielle transaksjoner.	Fullførte første utkast for innledning og kontekst. Modererte intervjuguide etter transkribering av intervju. Nøkkelinformantene bidro til å belyse temaet på en friere og mer åpen måte, og jeg oppnådde en bredere forståelse for temaet. Transkriberingen bidro til å starte empirikapittelet som sammen med dokumentstudiets analyse skapte et godt samspill mellom funn.
April	Gjennomførte 5 intervjuer med nøkkelinformanter og driftsleverandører. Skrev ut intervju og starte analyse av dem. Leverte førsteutkast i midten av april. Modererte problemstilling og forskningsspørsmål. Skrev videre på empirikapittel og startet på drøftingskapittel.	Genererte mer datamateriale til analyse og empiri. Analyse bidro til å videreføre empirikapittel og forståelsesprosessen for datamaterialet. Empiri-kapittelets utforming og foreløpige funn bidro til å spisse problemstilling og strukturere valg av teori. Skrev ut en foreløpig konklusjon for å vitalisere kunnskap og sørge for at drøftingen inkluderte funnene.	Reflekterte over om det som har blitt undersøkt faktisk besvarer problemstilling og hva som er de største funn til nå. Empirikapittelet bidro til å endre problemstilling, samt fikk start på drøftingsprosessen. En foreløpig konklusjon bidro til å bevisstgjøre hvordan drøftingen kunne forbedres, samt hvilke momenter drøftingen burde inkludere.

Når	Hva ble gjort	Hensikt	Oppnådd resultat
Mai	Kontaktet flere informanter for å generere mer datamateriale. I all hovedsak ble driftsleverandører og systemeiere kontaktet. Gjennomførte ett oppfølgningsintervju. Utvidet dokumentstudiet til å inkludere publikasjoner fra 2019. Omstrukturerte metodekapittel slik at det reflekterte min studie, for så at teorien støttet opp om mine metodiske valg. Omstrukturerte empiri-kapittelet tre ganger grunnet utydelige skiller mellom funnene. Modererte forskningsspørsmålenes ordlyd. Ferdigstilte empiri og drøftingskapittel, samt arbeidet videre med konklusjon.	Ønsket å intervjue flere driftsleverandører og systemeiere for å få en bredere representasjon fra den logiske defineringen. Oppfølgningsintervjuet hadde som hensikt å skaffe mer utfyllende informasjon, da informanten ble vurdert som svært kunnskapsrik og kunne bidra til flere interessante funn. Valgte å inkludere flere dokumenter da de tilbydde informasjon om det siste året. Gjorde en omstrukturering av metodekapittelet for å demonstrere at innsamlede data var fremdriften i metodeprosessen, og ikke teori. Omstruktureringen av empiri skulle også sørge for at det var en logisk sammenheng mellom teori, empiri og drøfting, og for å tydeliggjøre skiller mellom funn.	Lyktes ikke i å komme i kontakt med flere driftsleverandører eller systemeiere. Oppfølgingsintervjuet ga noen interessante funn, og basert på dette konkluderte jeg med at det ikke var behov for flere intervju. Ved å inkludere dokumenter som ble publisert i 2019 ble det gjort interessante funn knyttet til endring og utvikling til oppgavens overordnede tema. Metodekapittelets omstrukturering resulterte i at forskningsprosessen kom tydelig frem, og at forskningsprosjektets metode er støttet opp av metodelitteraturen. Omstruktureringen av empiri ble ved fjerde forsøk vellykket, og kapittelet ble ferdigstilt. Etter omstruktureringen ble det lettere å ferdigstille drøftingskapittelet, noe som synliggjorde den røde tråden gjennom oppgaven.
Juni	Modererte teksten slik at den hang sammen. Satt inn alle referanser og dobbeltsjekket tabeller og figurer. Korrektur ble lest.	Teksten ble justert, skrivefeil og språk ble korrigert. Ville forsikre meg om at det var en rød tråd gjennom hele teksten, og fjerne uklarheter.	Oppgaven ble levert 14. Juni 2019.

Tabell 1: Oversikt over fremdrift i forskningsprosjektet

Tabell 1 er en grundig gjengivelse av forskningsprosessen, og ble inkludert da den illustrerer den omfattende prosessen dette prosjektet har vært. Videre demonstreres det at det ikke har vært en lineær prosess, samt at det er gjort endringer underveis for å nå oppgavens målsetning.

4.2 Datainnsamling

Kvalitativ metode har vært utgangspunktet for å samle inn data i dette studiet. Gjennom dokumentstudiet har det blitt gjort en omfattende datainnsamling. Dokumentene som har blitt tatt i bruk er offentlig tilgjengelige på nett og er opplistet i vedlegg 1. Totalt har 62

dokumenter dannet grunnlaget for dokumentstudiet. En rekke ulike dokumenter er blitt tatt i bruk; nasjonale trussel- og risikovurderinger, IKT-risikorapporter, offentlige utredninger, sektorspesifikke risiko-, og sårbarhetsanalyser samt supplerende dokumenter fra relevante aktører. Videre har flere utgivelser av de ulike dokumentene blitt analysert for å kartlegge utviklingen over det siste tiåret. Derfor har for eksempel finanstilsynet sine årlige ROS-analyser fra 2009-2019 blitt analysert.

I dokumentene har jeg søkt etter alt som er relevant i forhold til cyber-risiko, cyber-trusler, ulike utviklingstrekk og tilnærming til risikostyring. Ved å gjøre ordsøk har det vært mulig å kartlegge hvor mange ganger begreper har blitt nevnt, eksempelvis antall ganger ordet «cyber» blir nevnt – dette vil bli trukket frem i kapittel 5. Ordsøk er ikke gjort med hensikten å kvantifisere, men fordi ordsøking og følgende tallfesting viser hvordan fokus har utviklet seg. Ved å analysere årlige publikasjoner over en tiårsperiode belyses trekk ved utviklingen av tilnærmingen til temaet. Eksempler på dette er hvordan begrepet IKT-sikkerhet og cybersikkerhet blir anvendt på tvers av de ulike dokumentene. Dokumentene som er tatt i bruk har blitt skrevet for å skildre hva som har vært fremtredende det gjeldende året, og gjør det mulig å trekke objektive fakta om trender, trusler og risikoer fra utgivelsesåret. Basert på dokumentene har det vært mulig å kartlegge rapporterte hendelser både i finanssektoren og i samfunnet forøvrig.

Datamaterialet har blitt bearbeidet for å muliggjøre en grundig analyse. Det ble vurdert om dataprogrammet Nvivo skulle benyttes i analysearbeidet, men jeg besluttet at det ikke var nødvendig. På bakgrunn av at forskningsspørsmålene kunne benyttes som overordnede tema i analyseprosessen fikk arbeidet med analysen svært tidlig en tydelig struktur med hensyn til tema. Deretter tillot de overordnede temaene bruken av reduksjonsteknikker som kategorisering og koding. Ved å trekke ut kategorier og koder fra datamaterialet, spiller forskerens sin subjektivitet inn hever Tjora (2012). Ettersom jeg som forsker har et formål med arbeidet, kan det påvirke retningen av analysen som gjør at det ikke blir en fullstendig objektiv eller nøytral analyseprosess (Blaike, 2010). For å minimere at funnene fra dokumentstudiet er farget av min subjektive fortolkning som forsker, har funnene fra dokumentstudiene bidratt til å danne tema, kategorier og spørsmål i intervjuene. På denne måten har den entydige tolkningen av dokumentene blitt nøytralisert ved bruk av intervjuer.

4.3 Datagenerering

Det andre metoden for å samle inn data ved bruk av kvalitativ metode er datagenerering. Tjora (2012) argumenterer for å bruke datagenerering heller enn datainnsamling i de tilfeller der dataen ikke «finnes», men når den konstrueres i forskningen – som i dybdeintervju. Bruken av intervju har vært hensiktsmessig av flere årsaker. Først og fremst har det gjennom bruk av dybdeintervju vært mulig å få støtte for eller svekke mine antakelser og funn fra dokumentstudiet. For det andre har intervjuene på den ene side bidratt til å gi mer informasjon og kunnskap om funn fra dokumenter, mens de på den andre siden har de gitt helt nye funn som ikke nevnes i dokumentene, samt bidratt til å demonstrere forståelsen av cyber-risiko i finanssektoren. For det tredje har informantene bidratt til å belyse hvilke momenter dokumenter ikke vektlegger, som for eksempel hvordan konkrete trusler forstås av eksperter i finanssektoren.

4.3.1 Logisk definering av utvalg

På bakgrunn av kompleksiteten og størrelsen til finanssektoren, valgte jeg å avgrense oppgaven til betalingssystemet, herunder interbanksystem og system for betalingstjenester. Avgjørelsen om denne avgrensningen ble tatt basert på ønsket om å gå i dybden på ett område i finanssektoren. Avgrensningen krevde kartlegging av ulike aktører som befinner seg i betalingssystemet, hvor funksjonene er tredelt mellom tilsynsmyndighet, systemeier og driftsleverandør. Tabell 6 i vedlegg 2 viser de ulike aktørene som har vært relevante å inkludere i dette studiet. Tabellen bidro til å plukke ut logisk definerte kandidater til intervju, forankret i betalingssystemloven (1999). Underveis som problemstilling og forskningsspørsmål har endret seg, ble det besluttet å inkludere nøkkelinformanter.

Nøkkelinformantene er personer som på et eller annet tidspunkt har befunnet seg i betalingssystemet, men som nå arbeider utenfor selve betalingssystemet. Valg av nøkkelinformanter handler om den kompetansen nøkkelinformanter innehar med tanke på at de har inngående kompetanse på både cybersikkerhet og i finanssektoren. Andersen (2006, s. 279) skriver at nøkkelinformanter er «en person som antas å ha særlig god oversikt over og innsikt i et spørsmål forskeren ønsker å få belyst». Nøkkelinformantene arbeider i og med finanssektoren i funksjoner utenfor betalingssystemet. Nøkkelinformantene var også villige til å la seg intervjue uten de samme bekymringene som informantene som arbeidet i og med betalingssystemet. Ettersom det er mye sensitiv informasjon i finanssektoren og knyttet opp

mot cybersikkerhet, er det naturligvis begrensninger for hva som kan deles. Dermed sto nøkkelinformantene friere til å dele informasjon og kunnskap da de ikke lenger hadde tilknytning til funksjonene gitt i betalingssystemet. Bruken av nøkkelinformanter har bidratt til å styrke empirien i dette studiet, dette vil jeg redegjøre for senere i kapittelet.

På grunn av sensitiviteten knyttet til informasjonen som har blitt delt er anonymitet etterstrebet. Det er valgt å ikke ta i bruk navn, beskrivelser eller karakteristikker som gjenkjenner informantenes person eller virksomheten informanten arbeider i. Anonymisering har hjulpet å generere informanter og verdifull kunnskap, med forbehold at informantens person og virksomhet ble skjermet. Det blir tatt i bruk koder når sitat trekkes frem fra ulike informantene. Følgende koder blir brukt i kapittel 5 og 6 «TM1, SE1, DL1, NI1»: Eksempel: «TM1= tilsynsmyndighet, tall for hvilken person». Utfyllende forklaring av koding som angir bakgrunnsinformasjon om informantene finnes i tabell 7, vedlegg 3.

4.3.2 Intervjusituasjon og intervjuguide

Det har blitt gjennomført totalt 11 dybdeintervjuer i dette studiet, fordelt på 15 informanter. I forkant av første intervju ble det utarbeid en semi-strukturert intervjuguide som var veiledende i intervjusituasjonene. Flere av spørsmålene var utformet i tråd med funn fra dokumentstudiet, for å undersøke hvorvidt disse funnene stemte overens med informantenes forståelser. I prosessen var det helt naturlig at intervjuguiden ble moderert, og det oppleves som uproblematisk ettersom tilnærmingen til oppgaven var abduktiv.

Det var viktig at intervjuguiden ble oppdatert slik at den ga rom for å undersøke andre temaer enn de som var definert fra dokumentene. Intervjuguidens fleksibilitet har tillatt oppmuntrende spørsmål og oppfølgingsspørsmål der det har vært relevant, særlig der informanter kan komme med utfyllende informasjon (Johannessen et al., 2011). Under et dybdeintervju er det ønskelig at informanter får gå inn i dybden på tema hvor de gis muligheten til å reflektere over spørsmålene. Informantene hadde ulik kompetanse og forståelse for temaet som ble undersøkt, og intervjuguiden ble tilpasset på en slik måte at hver enkelt informants ekspertise ble best mulig utnyttet. Funn fra ett intervju bidro til å forme det neste, i tillegg til at funn fra dokumenter skapte utgangspunktet for intervjuguiden.

Intervjusituasjonene har vært forskjellige. Under ett intervju to informanter intervjuet samtidig. Dette var svært formålstjenlig ved at de kunne kommentere og diskutere seg imellom. I dette intervjuet måtte en informant dra tidligere, noe som gjorde at de siste 20 minuttene kun var med en informant. Selv om det var ønskelig at begge informantene ble ut tiden, opplevdes det ikke som problematisk da spørsmålene ble besvart. Alle intervjuene varte mellom 45 og 70 minutter, hvor samtalen i de fleste intervjuer hadde en god flyt. Med unntak av intervjuet der hvor den ene informanten måtte dra, foregikk alle intervjuer uten ytre forstyrrelser eller avbrytelser. Alle intervju, med unntak av ett intervju har blitt tatt opp digitalt, på en kryptert enhet. Årsaken til at jeg ønsket å ta opp intervjuene var å begrense distraksjonene av å ta notater under intervjuene, og slik jeg kunne delta mest mulig aktivt i dialogen med informantene. Opptakene hjalp å forbedre min egen opptreden i neste intervju, ved å konkretisere spørsmål og ved å øke bevisstheten rundt egen opptreden i situasjonen. Bevisstheten om hvordan jeg som forsker hadde muligheten til å påvirke retningen av samtalen, har vært viktig for at hvert intervju skal gi utbytte. En gevinst av å lytte til opptakene flere ganger var for det sørget for riktig transkripsjon og bearbeidelse av data.

Intervjuet som ikke ble tatt opp digitalt skyldes plutselig endring i intervjusituasjonen. Den opprinnelige informanten valgte, uten forvarsel, å inkludere fire av sine kollegaer i intervjuet. Det ble derfor ett intervju med 5 nøkkelinformanter og ga ikke rom for opptak. Informantene tilbydde en oppfølging med individuelle intervju, men mine forespørsler i forhold til planlegging av å gjennomføre disse ble ikke besvart. Ettersom det har vært utfordrende å generere informanter valgte jeg å inkludere dette intervjuet i oppgavens empiri, basert på kunnskapen og den økte forståelsen som jeg tilegnet meg. Notatene jeg skrev underveis har vært nyttige for å sørge for at kunnskapen ble benyttet.

4.3.3 Forholdet mellom forsker og informant

Vanligvis i en intervjusituasjon har forsker styring og kontroll, og det er slike intervjusituasjoner som vanligvis skildres i metodelitteratur. Det representerer ikke alltid virkeligheten. Informantene i dette studiet er høyt utdannede og besitter sentrale posisjoner innenfor finanssektoren. Noen sitter, eller har tidligere sittet, i posisjoner med mye makt. Halvparten av respondentene hadde teknisk utdanningsbakgrunn, mens den andre halvparten hadde økonomibakgrunn. De fleste har jobbet i finanssektoren de siste 10 årene, med unntak av to av informantene som hadde jobbet spesifikt med cyber-risiko og cyber-trusler mot rikets

sikkerhet. Informantene representerer til sammen et solid faglig fundament, supplert med flere tiårs erfaring.

Som masterstudent har jeg følt meg svært underlegen når jeg intervjuet sentrale personer i noen av de største finansvirksomhetene i Norge, både når det kommer til erfaring og kompetanse i finanssektoren og knyttet til tematikken i oppgaven. Til tross for dette har informantene vært åpne, imøtekommende og ivrige etter å dele sin kunnskap og erfaring fra finanssektoren. I enkelte tilfeller kan forholdet mellom informant og forsker føre til en overflod av informasjon. Gleden over å bli intervjuet som en ekspert, sammen med følelsen av å være viktig kan føre til at informanter forteller historier fra sitt liv og sin erfaring, som ikke alltid er relevante for temaet som skal undersøkes (Engen, 2002). Det forekom i flere intervjuer. Det kunne føre til at informantene svarte på det de trodde jeg ville høre, slik at de tilfredstilte meg som forsker (Engen, 2002).

Engen (2002) foreslår at informanter som besitter mektige posisjoner kan bruke det til å påvirke oppførselen under et intervju, samt hvilken informasjon de deler. Det knyttes opp mot deres roller i virksomheter, særlig som ledere. Posisjonene de besitter konstituerer hvordan de prosesser og deler informasjon, dernest vil deres forståelser av virkeligheten bli sosialt konstruert gjennom påvirkning fra sektoren, deres posisjon og rollen de befinner seg i (Berger & Luckmann, 2000). Deres sosiale konstrukt av virkeligheten og deres maktposisjoner kan så bidra til en skjevfordeling i det tradisjonelle maktforholdet mellom forsker og informant. Ved å «kun» være en masterstudent uten teknisk kompetanse eller inngående kjennskap til finanssektoren, tillot jeg meg selv å stille de 'dumme' og 'enkle' spørsmål. Videre ble min underlegenhet en styrke ved at informantene opplevde at de var de virkelige ekspertene på området, som antageligvis førte til økt tillit mellom meg som forsker, og dem som informanter. Intervjusituasjonene har vært påvirket av forholdet mellom forsker og informant, selv om jeg har vært bevisst på det gjennom alle intervjuer.

4.4 Kvalitetskriterier

De vanligste kvalitetskriteriene som anvendes for å sikre forskningens kvalitet er reliabilitet, validitet og overførbarhet (Tjora, 2012: Johannesen et al., 2011). De tre kvalitetskriteriene vil bli redegjort for i denne seksjonen.

4.4.1 Reliabilitet

Reliabilitet postulerer en sammenheng mellom de empiriske funn, analyser og resultat et forskningsprosjekt gir (Tjora, 2012). Under forskningsprosessen er det flere elementer som kan minske reliabiliteten, som for eksempel personlige faktorer som forsker ikke er bevisst på. I dette studiet har jeg valgt en sektor som jeg for tiden jobber i, og et tema som jeg er svært interessert i. Det å være en del av selve sektoren jeg forsker på kan det være en svakhet ettersom det kan påvirke min evne til å være kritisk overfor sektoren. Samtidig har det vært en styrke da det har bidratt til å sette meg i kontakt med en rekke ulike personer i sektoren, også utenfor mitt arbeidsområde. Dernest har det å forske på sektoren samtidig som jeg har jobbet i den gjort meg mer bevisst og nysgjerrig. Tjora (2012) skriver at personlig engasjement både er en styrke og en svakhet i et forskningsprosjekt. Ved å redegjøre for mitt forhold til sektoren, og ved å være bevisst på det gjennom forskningsprosessen, har det minimert potensielle effekter på forskningen.

Min interesse og engasjement for cybersikkerhet og cyber-risiko har bidratt til en søken etter kunnskap for å forstå og lære mer om temaet. De antakelser jeg hadde gjort før jeg startet forskningsprosjektet, både i kraft av å være ansatt i sektoren og min store personlige interesse for tematikken, har jeg vært bevisst på under hele prosessen. Etter at datamaterialet har blitt generert, har det blitt systematisert ut ifra hva det faktisk demonstrerer. Forskningsprosjektets reliabilitet blir i stor grad påvirket av hvordan jeg som forsker og person tolker materialet. Derfor har bruken av opptak gjort mine intervjuer mer pålitelige, da jeg har kunnet forsikre meg om at uttalelsene fra mine informanter har vært korrekte, samtidig har alle informanter fått muligheten til å kvalitetssikre sitatene som har blitt anvendt i oppgaven. Dette styrker relabiliteten til forskningen.

Intervjusituasjonen der Skype ble brukt og der hvor flere informanter ble intervjuet samtidig, kan påvirke reliabilitet. Gjennom Skype kan man miste verdifull interaksjon mellom forsker og informant, noe som er en svakhet i forsøket på å skape dialog. Likevel opplevdes intervjuet som vellykket og dialogen var god. En ytterligere styrke ved Skype-intervjuet var at samtalen ble tatt opp og at det var mulighet for videre oppfølging etter intervjuet. Årsaken til at Skype ble benyttet for å gjennomføre intervju var for informanten befant seg i utlandet. Ett intervju ble gjennomført med to informanter simultant. Det var en styrke ved at de fikk muligheten til å utfylle og kommentere hverandres påstander, men det kan også være en svakhet ved at de

ikke delte deres egne personlige forståelser. Dette ble kompensert med et oppfølgingsintervju med respondenten som forlot intervjuet tidlig.

4.4.2 Validitet

Et prosjekts validitet, også henvist til som gyldighet, omhandler om man svarer på det man søker å besvare, og om det genererte datamaterialet besvarer problemstilling og forskningsspørsmål (Tjora, 2012). Gjennom forskningsprosessen har jeg flere ganger endret problemstilling og forskningsspørsmål. Det er ofte slik at forskere må justere sitt prosjekt underveis, særlig i møte med feltet man studerer. Ettersom jeg startet på en oppgave som tok for seg en virksomhets beredskap for IKT-hendelser, men underveis opplevde at sårbarheten knyttet til mine funn ville bli for store, måtte jeg endre oppgave. Denne bevisstheten kom ikke før jeg møtte feltet og skulle starte med intervjuer. Validitet har vært viktig gjennom hele prosessen, og problemstilling har derfor blitt brukt som et rammeverktøy som har blitt spisset gjennom innsamlingen av data – og etterhvert som jeg økte min kunnskap for temaet.

For å øke validiteten av min forskning har det blitt tatt i bruk litteratur som handler om cybersikkerhet og cyber-risiko i finanssektoren. Tidligere forskning har blitt brukt for å skape et solid fundament og støtte opp om empiriske funn i forskningsprosjektet. I retrospekt, ser jeg at intervjuguiden kunne hatt et bedre utgangspunkt – og flere av spørsmålene ble eliminert da de ikke var relevante. En annen utfordring knyttet til kvaliteten av data er at de fleste dokumenter er publisert i en offentlig kontekst. Interne dokumenter, analyser og vurdering ble ikke gjort tilgjengelige for dette studiet, grunnet faren for økt sårbarhet. Offentlige dokumenter er ofte preget av å tilbakeholde sensitive opplysninger, selv om de kommer med relevante bemerkninger. De blir gjerne moderert eller ikke gjort tilgjengelige i det hele tatt for offentligheten (Scott, 1990).

En utfordring er den historiske tilnærmingen i studiet. Informantene kan ha vanskeligheter med å huske detaljer over tid. Ettersom jeg undersøker en periode på 10 år, kan det være vanskelig for informanter å huske nøyaktige endringer fra år til år. Det som har bidratt til å øke validiteten er at informantene har bekreftet eller kommentert funn fra dokumentstudiet. Den siste utfordringen jeg ønsker å belyse er tematikken i oppgaven. Spørsmål knyttet mot risiko, trussel og sårbarhet flyter over i hverandre i svarene til informanter. De ulike tilnærmingene og forståelsene av risiko blant informantene bidrar til å forklare dette. I kapittel

5 blir dette redegjort for. På tross av dette, er jeg trygg på at den grundige gjennomgangen av dokumenter og intervju har bidratt til å forklare hvorfor cyber-risiko har utviklet seg i finanssektoren de siste 10 årene, samtidig som funn er støttet av tidligere forskning.

4.4.3 Overførbarhet

Dette forskningsprosjektet er et lite prosjekt, avgrenset til én sektor. En ytterligere avgrensing har blitt gjort til finansielle transaksjoner og i henhold til utvalget av informanter som ble logisk definert ut ifra aktører underlagt betalingssystemloven. Målet med samfunnsvitenskapelig forskning er ofte at den skal være overførbar og generaliserbar hevder Tjora (2012). Dette prosjektet, dets avgrensninger og derav begrensninger påvirker overførbarhet og generalisering. Funnene kan generaliseres til bank og betalingsformidlingstjenester, da både forsikring og verdipapir ikke har vært et fokus eller blir representert i dette studiet. Antageligvis vil ikke funnene være gyldige for alle virksomheter, men de demonstrerer cyber-trusler og cyber-farer, i tillegg til forståelsen av dem i finanssektoren. Det må også tas med i betraktningen at det er forskjeller mellom små og store virksomheter med tanke på hvordan en potensiell trussel eller fare kan materialisere seg.

4.5 Metodiske styrker og svakheter

Det finnes ulike metoder for å samle inn data i et forskningsprosjekt, som på ulike måter belyser et tema. Kvalitativ metode har både styrker og svakheter med sin metodologi. Triangulering gjennom å bruke både kvalitativ og kvantitativ metode, ville styrket forskningen særlig dersom funnene ble brukt for å belyse temaet på ulike, men komplementære måter. I denne omgang ble det besluttet å ikke gjøre en triangulering, basert på gjennomføringen av et omfattende dokumentstudie og den brede ekspertisen som er representert i utvalget av informanter.

Gjennom dokumentstudiet har det vært mulig å kartlegge cyber-risiko i finanssektoren over en tiårsperiode, basert på tilgjengelige dokumenter. Det har vært en styrke da det har vært mulig å avdekke utviklingstrekk som kunne undersøkes nærmere gjennom intervju. Intervjuene styrket datamateriale, ved at det ga et beriket kvalitativt materiale gjennom den unike ekspertisen hos informantene. Ekspertisen kom frem gjennom deres kunnskap og erfaring, samt variasjonen blant informantene. En styrke ved metoden er at man undersøker eksperters fortolkninger og forståelser. Derimot kan det være en svakhet dersom

ekspertkunnskap overskygger andre funn. Det er også en svakhet at det er usikkerhet om hvorvidt funnene er representative på nasjonalt og internasjonalt nivå, grunnet et begrenset utvalg. Datagrunnlaget er rett og slett for lite. Dersom det hadde blitt tatt i bruk kvantitative standardiserte spørreundersøkelser, er det tenkelig at utvalget ville blitt større, slik at det økte sin representativitet. Temaet som undersøkes er relativt «nytt» og det finnes lite tilgjengelige statistikker eller kvantifiseringer knyttet til tematikken. En kvantifisering ville trolig ikke styrket empirien nevneverdig. Kvantitative metoder gir muligheten til å øke datagrunnlaget og generaliseringsmulighet, men bidrar dermed med oversikt heller enn innsikt.

Kvalitativ metode blir kritisert for å være basert på forskers subjektivitet, og kritikken rettes både mot informanter og mot forsker. Ettersom jeg har en relasjon til finanssektoren, vil dette kunne betraktes som en svakhet – da det kan ha påvirket hvordan informantene responderte. I kartleggingen av utviklingen av cyber-risiko, bidrar det kvalitative materiale til å se helhet og sammenhenger, samt at det skaper forståelse rundt hvorfor utviklingen har vært som den har. Dette gjøres best ved å være i kontakt med feltet, og ved å kombinere skrevne dokumenter med levende informanter (Dalland, 2007; Jacobsen, 2005). Den kvalitative metoden har vært den beste metoden for å gjøre dette, og abduktiv forskningsstrategi har tillat veksling mellom teori og empiri. Det er en styrke i denne studien.

5. Empiri

I dette kapittelet presenteres funn som har blitt hentet ut fra 62 dokumenter og 11 intervjuer, som beskrevet i kapittel 4. Disse funnene bidrar til å svare på problemstillingen:

Hvorfor har cyber-risiko i finanssektoren utviklet seg de siste 10 årene?

Forskningsspørsmålene som bidrar til å besvare problemstillingen, utgjør strukturen i dette kapittelet. Det må likevel påpekes at flere av funnene glir over i hverandre, noe som gjør at det ikke alltid er tydelige skiller mellom funnene.

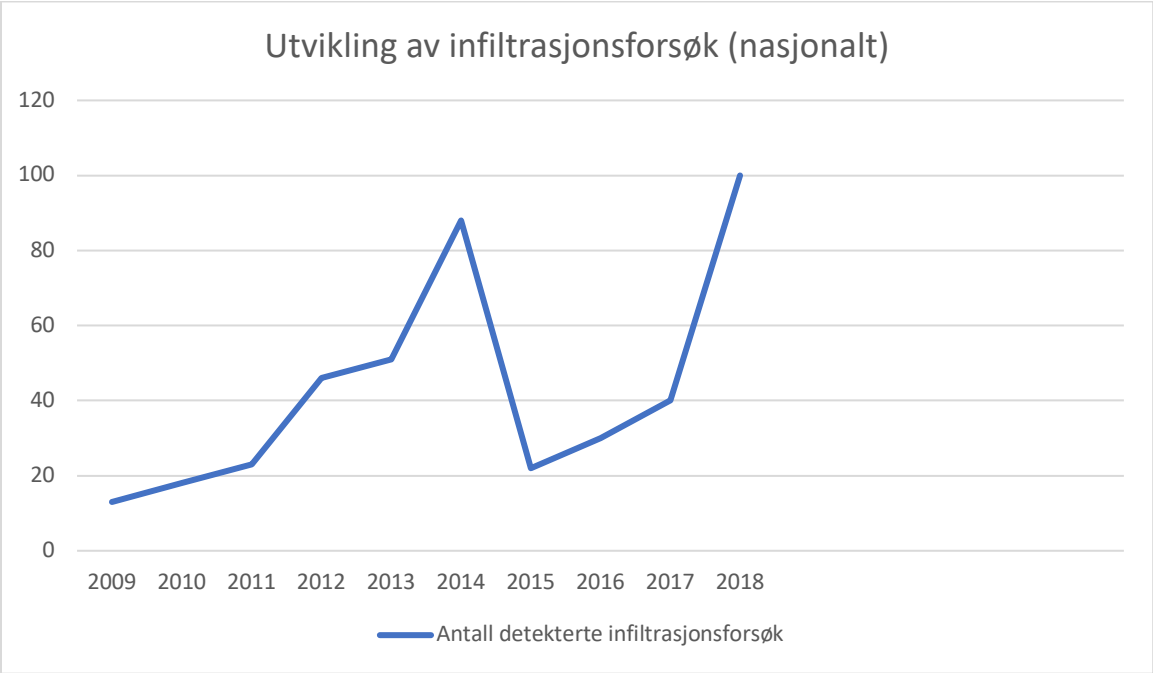
5.1 Hvordan har cyber-truslene mot finanssektoren utviklet seg de siste 10 år?

5.1.1 Nasjonalt trusselbilde

Det siste tiåret har risikobildet endret seg på flere måter, men flere trusler har holdt seg relativt stabile. PST trakk i trusselvurderingen for 2009 frem etterretningsvirksomhet mot Norge og norske interesser som høy (PST, 2009), og det samme ble skildret i trusselvurderingen for 2018 (PST, 2018). Selv om denne trusselen har vært vedvarende høy de siste 10 årene har det vært stor utvikling i metodikken som anvendes for å gjennomføre etterretningsoperasjoner. I 2009 vurderte PST at trusselen for etterretning i all hovedsak forekom gjennom tradisjonelle etterretningsmetoder, men at «flere stater er i ferd med å bygge opp betydelig kapasitet innenfor datanettverksoperasjoner» (PST, 2009). Datanettverksoperasjoner ble vurdert som en av de største truslene for både spionasje og informasjonsuthenting.

I 2009 ble det fremmet forslag om å øke den forebyggende innsatsen for å redusere sårbarhet i systemer, og i 2010 ble nødvendigheten av mer forebyggende innsats tydelig demonstrert. I NSM sin årsrapport, *Årsrapport om Sikkerhetstilstanden 2010*, avdekkes det nemlig alvorlige hendelser knyttet til forsøk på spionasje og IKT-angrep mot norske interesser (NSM, 2010). Gjennom bruk av e-poster med ondsinnede programvarer, bruk av trojanere og tjenestenektangrep ble departementer, embetsmenn, forsvaret og ammunisjonsprodusenten AMMO rammet av flere angrep (NSM, 2010). Intensiveringen av cyberangrep har siden 2009 vært økende, og gjennom dokumentstudiet er det funnet at antall hendelser og alvorlige sikkerhetshendelser har vært økende (NSM, 2018a NSM, 2018b,). NSM trakk i 2015 frem at selv om antall alvorlige angrep ser ut til å være betydelig redusert (fra 88 angrep i 2014 til 22

angrep i 2015) så skyldes reduseringen at utformingen av angrep har endret seg. Fra 2014 til 2015 ble angrepene enda mer avanserte og komplekse, hvilket førte til at håndteringen av det som ville bli klassifisert som et alvorlig angrep i 2014, ikke nødvendigvis kunne klassifiseres som det samme i 2015. De 22 angrepene som NorCERT håndterte i 2015, var spesialtilpasset og såpass avanserte at de ikke kunne sammenlignes med tidligere år. Figur 1 demonstrerer utviklingen i antall infiltrasjonsforsøk på norske virksomheter fra 2009 til 2018 (NSM, 2009-2018a).

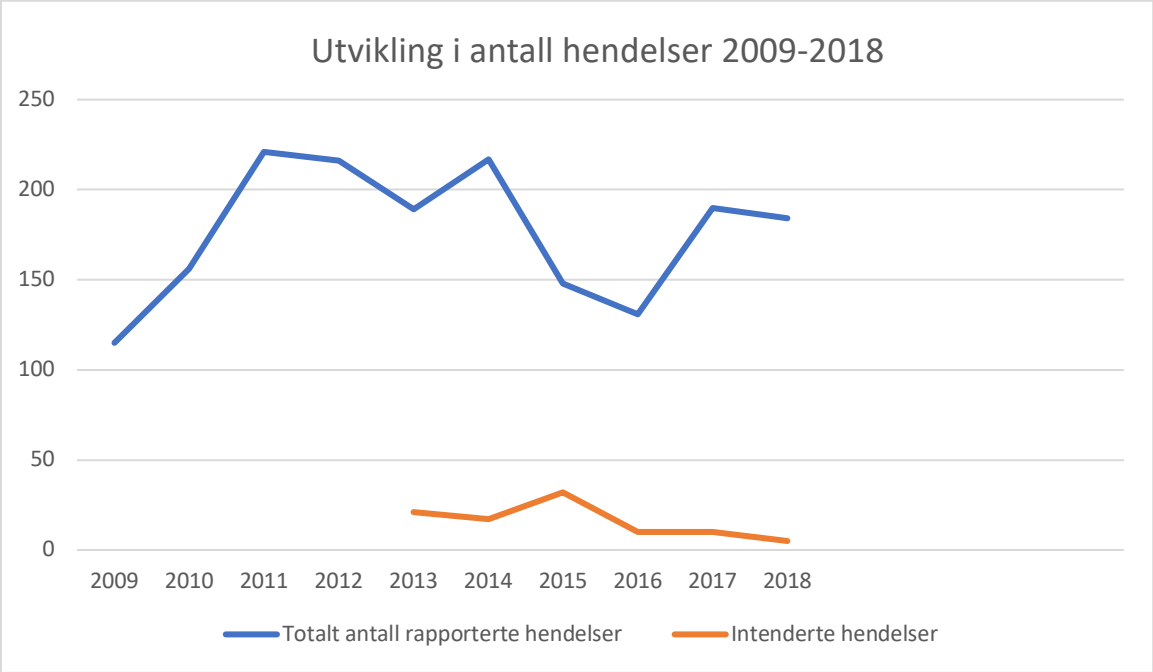


Figur 4: Antall detekterte infiltrasjonsforsøk 2009-2018

Det har vært flere endringer i angrepsmetodikken det siste tiåret. Endringene i angrepsmetodikken skyldes blant annet at kompleksiteten i både angrep og de tekniske systemene som brukes har økt. NSM skriver at «kompleksiteten er den største sårbarheten i det norske digitale samfunnet i dag» (NSM, 2018a, s.13). Det skyldes at de digitale løsningene består av lange verdikjeder, og tett koblede løsninger både i en sektor, men også på tvers av sektorer (NOU 2015:13). På en side vanskeliggjør det hendelseshåndtering, mens på den andre siden har det gjort hendelser vanskeligere å detektere. Kompleksdrivende teknologitrender som kunstig intelligens og robotisering er en trussel som har vokst særlig de siste årene, og det forventes at trusselaktører vil ta i bruk disse for å utvikle mer effektive metoder for å angripe sine mål (NSM, 2018a). Det nevnes av NSM for første gang i 2017 som en reell trussel.

5.1.2 Cyber-trusler mot finanssektoren

Nasjonale dokumenter og rapporteringer på risiko- og trusselbildet er preget av større overenstemmelser sammenlignet med analyser av trusselbilde for finanssektoren spesifikt. Finanstilsynet startet en frivillig hendelsesrapportering i 2007, som fra 1. Desember 2009 ble omgjort til en pliktig rapportering gjennom IKT-forskriften (Finanstilsynet, 2010). Kravet til rapportering innebærer at aktører i finanssektoren skal rapportere antall cyber-hendelser for å skape en oversikt og strategi for hvordan finanssektoren kan møte trusler. Grafen under baserer seg på finanstilsynets risiko og sårbarhetsanalyser fra 2009 frem til 2018, hvor antall innrapporterte hendelser og intenderte hendelser er illustrert. Det grafen ikke tar høyde for, er hvordan angrepsmetodikken har endret seg.



Figur 5: Antall rapporterte hendelser 2009-2018

Funnene fra Finanstilsynet sine ROS-analyser fra 2009 til 2019 demonstrerer en tydelig utvikling av cyber-risiko sin påvirkning i finanssektoren. For hvert år skrives det stadig mer om temaet, hvilket tyder på økt risikobevissthet og økt fokus hos finanstilsynet og foretakene som rapporterer til finanstilsynet.

I 2009 belyses problematikken og utfordringer som kriminalitet kan gi, men det er lite konkrete utfordringer som nevnes i forbindelse med cyber-trusler og cyber-risiko. Problematikken i finanssektoren fremstilles som at den i større grad er rettet mot kunder og deres betalingskort enn foretak og sektoren forøvrig. Det er et gjennomgående økt fokus på

angrep, selv om det ikke representerer betydelige tap i den norske finanssektoren sammenlignet med det internasjonale bildet. Det er tilnærmet ingen cyber-angrep mot den norske finanssektor, og dersom den digitale sfære brukes er det knyttet til betalingskort og ikke til nettbank. I 2009 og 2010 opplevde bransjen utbredt bruk av skimming-angrep, og det utgjorde en stor trussel for sektoren (Finanstilsynet, 2010; Finanstilsynet, 2011). Særlig i 2010 forekom det flere skimming-angrep mot minibanker, noe som synliggjorde behovet for nye risikoreduserende tiltak. De økonomiske tapene er relatert til tradisjonelle tyveri og ikke internettbaserte angrep. Skytjenester og overflytting til skybaserte løsninger nevnes i 2010 som en risiko da det er umodent for bankenes kjernesystemer.

Både dokumenter og intervjuer demonstrer at det skjer en endring i 2011, og at den norske finanssektoren blir utsatt for en rekke angrep. En av nøkkelinformantene nevnte denne endringen og fortalte følgende: «vi så en veldig oppsving i nettbanktrojanere mot privatkunder i 2011, 2012. Torpig og Zeus var to skadevarer som fikk stor utstrekning i Norge» (NI1). Dette stemmer godt overens med finanstilsynet sine funn, hvor det påpekes at 2011 var året for trojanerangrep mot nettbanker, hvor de mindre bankene led de største tapene som følge av sårbarhet knyttet til svakere forsvarsverk, responskapabiliteter og kompetanse (Finanstilsynet, 2012). Videre eksisterer en økt erkjennelse av at internett åpner for mer organisert digital kriminalitet, hvilket krever at finanssektoren må ligge i forkant. En av systemeierne trakk frem denne erkjennelsen, ved å nevne hvordan tilliten endret seg ved utbredelsen av det moderne internett. Han sa følgende: «når man fant ut at tillit ikke var en forutsetning for bruk av nett, og at man ikke kunne stole på andre folk så man en utvikling i IT-sikkerhet» (SE1).

Finanstilsynet fant gjennom tilsyn en manglende oversikt over robustheten i linjer og avhengighet, hvilket tyder på at finansforetakene i 2011 var sårbare uten selv å være klar over disse sårbarhetene. Det trekkes frem en økning av trusselen for interne misligheter, som utro tjenere som stjeler informasjon, økonomiske verdier eller kompromitterer integriteten i systemer. Videre var trusselen for organisert kriminalitet mot betalingssystemet et pågående og økende problem, selv om risikoen for kriminelle angrep fortsatt var størst i grensesnittet mellom banker og kunder (Finanstilsynet, 2012).

Fra 2011 til 2012 var det en markant økning av tjenestenekt-angrep (DDoS-angrep) mot finanssektoren, samt økte tap på betalingstjenestene. Trusselbildet endret seg noe, ved at det

ble rapportert om flere ondsinnede angrep på nettbank og internetthandler ved bruk av kort (Finanstilsynet, 2013). Kriminelle aktører forsøkte dermed å utnytte kortinformasjon til kunder gjennom internettsider som ikke krevde to-faktorautentifisering. Trojanerangrep forekom gjennom hele året, og trusselen økte gjennom at angrepene ble mer avanserte i 2012. Det trekkes frem noen nye trusler relatert til phishing og rekruttering av digitale «money mules». En bølge med phisning-epost rammet finanssektoren bredt i 2012, men resulterte i henholdsvis få tap. Rekrutteringen av digitale «money mules» demonstrerte at kriminelle trusselaktører utviklet seg og sine metoder for å gjennomføre kriminelle handlinger.

ROS-analysen fra 2013 viste at økningen av DDoS-angrep fortsatte, og digitaliseringen av finanssektoren syntes å gjøre sektoren mer attraktiv for kriminalitet og organiserte angrep mot betalingstjenestene (Finanstilsynet, 2014). Tapene var fortsatt moderate, noe som finanstilsynet mener skyldes et godt samarbeid mellom ulike aktører i sektoren. En forholdvis ny trussel som ble trukket frem i 2013 var malware (skadevare). Denne prosessen skisseres som komplisert og omfattende, samtidig som det vitner om økt kompetanse og erkjennelse om trusselen. Det forekom også en ny bølge av phishing mot finanssektoren, og en økning i phishing via telefon. Spear-phishing økte også i 2013, og dette var første gang spear-phishing nevntes som en trussel i analysene fra finanstilsynet. For første gang nevnte også foretak at de vurderte APT (advanced persistant threat) som en stor risiko. Trusselen for digital industrispionasje ble også trukket frem som en økende og utfordrende trussel.

I 2014 vurderte foretakene trusselen for at inntrengere fikk innsyn i IKT-system og infrastruktur gjennom målrettede angrep som økende. En ny form for trussel var utnyttelse av sikkerhetshull, som igjen øker trusselen for cybercrime. Finanssektoren kom til en ny erkjennelse i 2014, nemlig at digitale angrep kan true det finansielle markedet og finansiell stabilitet. Til tross for dette var risikoen størst i tilknytting til endringer i systemer, infrastruktur og organisasjoner (Finanstilsynet, 2015). Det skjedde omfattende endringer i 2015. Trusselen for angrep direkte på finansforetak og deres system økte. Tidligere år har trusselen vært rettet mot kunder og grensesnittet mellom kunder og banker, men dette ble endret i 2015. Foretakene vurderte blant annet datakriminalitet og inntrenging i systemer, samt brudd på konfidensialitet som de mest fremtredende truslene. Videre viste rapporteringen økt antall svindelangrep mot sektoren, og at svindelscenarioene mot betalingstjenestene er i størst grad basert på phishing. Driftsstabiliteten er et gjennomgående

tema i alle finanstilsynets risikoanalyser, og i 2015 hadde denne risikoen økt, samtidig som det ble observert en tiltakning i ondsinnede angrep mot betalingsformidlingen.

I 2015 nevntes svindel mot bedriftsnettbank og sanntids-phishing som nye metoder som ble anvendt av trusselaktørene. Videre hadde trusselen for utpressing rettet mot banker blitt vanligere, gjerne ved bruk av kryptering og ransomware. 2015 var året hvor ransomware virkelig utfordret sektoren. Cybercrime rettes ikke primært mot kunder eller foretak, men mot begge ved bruk av ulike metoder. Foretak ble utsett for APT og DDoS-angrep, mens kunder ble infisert av ondsinnede koder. Phishing var utbredt for å vinne tillit hos den som ble angrepet, for så å få tilgang til å kompromittere verdier. Tidligere år har trojanere vært hyppig anvendt mot sektoren, og det ble i 2015 identifisert egne bank-trojanere som antas å være skreddersydd for bank og finanssektoren. Banktrojaneren DYRE (også kalt Dyreza) trekkes frem som et slikt eksempel. Funnene fra 2015 tyder på at cybercrime er en fremvoksende industri for kriminelle, og at det ilegges stadig mer ressurser fra kriminelles side for å gjennomføre omfattende angrep. Kunnskap er lettere tilgjengelig gjennom cyber-domenet, hvilket resulterer i at kunnskap om ansatte og foretak kan utnyttes av både fremmede staters etterretningstjenester og kriminelle.

Det var en vesentlig økning i antall svindelangrep fra 2015 til 2016, på hele 48 prosent. En trussel som trekkes frem som økende, til tross for at det ikke forekom noen reelle angrep, var trusselen for angrep på mobilbetalinger. Flere foretak ble i 2016 utsatt for ransomware-angrep, hvilket tyder på at også denne trusselen er økende. En endring i trusselbildet er at kriminelle i større grad benytter seg av phishing og sosial manipulering for å trenge inn i foretakenes systemer. Foretakene vurderer også i 2016 datakriminalitet og inntrenging i system som en vesentlig trussel. En ny svindeltype som ble avdekket er vannhullsangrep, men angrep på betalingstransaksjoner utgjorde hovedtyngden av angrep mot betalingstjenester. Det omfattende SWIFT-angrepet som rammet sentralbanken i Bangladesh tydeliggjorde hvilke konsekvenser dataangrep kan gi, og skapte store uroligheter i finanssektoren. Sikkerhetshull utnyttes aktivt av angripere og sårbarhetene brukes for å ødelegge tjenestene.

I løpet av 2017 ble ingen i den norske finanssektoren rammet av alvorlige dataangrep, til tross for økt aktivitet. Finanstilsynet (2018) rapporterte at risikoen for cyberangrep var forventet å øke, i tillegg til at alvorlighetsgraden av hendelser ville øke. Konsekvensene dersom det først forekom et alvorlig cyberangrep betegnes i 2017 som svært alvorlige, da digitaliseringen har

skapt stor avhengighet og integrasjon av systemer. Trusselen for phishing og sosial manipulering viste seg også å være økende, blant annet ved at trusselaktører rettet fokus både mot økonomisk svindel og tilegnelse av informasjon. Videre ble CEO-svindel trukket frem som en tilstedeværende trussel, og at denne hadde blitt mer utfordrende ettersom de kriminelle har utviklet seg og blitt mer sofistikerte. Selv om risikoen for et cyberangrep var økende i tråd med et uoversiktlig trusselbilde, var sikkerheten i den norske finanssektoren på et nivå som gjør det mer attraktivt å gjennomføre angrep som er mer tradisjonelle og mindre tekniske.

Finanstilsynet ga ut ROS-analyse for 2018 den 9.Mai 2019, og rapporten avdekket flere interessante funn. Den belyste blant annet at trussel fra 2017 til 2018 har økt, og at det forekom 5 sikkerhetshendelser og 184 driftshendelser i 2018 (Finanstilsynet, 2019). De største sårbarhetene knyttes mot operativ drift, cybercrime, konfidensiell informasjon og tilgangsstyring. Det påpekes også at sektoren må fortsette å styrke cybersikkerhet. Videre trekker finanstilsynet frem at kompleksiteten i teknisk infrastruktur er økende og at det er utfordringer knyttet til bruk av ny teknologi.

5.1.3 Trusselaktører

Da en av systemeierne skulle beskrive hvem som er trusselaktørene mot finanssektoren svarte han:

> Trusselaktørene kan være alt fra 14 åringer på gutterommet som med enkle grep kan stelle i stand ganske mye trøbbel, vi har profesjonelle organiserte kriminelle til nasjonalstater, så det er et bredt spekter av trusselaktører som man må beskytte seg mot. (SE2).

Beskrivelsen av et bredt spekter av trusselaktører mot finanssektoren, sammenfaller til en viss grad med trusselaktørene på det nasjonale nivået. NSM (2018a) skiller mellom fire ulike trusselaktører på cyberdomenet: fremmede stater, kriminelle, aktivister (hackivister) og patriotiske hackere. E-tjenesten og PST trekker frem etterretningstjenester og organiserte kriminelle som sentrale trusselaktører (PST, 2018; E-tjenesten, 2018). I trusselvurderingen fra 2015 oppgir PST for første gang Kina som en etterretningstrussel mot Norge, og Kina blir ansett som en sentral trusselaktør de påfølgende årene. I 2019 skriver PST at:

> Det er de russiske sikkerhets- og etterretningstjenestene som vil representere de største utfordringene. Samtidig vil også tjenester fra andre land, som for eksempel Kina, utføre etterretningsoperasjoner mot mål og virksomheter her i landet. Om de lykkes med operasjonene, kan de påføre Norge og norske interesser stor skade (PST, 2019, s.7).

NSM belyser, i likhet med PST og E-tjenesten, at fremmedstatlig etterretning sammen med datakriminalitet representerer de største truslene mot Norges digitale sikkerhet (NSM, 2018a). Aktivister og opportunistiske hackere får mindre oppmerksomhet i dokumentene, og i siste utgivelse av IKT-risikobilde skriver NSM at den digitale risikoen fortsetter å øke og at de største digitale truslene fremdeles kommer fra fremmedstatlig etterretning og datakriminalitet (NSM, 2018a, s.7).

Det siste tiåret har det vært gradvis endring i trusselen fra ulike aktører, samt mangfoldet av at trusselaktører har økt. Endringen og utviklingen av aktørene som representerer en trussel, kan være vanskelige å detektere. En informant belyste denne utfordringen: «trusselaktørene er noe ukjente, men en del angrep er lettere å oppdage, mens de mer avanserte går under radaren, som fra statlige aktører og slik som er vanskeligere å oppdage» (TM1). Videre viste en annen informant til at de ulike grupperingene og modusene som forekommer innenfor cybercrime, øker utfordringene med å håndtere dem. Dette ble forklart på følgende måte:

> Det vil hele tiden være en evig kamp i forhold til at aktører der ute har det som sin profesjon å finne opp noe, mens bankene og foretakene sin profesjon er å avdekke. Det er to forskjellige kompetanser. (TM4).

Finanstilsynet sine rapporter fra 2009 til 2019 vektlegger stater og organisert kriminalitet som de fremste trusselaktørene. NSM nevner derimot også enkeltindivider (asosiale individer) som aktører som kan gjennomføre handlinger som gir betydelige konsekvenser, og for finanssektoren. En annen informant besvarte spørsmålet om hvem som er trusselaktørene med: «Nei, det er alt mulig. Det er jo flere typer kriminell digital aktivitet, det er egentlig alt fra gutteromsstreker til statlige aktører» (TM4). Selv om truslene kan være fra «gutteromsstreker» til statlige aktører, er det mye ressurser som blir brukt på å håndtere cybercrime rettet mot bank og finanssektoren. Lederen i en av virksomhetene som til daglig arbeider med håndtering sa «cybercrime er det vi bruker mest tid på». Videre fortalte han:

«(...) de har hatt et tiår hvor de har tjent mye penger og bygget mye ressurser, dette fungerer og de investerer. Dette er ikke pent». (NI2).

Finanstilsynet trekker frem APT som en alvorlig og økende trussel mot finanssektoren de siste årene (Finanstilsynet, 2018). NSM vektla også APT som en økende trend i 2015 (NSM, 2015). Aktørene som står bak denne trusselen kan være både fremmede stater og organiserte kriminelle. Det antas at det kan være et samarbeid mellom stater og kriminelle i å gjennomføre angrep. En av informantene forklarte:

> Det ble påstått at det ofte er et samrøre (samarbeid) mellom nasjonale sikkerhetsmyndigheter som gjør mye gale ting, som spionasje, og organiserte kriminelle. Det er liksom et samarbeid og kan avtale at nå gjør de det på oppdrag. De kompetansemiljøene man bygger for å angripe banker, nettbank, de miljøene blir også brukt av etterretning og de hjelper kanskje til og med på organisert kriminalitet. (TM2).

Det kan være et utydelig skille mellom statlige aktører og organiserte kriminelle, særlig relatert til trusselen APT gir. NSM kategoriserer APT som en del av etterretningstjeneste og informasjonssamlere, hvor «(...) det antas at betydelige mengder informasjon stjeles på denne måten» (NSM, 2015, s.29). Videre skrives det at APT ofte er rettet mot finansinstitusjoner, og at det har forekommet i Norge (NSM, 2015). Det trekkes også frem et skille mellom hvilke aktører som angriper ulike virksomheter. For kommersielle virksomheter, slik som banker, kan man forvente at organiserte kriminelle og cybercrime utgjør hovedvekten av trusselaktører, mens for offentlige virksomheter som for eksempel Norges Bank er trusselaktørene knyttet mot statlige trusselaktører. En informant sa: «det er helt avhengig av hvor man er (i finanssektoren)» (TM3).

Motivasjon

Motivasjonen til en potensiell trusselaktør kan være et skille når man kartlegger hvilke aktører som kan tenkes å angripe sektoren, da motivasjon gir ulike formål med aktiviteten og angrepene som gjennomføres. Finanssektoren sine verdier kan grovt deles i to og ble av en informant forklart slik: «vi har to store verdier – bortsett fra folk og fe og sånn, og det er penger (...) og den andre siden er jo informasjon (...) man sitter på ekstremt mye sensitiv

bedriftsinformasjon og konfidensiell informasjon som må beskyttes» (NI1). De to verdiene som sektoren besitter gjør den særlig attraktiv for uønsket aktivitet. Verdiene kan ikke bare være viktige for virksomhetene, men også for ulike individer, andre sektorer og nasjonen forøvrig. Når en av driftsleverandørene ble spurt om hva som er motivasjonen svarte han: «det er penger kan du si, det og å innhente informasjon, industrispionasje, alt det her. Hva tror du de kan ha hentet ut av Hydro? Det er jo et veldig interessant spørsmål» (DL1).

Ettersom de to største truslene mot finanssektoren er digital kriminalitet og statlig etterretning (NSM, 2018a, s.7), blir det mulig å skissere ulike aktørers motivasjon. Selv om denne skisseringen er tilsynelatende enkel, viser funn at motivasjonen og formålet til trusselaktørene stadig flyter mer over i hverandre. En av informantene fortalte at: «det er jo relativt greit for er det cybercrime så er det økonomisk motivert, men en del av disse andre truslene som nødvendigvis ikke er økonomisk motivert, de kan være mer utfordrende å forholde seg til» (NI2). Utfordringene som følge av ulike motivasjoner og formål, gjør det vanskeligere å ha kontroll på de ulike aktørene. En av systemeierne utdypet dette med: «men det vi kanskje frykter mest er organisert kriminalitet som kan komme inn å stjele hundrevis av millioner dollar, og det finnes dessverre noen eksempler på det og plutselig er det i Norge det skjer» (SE2).

De ulike grupperingene som typisk står bak APT-angrep viser noe av kompleksiteten i motivasjon. Frem til omlag 2011 demonstrerer funn at man har hatt en oppfatning av at kriminelle er økonomisk motiverte, mens etterretningstjenester er fremmede stater som er motivert av informasjonsuthenting. Nord-Korea, som en fremmed stat og etterretningstjeneste, antas å være motivert av både penger og informasjon. En av systemeierne forklarte nærmere: «man har jo for eksempel enkelte grupperinger som er veldig rettet mot bank/finanssektoren (...) som Cobalt gang, Lazarus, er man jo ganske trygg på er knyttet til Nord-Korea» (SE2).

Fremmede stater utgjør i dag en større del av trusselbildet. Som nevnt tidligere i kapittelet har denne aktiviteten økt nasjonalt og inn mot finanssektoren. Solberg-regjeringen trekker i den forbindelse frem et interessant aspekt, nemlig at grensen mellom krig og fred er mer flytende, særlig på det digitale domenet (Departementene, 2019). En av informantene trakk også inn denne problemstillingen: «så har vi den statlige tematikken, tror vi at noen statlige aktører ønsker å ødelegge så mye at det (*finanssystemet*) bryter sammen, eller er vi da i en

krigssituasjon?» (TM4). Dette spørsmålet bidrar til å belyse problematikken, og demonstrer alvorligheten et angrep på finanssektoren kan gi. Dersom motivasjonen til fremmede stater ikke er penger eller informasjon, men destruksjon, er det noe som i prinsippet kan gjøres gjennom et cyber-angrep. Cyber-trusselens karakter blir dramatisk endret dersom formålet går fra å angripe verdier til å angripe infrastruktur for å ramme nasjoner. NSM trekker frem at cyber-spionasje ofte er økonomisk motivert, men at «det må regnes med at en betydelig andel er sikkerhetspolitisk eller maktpolitisk motivert» (NSM, 2015, s.30) Dette kan bringes videre til trusselaktørenes kapabilitet og utvikling.

Kapabilitet og utvikling

De ulike trusselaktørene har ulike kapabiliteter, og utviklingen hos aktørene gjør at de representerer en betydelig trussel. Finanstilsynet belyste i ROS-analysen for 2016 at kompleksiteten i målrettede angrep var økende, og at foretak så på det som en økende trussel (Finanstilsynet, 2017). Den ene nøkkelinformanten redegjør for utviklingen på følgende måte:

> Norsk banksektor gjorde betydelig digitalisering på 70 og 80-tallet, men da var det i praksis ingen trusselaktører som hadde kapasitet til å angripe de digitale systemene, og i mange år levde man i trygghet (...) dette fortsatte frem til 2010-2011, det er ikke noe særlig trøkk på cybersikkerhetsrisikoer, hvert fall ikke på, altså på tilgjengelighet men ikke noe annet. Men så kommer de. (NI1).

Han viste til at oppblomstringen virkelig tok fart rundt 2011-2012, noe som også nevnes i finanstilsynets risikoanalyser (Finanstilsynet, 2012; Finanstilsynet, 2013). Videre sa nøkkelinformanten følgende: «du får noen eksempler på at hackere er ute etter banken» (NI1). Tryggheten man i mange år har hatt kan bidra til å vanskeliggjøre scenariotenkningen for hva som er mulig å gjennomføre og hva aktørene er ute etter. Ettersom verden utvikler seg og blir mer digitalisert, er det helt naturlig at også de kriminelle digitaliser sin aktivitet. Dette bidrar til å forklare hvorfor trusselaktørene har utviklet seg, og hvorfor særlig organisert kriminalitet utgjør en større trussel for hvert år som går. Deretter ble det forklart at: «de kriminelle som fortsatt drev med gammel kriminalitet i 2009 har blitt digital, verden har blitt mer global og alt har blitt digitalisert» (NI1).

Intervjuene og dokumentene som dette studiet tar utgangspunkt i, beskriver utviklingen til trusselaktørene gjennom fem felles utviklingstrekk. For det første har aktørene fra 2009 til 2019 blitt mer profesjonaliserte, og denne profesjonaliseringen øker fra år til år. En av informantene beskrev det som: «Så er det det her med profesjonaliteten hos cyberkriminelle. Det er jo skikkelig proft» (SE2). Profesjonaliseringen og «yrket» som cybercrime har blitt, skaper et mer komplekst trusselbilde, som bringer meg til det andre utviklingstrekket.

Det andre utviklingstrekket er at aktørene blir stadig mer avanserte, sofistikerte og benytter kompliserte metoder for å gjennomføre uønsket aktivitet. Utviklingen av APT for etterretningsvirksomhet demonstrerer nettopp dette. Ondsinnet programvarer og spyware kan ligge i systemer i årevis uten at de blir detektert, som gjør at trusselaktørene kan hente ut den informasjonen de ønsker. Angrepene er mer komplekst sammensatt og langt mer teknologisk avanserte enn tidligere. Et tredje utviklingstrekk er det informantene omtaler som *uoversiktlighet*. Det finnes flere ulike grupperinger og aktører som kan forsøke å gjennomføre uønskede handlinger mot finanssektoren. Det gjør det nesten umulig å holde oversikten. Denne uoversiktligheten kan knyttes tilbake til profesjonaliseringen av aktørene, og det faktum som en informant nevnte: «så har man jo også cybercrime ″as a service″ – de hjelper hverandre i et globalt nettverk av kriminelle, kjøper malware og hjelper hverandre å sette opp servere som ikke er sporbare» (SE2). Uoversiktligheten blir forsterket som følge av stater som samarbeider med organiserte kriminelle nettverk, dette nevnes av flere informanter.

For det fjerde har trusselaktørene blitt ekstremt tilpasningsdyktige og utvikler seg hurtig. Dette fører til at et allerede uoversiktlig trusselaktørbilde blir enda mer utfordrende. Aktørene har motivasjon og kapabilitet til å tilpasse seg og finne nye måter å gjennomføre angrep på. Det blir et «våpenkappløp» (TM4) mellom å bygge opp gode nok forsvarsverk og å finne metoder for å rive dem ned. En trusselaktør kan bestemme seg for én metode, én virksomhet eller én sektor den ønsker å angripe, mens finanssektoren må beskytte seg mot alt. Det siste utviklingstrekket, som i seg selv bidrar til de andre utviklingstrekkene er at trusselaktørene har voksende ressurser som følge av økende profitt. Kapabilitetene til trussselaktørene kan med andre ord sies å ha økt med årene. Flere informanter beskriver cyber-truslene og cybercrime som «en kjempebusiness» (DL2).

Utviklingstrekkene er overførbare til de fleste trusselaktører, selv om trusselaktørene representerer ulike risikoer mot sektoren. Kapabilitetene og utviklingen skaper trusler og

angrepsformer man ikke trodde var realiserbare. En informant fortalte «de blir flinkere og flinkere til å kamuflere, de gjør ting på nye måter og skifter moduser» videre utdypet han «det vil hele tiden være en evig kamp i forhold til at aktører der ute har det som sin profesjon å finne opp noe, mens bankene og foretakene sin profesjon er å avdekke.» (TM4). NSM støtter opp om denne observasjonen, og skriver at «det er sannsynlig at norske banker utsettes for omfattende hackerforsøk, der profesjonelle aktører står bak» (NSM, 2015, s.29).

Metodene som brukes for å gjennomføre cyber-angrep er flere, og de endres stadig i sin utforming (se vedlegg 8 for beskrivelse av metoder). Intervjuer og dokumenter har gjort det mulig å identifisere ulike angrepsmetoder, de er oppgitt i tabellen under:

Metode:
DDoS-angrep (tjenestenektangrep)
Trojansk hest
Orm
Malware
Spyware
Kryptoware
Ransomware
Phishing
Spear-phishing
Zero days
Vannhullsangrep
Tredjeapartsangrep
Påvirkningsoperasjoner
Informasjonslekkasje
RAT (remote access trojans)
Fysiske implanter (Fysisk/cyber)

Tabell 2: Metoder for intenderte cyber-hendelser

De ulike metodene vil følge utviklingen, for eksempel ved at de har blitt bedre på å gjennomføre et ransomware-angrep ettersom de er mer sofistikerte, avanserte og kompliserte. Økende antall angrep mot nettbankene demonstrer også at trusselaktørene representerer enn større trussel mot foretakene sine systemer, og ikke primært mot kunder (Finanstilsynet, 2018). Trusselaktørene drar fordel av den teknologiske utviklingen det siste tåret. NSM belyser dette i sin rapport om IKT-trusselbildet i 2015 og skriver «mens det tidligere ble utført

enkle angrep som forårsaket begrenset skade, gjennomføres det nå sofistikerte angrep som kan forårsake betydelig skade for virksomheten som blir angrepet» (NSM, 2015, s.30).

5.1.4 Økende trussel

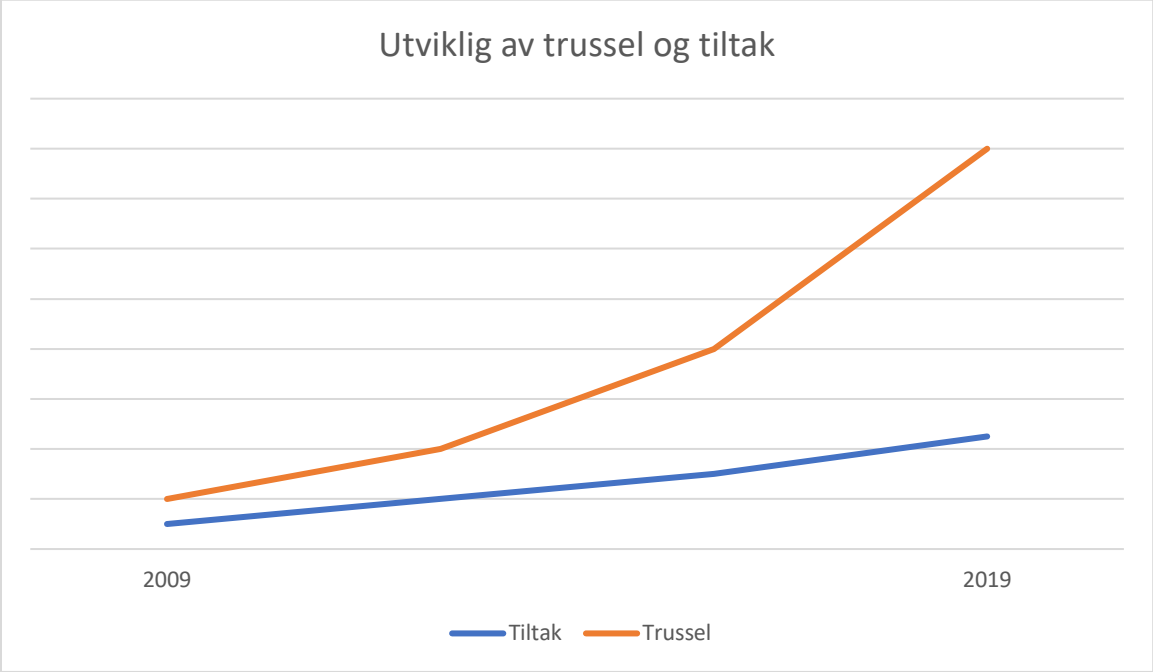
Cyber-trusselen mot finanssektoren forstås som økende på tvers av dokumenter og intervjuer. «I praksis har man laget en svær arena hvor kriminaliteten øker. Og den organiserte kriminaliteten, den er kjempediger» (TM2). Informantene belyste at cyber-trusler og de tilsiktede angrepene er det man har muligheten til å forsvare seg mot, og derfor legges mye av fokuset her. En annen forståelse for hvorfor trusselen øker er: «det at hele dette økosystemet øker og blir større, mer komplisert og mer sofistikert» (TM4).

Den totale økningen av cyber-truslene har flere årsaker. Først kan det knyttes opp mot trusselaktørenes utvikling. De fem utviklingstrekkene, henholdsvis profesjonalisering, mer avansert-, komplisert- og sofistikert, uoversiktlighet, tilpasningsdyktighet, og økte ressurser hos trusselaktørene er blant årsakene til at trusselen oppleves som økende. «Men på en måte kunnskapen, hva er mulig å gjennomføre av angrep og hvor lett er det å forsvare seg og hvilke aktører har sett og er villige til å bruke det – det har forandret seg.» (NI2). En annen forandring som har bidratt til å øke trusselen knyttes til interne misligheter. Innsider-trusselen er økende, og utro tjenere kan selv være utsatt for press utenfra. Dette ble belyst av en informant:

> Det er selvfølgelig en trussel at noen kan komme inn i en virksomhet og gjøre ett eller annet (...) så er det trusler som utro tjenere, folk som blir utsatt for trusler. Du har hele spekteret på hva som kan være trusselområder som foretaket må jobbe med og ha fokus på. (TM4).

Finanstilsynet trekker frem at risikoen for at ansatte kan tvinges til å gjennomføre uautoriserte handlinger øker, noe som harmonerer med foretakenes bekymring om interne misligheter (Finanstilsynet, 2017). Dernest hevdes trusselen å øke ettersom man ikke lenger trenger «teknologisk know-how for å utgjøre en trussel» (SE1). Som nevnt tidligere i kapittelet tilbys nå «cybercrime ″as a service″», og dette bidrar til å øke omfanget av uønsket aktivitet mot sektoren. Dette vil i sin tur bidra til å øke den totale trusselen.

Finanstilsynet skriver at «etterretningstrusselen fra statlig aktivitet har vært økende fra 2007, men de siste to årene har det vært en akselerasjon» (Finanstilsynet, 2018, s.53). Det kan kobles mot at det har vært en lang tidsperiode hvor trusselaktører har utviklet kapasiteter. Samtidig utgjør APT en betydelig trussel mot finanssektoren, og det er forventet at denne vil øke de kommende årene (NSM 2018a, Finanstilsynet 2018). Det kan stilles spørsmål ved hvorfor trusselen har økt når det har blitt dedikert stadig mer oppmerksomhet til cybersikkerhet det siste tiåret. Oppmerksomheten kan eksemplifiseres med antall ord som har blitt brukt i ROS-analysene til finanstilsynet fra 2009-2019, som har økt for hvert år (vedlegg 7). Økt risiko har vært fulgt av utvikling og investering i cybersikkerhet. Selv om det har blitt bygget opp store sikkerhetsorganisasjoner og cybersikkerhetsavdelingene har vokst, ser det ut til at trusselaktørene har utviklet seg hurtigere enn tiltakene. En av informantene illustrerte denne utviklingen (se figur 6) og sa: «trusselbildet øker bratt, mens tiltakene ikke klarer å henge etter. Man får da et økt gap» (NI1).



Figur 6: Utvikling av trussel og tiltak

Selv om man opplever en økt trussel og nye former for farer, er det ikke nødvendigvis en økning i cyber-risikoen for finanssektoren. Det ble forklart med følgende «trusselen har økt, og økt antall hendelser har vært viktig for å skape økt bevissthet og ført til tiltak». (NI1). Det har vært en dokumentert økning i tiltakningen av trusler (Finanstilsynet, 2017), men det er mindre sannsynlighet for nedetid i forhold til de effektive barrierene og robustheten i infrastrukturen som finanssektoren består av.

En faktor som endrer trusselbildet og bidrar til økt risiko i lys av angrep er bruken av kunstig intelligens (KI). KI forventes å bli misbrukt av fremmede stater og organiserte kriminelle for å gjennomføre mer avanserte angrep (NSM, 2018a; Finanstilsynet, 2018). Denne utviklingen krever en løpende oppdatering i forsvarsverk, og krever at også finanssektoren tar i bruk KI for å være i stand til å lage scenarioer og identifisere sårbarheter som KI-enheter vil kunne avdekke (Finanstilsynet, 2018). Trusselen mot finanssektoren har vært økende for hvert år det siste tiåret, og som en informant forklarte: «forventer at det vil komme flere målrettede hendelser mot finanssektoren, slik som Cobalt Gang, bare at de er enda vanskeligere å detektere» (SE1). Det er bred enighet om en økende trussel, men hvorvidt det gir en økt risiko finnes det uenigheter om.

Videre er sårbarhetene på det digitale domenet dynamiske – når en lukkes åpnes en annen. Det kan knyttes mot trusselbildet «sårbarheten vil også avhenge av hvordan trusselbildet utvikler seg» (TM1). Ved endringer i trusselbildet vil det dermed være endring i sårbarhetsnivået som påvirker robustheten i finanssystemet. En av informantene hevdet at «det går på samfunnets robusthet også, for vi er jo ikke så robuste som for 30 år siden, med våre leiligheter uten vedovn, og elbil som eneste transportmiddel.» (NI1). Sårbarhetene representerer dermed også en trussel for sektoren, selv om de ikke er tilsiktet. Hvordan sårbarhetene har utviklet seg, forstås forskjellig i sektoren. En informant oppfattet sårbarhetene som stabile og sa: «trusselen har økt, kanskje, det objektive eller tekniske trusselbildet. Sårbarhetsbildet er ganske likt tenker jeg» (NI2). I flere dokumenter refereres det til to kategorier for sårbarhet (Departementene, 2019; NOU 2015:13; E-tjenesten ,2011). Den første handler om de sårbarhetene som er kjente og aksepterte, mens den andre handler om sårbarhet som enten er ukjente, feilvurdert, ikke forstått eller mangelfullt kommunisert (NOU 2015:13). Sårbarheter kan derimot også utnyttes av trusselaktører. De ukjente sårbarheter representerer en økt trussel, da trusselaktører aktivt kan forsøke å utnytte dem. Videre kan en sårbarhet påvirke cyber-farene tilknyttet cyber-domenet, noe som kan øke cyber-risiko.

5.1.5 Oppsummering

Empirien som har blitt presentert i denne seksjonen demonstrerer at utviklingen av cyber-risiko har vært gradvis, og at trusselen knyttet til cyber har økt betydelig. Fra det nasjonale risikobildet er det lagt særlig vekt på etterretning og statlig spionasje som fremtredende

trusler. Videre trekkes det på det nasjonale plan frem at det er endringer i risiko- og trusselbildet, og at denne trusselen synes å være økende årlig. Flere av truslene mot nasjonal sikkerhet gjenspeiles i sektoren, men det er rettet stor oppmerksomhet mot trusselen cyberkriminalitet. For finanssektoren har det vært store utfordringer knyttet til beskyttelse av verdier, som penger og informasjon. Som belyst i kapittelet er trusselaktørene i stadig utvikling, noe som utgjør en stor utfordring for finanssektoren. Særlig knyttet til de ulike metodene som tas i bruk for å gjennomføre vellykkede cyberangrep. Det forventes at trusselaktører, særlig organiserte kriminelle og fremmede stater, vil øke sine kapabiliteter til å gjennomføre cyber-operasjoner som kompromitterer tilgjengeligheten, konfidensialiteten og integriteten til finanssektorens verdier. Det er en utbredt forståelse at cyber-trusselen er økende, og at det kreves enorm innsats for å få bukt med denne trusselen. Det er lite som tilsier at denne trusselen vil avta i nær fremtid, særlig ettersom hele samfunnet digitaliseres og kritisk informasjon, infrastruktur og verdier flyttes over i cyber-domenet.

5.2 På hvilken måte påvirker cyber-farer finanssektorens cyber-risiko?

I cyber-risikolandskapet er det flere faktorer som bidrar til å skape risiko. Trusler kan føre til risiko, men det er også farer tilknyttet digitalisering og teknologi. Cyber-risiko kan i like stor grad påvirkes av uintenderte hendelser som menneskelige feil eller driftshendelser. Det betyr at både cyber-trusler og cyber-farer er faktorer som kan påvirke den totale cyber-risikoen i finanssektoren. Forståelsen for hvilke farer som representerer og kategoriseres som risiko er sprikende i dette studiet. I denne seksjonen presenteres ulike forståelser for begreper knyttet cybersikkerhet, IKT-sikkerhet og informasjonssikkerhet og funn knyttet til cyber-farer.

5.2.1 Ulike forståelser av terminologi og begreper

Forståelsen av cyber-trusler og cyber-risikoer er noe varierende mellom både informanter og dokumenter. Det kan forklares ved bruken av ulike begreper, og hvilken effekt begrepene har på hva som kategoriseres som cyber-, IKT-, IT- og informasjonssikkerhet. I dokumentstudiet ble det avdekket flere uregelmessigheter i bruken av begrepene. I noen tilfeller ble det referert til IKT-trussel og IKT-risiko, mens i andre ble det referert til cyber-trusler og cyber-risiko. Forståelsen og begrepsfestelsen for «fenomenet» knyttet til cyber kan gjøre at det skapes ulike forståelser for hvilken risiko og trussel digitaliseringen kan medføre. Det betyr at både risiko og trusselbildet knyttet til cyber kan påvirkes av hva som kategoriseres som cyber-, IKT-, IT- og informasjonssikkerhet.

I offentlige dokumenter og litteratur brukes IKT og cyber i enkelte tilfeller om hverandre, mens i andre tilfeller sammenfaller IKT med informasjonssikkerhet og overholdelse av integritet, konfidensialitet og tilgjengelighet av informasjons og kommunikasjonsteknologi (NOU 2015:13; NOU 2018:14; NSM 2015-2018; Finanstilsynet, 2009-2019). IKT utgjør dermed det «store bildet» hvor cyber blir en mindre del av helheten. Når det henvises til cyber-hendelser, blir det ofte brukt synonymt med angrep, som en tilsiktet hendelse med formål å ramme eller ødelegge et systems funksjonalitet.

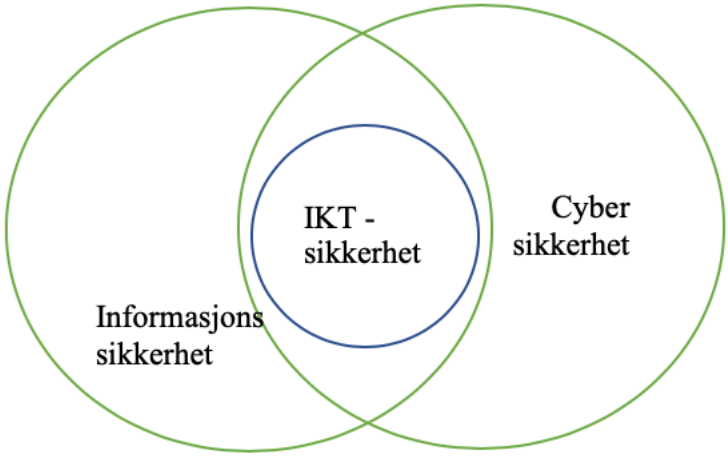
I andre dokumenter forstås cyber som «helheten», hvor cybersikkerhet handler om alle de prosesser, tiltak og virkemidler som tas i bruk for å sikre hele det digitale systemet. Det kan for eksempel være alt fra systemer som brukes på datamaskinene i en virksomhet til den digitale infrastrukturen i samfunnet. Da regjeringen kom med den første nasjonale strategien som handlet om digitalisering, var det en strategi for *informasjonssikkerhet*, mens den siste strategien som ble utgitt i 2019 fikk navnet nasjonal strategi for *digital sikkerhet* (Departementene, 2012; Departementene, 2019).

Selv om IKT-sikkerhet og cybersikkerhet brukes om hverandre som synonymer, har begrepet «cyber» mottatt økt oppmerksomhet de seneste årene. En av forklaringene ligger i at angrepsflaten på det digitale domenet har blitt større, og i det internasjonale miljøet refereres det til cyber-angrep heller enn IKT-angrep. Samtidig har cybersikkerhet også fått økt betydning ettersom samfunnet har blitt enda mer digitalisert og det har vært en eksponentiell vekst i teknologien. Norge er et av de fremste landene når det kommer til å anvende ny teknologi – som også betyr et økt fokus på og behov for cybersikkerhet (PWC, 2018a). Det som virker særlig interessant, er at cyber-hendelser ifølge funn referer til noe tilsiktet, mens IKT-hendelser refererer til både tilsiktede og utilsiktede hendelser. Informantene i dette studiet hadde varierende oppfatninger av begrepsbruken.

Alle informantene ble spurt om forskjellen mellom IKT-sikkerhet og cybersikkerhet, og bekreftet at det finnes ulike forståelser for begrepene. Fem av informantene mente at IKT-sikkerhet og cybersikkerhet var det samme og gjorde ingen skiller mellom dem, mens fem av informantene mente at begrepene refererte til to ulike konsepter. Den ene informanten forklarte sin differensiering slik:

> Nei, jeg tenker forskjellig. Jeg liker CCIS på Gjøvik som tegnet et sånn venn-diagram på informasjonssikkerhet, cybersikkerhet og IKT-sikkerhet (informant tegner venn-diagramet på en whiteboard). Cyber er alt som er sårbart (...), det kan jo også være om toget går i rute, men jeg tenker at for en bank så er jo ikke det IKT eller informasjonssikkerhet, informasjonssikkerhet handler om det at vi snakker sammen her eller på toget og noen lytter, det er bredere enn IKT-sikkerhet. Jeg tenker på IKT-sikkerhet som mye smalere og systemavhengig. Jeg er enig i at de brukes upresist og veldig mye omtales som IKT-sikkerhet. (NI2).

Informantens illustrasjon er gjengitt under:



Figur 7: Venn-diagram for digital sikkerhet

En annen informant hadde en helt motstridende oppfatning:

> Det er risiko knyttet til all bruk av IKT. Vi snakker mye om IKT-risiko og cyber-risiko, men cyber-risiko er en del av IKT-risikoen, det er ikke noe som eksisterer ved siden av. Det er en del av IKT-risiko er mer enn bare cyber-risikoen. Det går på risiko for deg og meg som brukere, og operatørene i virksomhetens bruk av systemer, ikke bare den trusselen man blir utsatt for utenifra. (TM4).

Da NSM for første gang ga ut sin rapport om IKT-risikobildet i 2015, ble det fremmet et sikkerhetsfaglig råd der man brukte begrepet cybersikkerhet om IKT-sikkerhet (NSM, 2015, s.13). I deres rapportering skilles det ikke mellom IKT-sikkerhet og cybersikkerhet, men cybersikkerhet er det som refereres til i internasjonal litteratur, rapportering og forskning. Det

digitale sårbarhetsutvalget, Lysne-utvalget (NOU 2015:13), trakk frem at i likhet med NSM, ville begrepene IKT-sikkerhet og cybersikkerhet bli brukt som synonymer. En av driftsleverandørene sa: «jeg føler det flyter ganske over på hverandre» (DL1), mens en av systemeierne forklarte cyber som: «det er bare et trendord tenker jeg, jeg har ikke noe skille på det egentlig» (SE2). Cybersikkerhet «handler om å beskytte IKT og informasjonssystemer mot uønskede hendelser» (NOU 2015:13, s.34). En av informantene behandlet IKT-sikkerhet og cybersikkerhet «som det samme» (NI1). Videre forklarte han:

> Jeg behandler det også sånn, altså hvorfor bruker jeg cyber, jo fordi at det er alt. Alt er i ferd med å få prosessorkraft og kobling mot internett (...) Det handler om å beskytte informasjon som er der og der, men det er litt pretensiøst å si at det gjelder alt, men for meg så gjør det det i det moderne samfunn. (NI1).

Hele det moderne samfunn digitaliseres, noe også finanstilsynet peker på i sin ROS-analyse (Finanstilsynet, 2018). Lysne-utvalget beskriver cybersikkerhet som «alt som er sårbart fordi det er koblet til, eller på en annen måte er avhengig av, informasjons- og kommunikasjonsteknologi» (NOU 2015:13, s.34).

5.2.2 Cyber-farer som påvirker cyber-risiko

Finanstilsynet gjør et skille mellom operasjonelle hendelser og sikkerhetshendelser, som kan knyttes mot cyber-trusler og cyber-farer. En cyber-fare kan forstås som en operasjonell hendelse, altså en utilsiktet hendelse, mens sikkerhetshendelser refererer til tilsiktede, ondsinnede hendelser (Finanstilsynet, 2018).

Finanstilsynet refererer i 2009 til noen spesifikke utviklingstrekk når de redegjør for faktorer som kan påvirke den operasjonelle risikoen i finanssektoren (Finanstilsynet, 2009). Disse utviklingstrekkene representerer i all hovedsak farer, med unntak av internettkriminalitet som kan betegnes som en trussel. Hovedvekten av antall hendelser de siste 10 årene er forårsaket av cyber-farer som fører til operasjonelle eller driftsrelaterte hendelser (Finanstilsynet, 2009-2019). Gjennom intervjuene og dokumentstudiet har det vært et gjennomgående fokus på følgende seks farer, nemlig kompleksitet, utkontraktering, konsentrasjonsrisiko, avhengighet, nedetid og menneskelige feil.

Kompleksitet

En fare som representerer en betydelig risiko er kompleksiteten i infrastruktur og systemer (Norsk senter for informasjonssikkerhet, 2017; Departementene, 2019). En av informantene beskrev denne kompleksiteten på følgende måte: «hvis du begynner å dukke ned i det (systemet) så er det helt uhyre komplekst, men jeg tenker at det er sånn nøkkelpunkt at det er mye gammel teknologi man ikke får gjort så mye med» (SE2). Selv om systemet er komplekst skapes også kompleksitet når nye og gamle system er i interaksjon med hverandre. Interaksjonen mellom ny og gammel teknologi kan være svært utfordrende og det ble trukket frem av en annen informant: «kompleksitet går mest på legacy, gamle ting (...) mye arv og det genererer mye kompleksitet i de fleste finansinstitusjoner» (TM3). Selv om kompleksitet kan genereres i grensesnittet mellom ny og gammel teknologi og systemer, fører dette til en infrastruktur som er tett sammenkoblet og kompleks. En «spagetti-infrastruktur, ved at norske banker har fusjonert og bygget sin IT over mange år(...)» (NI1) kan føre til at nye sikkerhetsmekanismer og ny teknologi blir vanskeligere å implementere.

Dersom man konstruerer systemer med for mange barrierer og sikkerhetsmekanismer for å skape redundans, kan det være en utfordring i seg selv. Det ble utdypet av en systemeier: «altså du kan jo for eksempel bygge, sånn typisk ingeniører, så fantastisk og superredundante systemer som gjør at når det først feiler så er det ingen som skjønner en dritt av hvordan dette henger sammen» (SE2). Å lage sikre systemer som er mer robuste er en faktor for kompleksitet, det ble også trukket frem av en tilsynsmyndighet: «det er klart at bedre stabilitet og jo mer sikkerhet du bygger inn i forhold til operasjonell drift – jo mer kompleksitet blir det. Og ved feil i denne kompleksiteten blir konsekvensen litt større og mer komplekse hendelser» (TM4).

Kompleksitet er dermed en faktor som ikke bare øker risiko, men kan føre til større konsekvenser. Kompleksitet knyttes sammen med lengre verdikjeder. Det trekkes frem at lengre verdikjeder øker kompleksiteten i finanssektoren, noe som øker den totale cyber-risikoen (NOU 2015:13; DSB, 2019). Årsaken til at verdikjedene har blitt lengere er flere. En av årsakene er samhandling mellom ny teknologi og flere aktører. En informant forklarte dette med følgende:

> Noe jeg har sagt flere ganger, er at det er ikke sikkert at nye aktør gir en større risiko i seg selv enn den risikoen eksisterende aktører utgjør ut over at aktøren er ny. Det at det blir flere aktører gjør at det samlet sett blir økt risiko i hele systemet, og at verdikjedene blir lenger, gir i seg selv også en økt risiko. (TM4).

Flere aktører involveres i betalingssystemet både i form av systemeiere og som tjenesteleverandører. Det fører til en ny fare, nemlig faren forårsaket av utkontraktering.

Utkontraktering

Finanstilsynet belyser allerede fra 2009 at utkontraktering av finanssektorens IKT-systemer representerer en fare. Norges Banks årlige rapporter «Finansiell Stabilitet» og «Finansiell Infrastruktur» nevner også utkontraktering som en fare, dersom det ikke blir gjort på en tilfredsstillende måte (Norges Bank, 2009a-2018a, Norges Bank, 2009b-2018b). DSB trekker også frem tjenesteutsetting (utkontraktering) som en fare for finanssektoren (DBS, 2019). Under intervju ble alle informantene spurt om risiko knyttet til utkontraktering og en av dem svarte følgende: «utkontraktering er en veldig stor risiko, for du er ikke sikrere enn det svakeste leddet. (...) det er utrolig viktig å ha godt fokus på leverandør og sikkerhet hos dem» (TM3). En annen informant trakk frem at man må sørge for at: «den du outsourcer til har samme sikkerhetsstandard som den i din egen organisasjon, hvis ikke har du en risiko der» (SE1). Videre kom det frem at:

> Hvis du outsourcer til noen som har den samme forståelsen for cybersikkerhet som deg så vil det være en fordel på det teoretiske nivået, og store institusjoner vil vanligvis outsource på grunn av spesialisering. Det vil også avhenge av hva du outsourcer, hvis du outsourcer markedsføringsdetaljer, så trenger man gjerne ikke høy sikkerhetsklarering for du deler ingenting konfidensielt, men hvis det er noe kritisk som kan være en risiko, så må man forsikre seg om at sikkerheten er på plass. (SE1).

Farene knyttet til utkontraktering har vært i finanstilsynets søkelys i en årrekke, noe som også demonstreres gjennom rundskrivet de ga ut i 2010 'Utflytting av bankenes IKT-oppgaver'. Finanstilsynet skriver i sin risikoanalyse fra 2011 at «det er viktig å sikre nødvendig kompetanse og tid til fullt ut å kunne styre og kontrollere det driftsmessige forholdet både til egne operasjonelle ressurser og til IT-leverandører med eventuelle underleverandører.

Finanstilsynet tok denne problemstillingen opp i rundskriv 2010/2011» (Finanstilsynet, 2012, s.20). Rundskrivet har bidratt til å kontrollere farer ved å å minske risiko, og en av informantene nevnte at det krever at virksomheter må gjøre «risikoanalyser knyttet til aktiviteten som utkontrakteres» (TM2).

Konsentrasjonsrisiko

Utkontraktering kan også føre til konsentrasjonsrisiko. Konsentrasjonsrisiko refererer til den risikoen som oppstår når man samler tjenester, systemer og infrastruktur på en geografisk lokasjon eller hos en leverandør. Det er få driftsleverandører som tilbyr de tjenestene som utkontrakteres. Norges Bank vektlegger særlig denne risikoen i 2018-rapporten om finansiell stabilitet. «Et stort antall aktører i bank- og betalingssystemet er avhengige av noen få sentrale IKT-leverandører som leverer og vedlikeholder kritiske systemer og maskinvare. Dette utgjør en konsentrasjonsrisiko for det norske finansielle systemet.» (Norges Bank, 2018a, s.26). Konseptualiseringen av konsentrasjonsrisiko blir utfordret av informantene. To av informantene var ikke kjente med begrepet, men særlig en av de 15 informantene mente at konsentrasjonsrisiko var en «filosofisk diskusjon». Han forklarte dette på følgende måte:

> Jeg tenker at det er en filosofisk diskusjon, og jeg er ikke sikker om jeg kjøper argumentet om at det er konsentrasjonsrisiko. Hvis du tar eksempel som bankID-infrastrukturen, hvis du tenker på det som en sånn, det er jo et system og det er klart at hvis noen gjør noe med det vil vi slite litt, for vi har ikke et alternativ. Fordelen med det er at da vet vi det, og vi vet hva som må til for å fikse det og holde det under kontroll. (...) jeg tror kanskje man må tenke litt på måten man tenker på det på. (NI2).

Styrkene som utfordrer konseptet konsentrasjonsrisiko trekkes frem ved at det er mer oversiktlig å være kjent med systemene og aktørene som leverer enkelte tjenester. Det trekkes frem i et annet intervju også ved at de få leverandørene som brukes for å levere disse tjenestene gir fordeler: «fellesløsninger er mye av effektiviteten» (TM1). Videre stilte en informant spørsmålet: «var det noe bedre å ha 4-5 som var mer utsatt for feil fordi man ikke kunne legge like mye arbeid i kvalitet og sikkerhet?» (TM2). Konsentrasjonsrisiko kan trekkes tilbake til kompleksitet, slik som en informant gjorde i redegjørelsen for tankegangen knyttet til konseptualiseringen av konsentrasjonsrisiko:

> Tankegodset er jo at diversitet er bedre og at istedenfor å ha et sentralt punkt så tar du det punktet og desentraliserer det til flere punkter og systemer. Det er tankegodset, og hvis du skal løse det så vil du jo på en eller annen måte lage mer diversitet, det du også får er mer kompleksitet og det trekker i feil retning. Så det å løse opp i konsentrasjonsrisiko uten å øke kompleksitet vil være kunsten. (NI2).

Avhengighet

En annen fare som trekkes frem blant annet av Lysne-utvalget (NOU 2015:13) er avhengighet mellom finansielle system og tjenester (finanssektoren) og annen kritisk infrastruktur. Her trekkes særlig avhengigheten til elektronisk kommunikasjon (EKOM) og kraftforsyning frem. Denne avhengigheten belyses også av NSM hvor det i 2018 nevnes at samfunnet er avhengige av IKT, mens det i 2015 trekkes frem at IKT-systemene er avhengige av annen kritisk infrastruktur. I 2014 var det mye nedetid og forsinkelser i bankenes betalingssystem, som synliggjorde at finansiell stabilitet til del er avhengig av støttefunksjonene fra IKT-systemene (Norges Bank, 2015a; NSM, 2015). Denne avhengigheten representerer en fare for banker hevder direktoratet for samfunnssikkerhet og beredskap (DSB, 2019, s.201). Det samme nevner Norges Bank i sin rapport om Finansiell Stabilitet (2018a), hvor avhengighet ikke bare er en fare, men en sårbarhet. En informant trakk også frem denne avhengigheten:

> Det er jo slik at finansnæringen er heldigital, er du Norges Bank på finansiell stabilitet, så er man på en måte, man er jo avhengige av det det fungerer og det å faktisk garanterer at hele finansnæringen er oppe og fungerer, og at penger flyter som de skal. (NI2).

Denne avhengigheten kan både være et operasjonelt problem, men den kan også bli utnyttet for eksempel av cyberkriminelle. Norges Bank skriver «finansiell sammenkobling og operasjonell avhengighet kan fungere som spredningskanaler ved alvorlige hendelser» (Norges bank, 2018a, s.25). Avhengigheten til og imellom teknologi og systemer er svært omfattende i finanssystemet. En av nøkkelinformantene sa: «så avhengigheten til digitale tjenester har jo blitt større, selv om den var stor også for 15 år siden» (NI2).

Nedetid

I dokumentene og intervjuene nevnes det flere farer som påvirker cyber-risiko. En av de største farene som ikke har blitt nevnt enda, er nedetid. «For meg er nedetid en betydelig cyber-risiko, det er en topprisiko» (NI1) sa en av informantene. Nedetid kan forårsakes av alle de farene som nevnt over, og representerer alene en stor risiko for det finansielle systemet. Konsekvensene knyttet til nedetid er enorme, og dersom det strekker seg over lengre tid kan det gi store økonomiske følger. Påskehendelsen i 2011(se vedlegg 8), forekom som følge av at telenettet var nede førte til nedetid i det finansielle systemet ved at betalingsterminaler og minibanker fikk problemer, og transaksjoner ble forsinket. Finanstilsynet skrev følgende «flere operatører hadde ikke tilgang til alternative rutingsveier og ble derfor hardt rammet» (Finanstilsynet, 2013, s.7). Risikoen knyttet til nedetid kan dermed gi mer alvorlige konsekvenser etterhvert som alt digitaliseres og flyttes over på cyberdomenet. Påskehendelsen demonstrerer ikke bare hvilke konsekvenser nedetid kan ha, men også hvilken fare avhengighet utgjør.

5.2.3 Menneskers handling kan bidra til økt cyber-risiko

Videre kommer det frem at mennesket spiller en stor rolle på cyber-domenet da flere av prosessene og handlingene i de teknologiske systemene er knyttet til menneskelig aktivitet. Funnene fra dette studiet belyser hvordan mennesker kan bidra til økt cyber-risiko i finanssektoren henholdsvis gjennom utilsiktede handlinger ved å gjøre feil og ved å bli lurt.

Menneskelige feil

Menneskelige feil kan være vanskelige å kategorisere – er det en fare eller en sårbarhet? Noen av informantene beskrev «menneske som det svakeste leddet i cyber-forsvaret» (TM1) og finanstilsynet skriver «til tross for stadig modnere driftsrutiner, er menneskelige faktorer fortsatt en avgjørende og medvirkende årsak til at en hendelse oppstår» (Finanstilsynet, 2018, s.30). En av informantene svarte på spørsmålet om mennesket som det svakeste ledd: «ja, de er det, definitivt» (TM4) og forklarte hvorfor på følgende måte:

> Nei, du får ikke bort mennesker og det er den menneskelige aktivitet som er trussel i forhold til sårbarhet, for det er ofte menneskelig handling som gjør at noe – som gjør at ting blir "iverksatt" inn i systemet. Typisk som jeg var inne på, at du får en epost og er ikke varsom nok, du åpner vedlegg og surfer på Internett på sider som ikke er sikre.

> Den type tema utgjør en operasjonell risiko. Mennesker er den største sårbarheten og den største sårbarhetsfaktoren. (TM4).

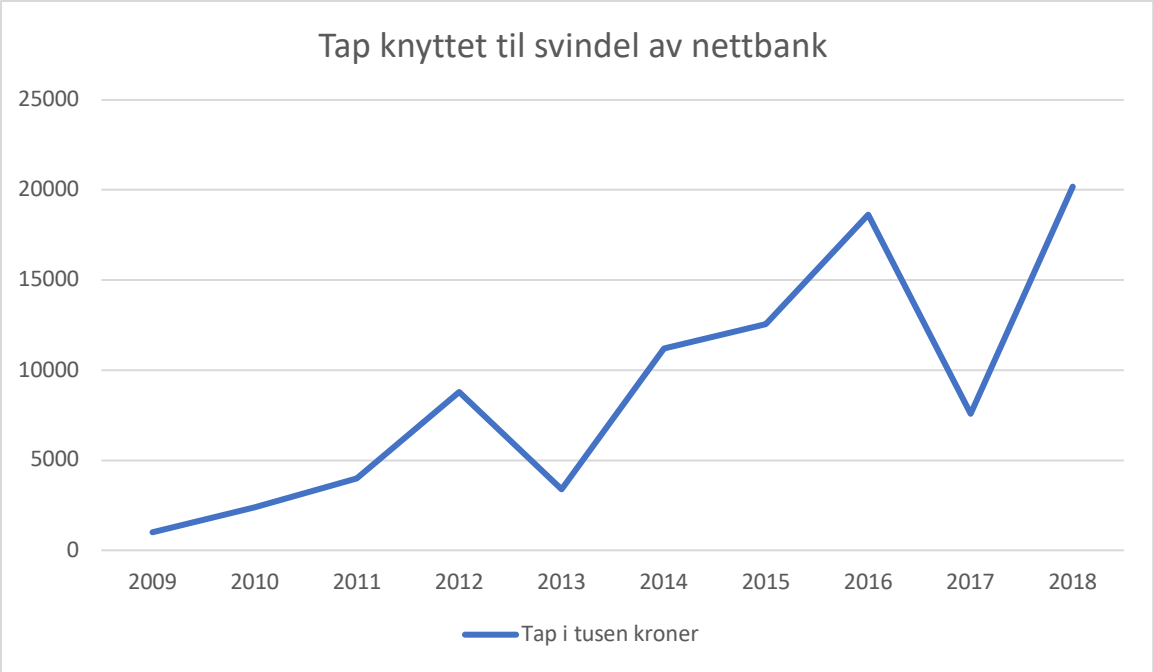
Selv om mennesker kan være både en sårbarhet og en fare, er det ofte uintenderte handlinger og aktivitet som fører til uønskede hendelser. Som informantene nevner er menneskelig aktivitet og feilhandling en sårbarhet som også er knyttet til det operasjonelle, eksempelvis ved uønskede driftshendelser. Disse feilene kan knyttes opp imot organisatoriske forhold. Dette vil bli belyst nærmere i kapittel 5.3. En informant sa: «det er to forskjellige kompetanse- og fokusdimensjoner, som gjør at det alltid er noen som får til noe (uønsket), og noen som er dumme, uforsiktige, eller i vanvare» (TM4). Dermed er det ikke kun det faktum at mennesket gjør feil som representerer en utfordring for cybersikkerhet, men også at mennesket utnyttes av aktører med ondsinnede intensjoner.

Når mennesket blir lurt – svindel og bedrageri

Underveis i dette studiet har det blitt avdekket ulike forståelser for hvilken fare og sårbarhet mennesket representerer. De ulike forståelsene kan knyttes opp imot svindel og lureri på cyber-domenet, og hvorvidt det er en cyber-risiko eller ei. «Det eksisterte før cyber og det eksisterte fortsatt, og det er ikke en cybertrussel. Det at mennesker blir lurt» (NI2), mente en av nøkkelinformantene. Mens en av tilsynsmyndigheten hevdet:

> Det er ikke så lett å oppdage, og det kan gjøres såpass avansert at selv ikke jeg hadde oppdaget det. Jeg kan få en mail fra sjefen, med et vedlegg som jeg åpner også infiserer det datamaskinen min (...) Det man ser er forsøk på å sende phishing mail med lenker og vedlegg som prøver å få folk til å åpne dem, så er det et spørsmål om man har gode forsvarsmekanismer som gjør at de ikke går gjennom. (TM3).

Selv om det er uenighet om hvorvidt svindel er en trussel eller et tradisjonelt samfunnsproblem i form av kriminalitet, gir dokumentstudiet godt grunnlag for å hevde at det er et økende problem på cyber-domenet og at antall svindelforsøk mot finanssektoren øker. Finanstilsynet demonstrerer disse tapene i form av økonomiske tap, som har vært stigende det siste tiåret.



Figur 8: Tap knyttet til svindel av nettbank (Finanstilsynet, 2009-2018)

Tapene som demonstreres i figur 8 viser at svindel gjennom cyber er en reell risiko for finanssektoren. Tapstallet bygger på fire ulike svindeltyper, det er gjennom angrep ved bruk av ondartet programkode, tap/stjålet sikkerhetsmekanisme, phishing og falske BankID-brukersteder og ukjente årsaker (Finanstilsynet, 2018). Derimot er informantene uenige i hvorvidt dette er en cyber-risiko. En informant hevdet at: «svindel er mer et samfunnsproblem, ikke en cyber-risiko» (TM4). En av driftsleverandørene svarte følgende når han ble spurt om svindel er en cyber-trussel:

> Ja, for det er jo det som er virkeligheten. Det er der de største tapene er, og den største banken i Norge ville jo hatt ganske formidable tap dersom den ikke hadde bygget opp denne anti-fraudavdelingen. Det her med bedrageri som vi har sett tidligere, det er jo småtteri i forhold til den elektroniske og det som skjer via nett. Cyber-angrep, det er jo der vi har, det er der det er mest fokus og der det er størst utfordring. (DL1).

Driftsleverandøren inkluderte dermed svindelmetodikken som en form for cyber-angrep, selv om det forekommer på mange forskjellige måter. Særlig for cybercrime er bruken av phishing, sosial manipulering, CEO-fraud og love-scam utbredt, og det brukes for flere formål. I finanstilsynet sin risikoanalyse for 2018 blir tapene knyttet til sosial manipulering presentert i følgende tabell:

Type svindel	Tap (i 1000kr)
Betaling for å leie et objekt mottager av pengene ikke eier	948
Innskudd etter løfter om store utbetalinger senere	99 091
Kjærlighet	88 191
Investering falske selskaper	92 073
Betaling for varer som ikke leveres	11 972
Endret mottakerkonto	8 606
Direktørsvindel (CEO-fraud)	33 913
Falsk faktura	32 982
Andre/ nye typer	19 593
Totalt	297 369

Tabell 3: Tap som følge av sosial manipulering

For finanssektoren kan dette ramme både kunder og ansatte – og det har potensiale til å gjøre store skader i form av økonomiske tap (som tabell 2 demonstrerer). En av informantene formulerte dette på følgende måte: «jeg tenker ikke på det som cybertrusler, svindel er noe annet. Det eksisterte før cyber og det eksisterer fortsatt, og det er ikke en cybertrussel – det at mennesket blir lurt» (NI2).

Mennesket er også en trusselaktør. Dette kan for eksempel manifesteres i form av utro tjenere, også referert til som innsidere og interne misligheter. Finanstilsynets risikoanalyser trekker frem at virksomhetene anser trusselen for innsidere som høy (Finanstilsynet, 2018). Informantene trekker også frem innsider-trusselen som en stor bekymring, og at det har vært et område man har dedikert mye ressurser til – som ved oppretting av personkontroll og personellsikkerhet. En av informantene forklarte:

> Så har den rare stemor 'personellsikkerhet' ansvar for interne misligheter og liknende, enten for folk som er dumme og ikke vet bedre, eller fordi de er ondsinnede og det er internt. Den biten har tradisjonelt vært en del av banken for det har vært folk som stjeler penger, det er et gammelt fagområde, men det har blitt digitalt. (NI1).

Selv om det er stor uenighet blant informantene om hvorvidt svindel er en cyber-trussel eller ei, er mennesket som en potensiell trusselaktør et kjent fenomen. Det kan være problematisk å hevde at svindel er en cyber-trussel, men det kan betegnes som cyber-fare som påvirker cyber-risiko i finanssektoren.

5.2.4 Oppsummering

Det er ulike forståelser knyttet til terminologi og forståelsen av cyber-farer i sektoren. I hvilken grad de ulike forståelsene av begrepene utgjør en sikkerhetsmessig utfordring er imidlertid usikker, men vil trolig være liten. Dette kan man anta basert på at dokumentene og informantene som har vært objekter i dette studiet nevner spesifikke tiltak og aksjoner for å detektere, forebygge og respondere på uønskede hendelser på det digitale domenet. Den ulike forståelsen knyttet til hva som er en cyber-trussel kan derimot prege sektoren. Empirien har belyst hvilken fare kompleksitet, utkontraktering, konsentrasjonsrisiko og avhengighet kan være, og at det er faktorer som må inkluderes i evaluering av cyber-risiko. Dernest trekker både dokumenter og informanter frem nedetid på systemer relatert til drift som en fare. Videre belyses det gjennomgående i dokumenter og intervjuer at mennesket i seg selv representerer en fare og sårbarhet som i sin tur kan påvirke cyber-risiko. Mennesker gjør feil i samhandling med teknologi, både intendert og uintendert. Samtidig ser man at trenden for å utnytte mennesker er økende, illustrert i økt tap knyttet til svindel gjennom cyber-domenet. I kapittel 5.1 ble det redegjort for utviklingen av trusler mot finanssektoren, mens dette kapittelet har undersøkt farene som kan gi risiko. Spørsmålet om hvorvidt utvikling av farer og trusler gir en økt risiko, må ses i sammenheng med hvilke tiltak som har blitt gjort for å kontrollere og styre risiko.

5.3 På hvilken måte har risikostyring for cyber endret seg?

Ettersom cyber-trusler-, -farer og -risiko har endret seg betydelig det siste tiåret, vil det være naturlig at måten risiko styres har endret seg. I 2010 etterlyses styring og kontroll av IKT-områder på tvers av virksomhetene (Finanstilsynet, 2011), og i ettertid har det skjedd omfattende endringer. Departementene (2019) legger tydelige føringer for digital sikkerhet i den nylig oppdaterte nasjonale strategien. Strategien fokuserer på nasjonalt, organisatorisk og individuelt nivå, for å tydeliggjøre at det må en helhetlig tilnærming til for å ha kontroll på risikoene. «Det er i samspillet mellom de forebyggende tiltakene, en robust digital infrastruktur, evnen til å håndtere digitale angrep, bekjempelsen av data- og IKT-relatert

kriminalitet og tilstrekkelig digital sikkerhetskompetanse at vi oppnår en helhetlig beskyttelse mot digitale hendelser» (Departementene, 2019, s.11). Risikostyring er et virkemiddel for å gjennomføre forebyggende tiltak og håndtering av angrep. Det skrives at virksomhetene selv er ansvarlige for å gjennomføre risikovurderinger og å gjennomføre tiltak (Departementet, 2019).

5.3.1 Tilnærming til styring av sikkerhet

En av endringene som kan knyttes opp mot risikostyring er hvilken tilnærming man har til styring av sikkerhet, eller nærmere bestemt cybersikkerhet. Denne endringen ble nevnt av en informant:

> Cybersecurity framework, der det er identify, protect, detect, respons og tilbakestill, for 15 år siden var sikkerhetsarbeidet identify, protect. Ha risiko, gjør tiltak – yes, da har du gjort jobben. I 2018/2019 holder ikke det, da er det også detect/respons, det at man må ha aktivt forsvar, det er viktig og nødvendig, men at man i det arbeidet jobber med å på en måte like mye 'hva er trussel, hvem er aktør', det har utviklet seg. (NI2).

Cybersikkerhet har utviklet seg til å bli en omfattende prosess som også forstås som et virksomhetsomgripende tema. Videre har det blitt en utbredt forståelse at man må forstå hvilken risiko som er knyttet til cyber, for slik å kunne håndtere den. Dette ble nevnt av flere informanter, og en av nøkkelinformantene hevdet: «det som kjennetegner en god cybersikkerhet i en virksomhet tenker jeg er noen som forstår sin egen verdi, systemer, avhengigheter til det og er i stand til å forsvare det. De må kjenne sin risiko» (NI2). Det ble også nevnt at tilnærmingen til sikkerhet må være risikobasert.

For å være risikobasert må man være kjent med både risiko og trusselbildet, og trusselbildet mot finanssektoren spesifikt beskrives som «kompetansekrevende å kjenne» NI2. I den nye digitale strategien fremmes det forslag om at virksomheter burde bruke anerkjente rammeverk, standarder og styringssystemer for å ha en «risikobasert tilnærming» til cybersikkerhet (Departementet, 2019). Det trekkes frem at det har skjedd endringer både i det proaktive og det reaktive sikkerhetsarbeidet – en informant sa at: «det er veldig stort fokus på å bygge opp reaktiv kapasitet» (SE2). En annen informants uttalelse støttet denne endringen:

> Fokuset var tidligere mest på å beskyttelse for å forhindre, mens nå er det oppdag og håndter. Det er omtrent 50/50, kanskje mer på oppdag, håndter og til og med forutse. Tradisjonelt har tilnærmingen vært forhindre – ha brannmur, antivirus og så videre. (TM3).

Den tradisjonelle tilnærmingen til styring av sikkerhet ved å forhindre ser dermed ut til å ha endret seg, og det viser også funn fra finanstilsynet og øvrige dokumenter. Rapportering og regulering kan ha påvirket denne endringen, og har på sin side utviklet seg til å bli mye mer omfattende det siste tiåret.

5.3.2 Rapportering og regulering

Funn fra dokumentstudiet viser at finanssektoren i 2009 ble pliktige til å rapportere IKT-hendelser, både operasjonelle- og sikkerhetshendelser, som ble vurdert alvorlige og som påvirket virksomhetens evne til å fungere normalt (Finanstilsynet, 2010). Rapporteringen fra finansvirksomhetene er et tiltak som har flere positive effekter. Det bidrar til at finanstilsynet kan kartlegge og føre tilsyn med sektorens bruk av IKT. Gjennom å føre tilsyn blir virksomhetene tvunget til å ta stilling til risiko, sårbarheter og utfordringer knyttet til bruken av IKT. Finanstilsynet har myndighet til å trekke konsesjonsretten fra virksomheter dersom kravene tilknyttet forsvarlig og sikker bruk av IKT ikke opprettholdes. Man vil da være «out of business» som en av informantene sa (TM3). Han forklarte videre at han opplevde at:

> Det har nok en effekt på at man må gjøre tiltak for å unngå at det skjer igjen, så det har en god effekt på finansinstitusjoner at man må gjøre rapportering i form av at man og må gjøre tiltak. Finanstilsynet stiller jo spørsmål hvis det skjer flere ganger uten tiltak. (TM3).

Finanstilsynets krav til rapportering oppleves som svært positivt, selv om flere av informantene opplever at det er «flaut» å rapportere, så har det en effekt. En av systemeierne utdypet «så jeg tenke det er positivt ja, da kan man bruke det. Vi som jobber med sikkerhet kan bruke det som en brekkstang for å få endring på rutiner eller gjennomslag for å få system i sving» (SE2).

Rapportering bidrar til at man får fokus, øker erkjennelsen og demonstrerer behovet for å gjøre tiltak. Funnene fra ROS-analysene til finanstilsynet fra 2009-2019 viser at det har vært

en varierende rapporteringsgrad mellom ulike virksomhetsområder i finanssektoren. Det er definitivt virksomheter knyttet opp mot betalingsformidling og finansielle tjenester som har vært «flinkest» til å rapportere. Verdipapir og forsikringsområdene har i løpet av de siste årene økt rapporteringsgraden for sitt område. Dette støttes opp av informantene, hvor en sa følgende: «banksiden har jo vært flinke i alle år, men det hender at informasjon må etterspørres» (TM4). I forhold til ulik rapportering mellom virksomheter og områdene i sektoren, vil det trolig ikke minske effekten av å måtte rapportere. Som en informant forklarte så: «gir det en effekt for når det stilles krav til arbeidet med hendelsen. (...) det er ikke sikkert at dette arbeidet hadde vært like godt dersom det ikke ble stilt noen krav» (TM1). Videre sa informanten: «det er helt klart at det har en effekt». Varierende rapportering knyttes opp mot størrelse på virksomheter, som må forstås i lys av store og små virksomheters evne til å håndtere ulike hendelser. For eksempel vil et DDoS-angrep mot DNB trolig ikke ramme like hard som hos en lokal sparebank, fordi DNB har en egen sikkerhetsenhet dedikert til å detektere og håndtere slike hendelser. De har mer ressurser og mulighet til å investere i slike tjenester enn mindre foretak (Finanstilsynet, 2018; Departementene, 2019; Næringslivets sikkerhetsråd, 2018).

Rapportering sørger for at virksomheter til enhver tid følger reguleringer og bidrar til å sette fokus på gjeldende reguleringer. I løp av det siste tiåret har regulering økt for å sørge for god cybersikkerhet. Gode eksempler er Nasjonal Strategi for Digital sikkerhet 2019, EU sin personvernsordning GDPR, NIS-direktivet og ny sikkerhetslov. Både rapportering og regulering betraktes som positive tiltak for å øke sikkerheten knyttet til cyber-domenet. En av informant sa følgende:

> Det jeg pleier å si, litt sånn halv-flåsete, er at det du ikke blir fulgt opp på bruker du ikke tid eller energi på som det du blir fulgt opp på. Så uten disse kravene ville nok foretak hatt en noe mer lemfeldig håndtering av dette her tror jeg. (TM4).

Den omfattende oppfølgingen finanstilsynet gjør i forhold til rapportering bidrar dermed til at virksomheter fatter tiltak og selv holder oppsyn med bruk av IKT. Reguleringen knyttet til for eksempel utkontraktering av IKT-tjenester (se kapittel 5.2) demonstrerer at tilsynsmyndigheter stiller krav og krever tiltak for at utkontraktering skjer innenfor et akseptert sikkerhetsnivå. Nøkkelinformantene belyste også dette med følgende: «så man har kniven på strupen for å følge reguleringer, og der har det jo også blitt mer fokus på sikkerhet»

(NI1). Reguleringen gir en positiv effekt på sikkerhet, ved at det settes mer fokus. I tråd med organisatoriske endringer kan regulering være en faktor som bidrar til at ledelse erkjenner risikoen og dermed at fokuset i organisasjonene blir større.

Regulering oppleves tidvis som en utfordring, særlig blant ledere, viser PWC sin årlige CEO-survey (PWC, 2018b). Overregulering som fører til en «compliance risiko» er en stor bekymring hos toppledere, det samme er cybersikkerhet. Regulering blir da et nødvendig onde, for å forsikre seg om at virksomheter har en praksis som er sikker nok. En av informantene trakk frem reguleringsproblematikken og utdypet:

> Jeg tror det alltid er en bekymring, men alt i alt er min observasjon at for eksempel GDPR løfter informasjonssikkerhet og samfunnssikkerhet veldig. Altså det skapes bevissthet. Det har blitt gjort ting internt hvor det blir oppdaget at man må gjøre sikkerhetstiltak, så begynner man å bli bedre på sikkerhet. (NI1) .

Selv om det kan være utfordrende å holde følge med reguleringer, særlig ettersom det kommer nye reguleringer, nye lover og nye krav, har det en reell effekt ettersom den fører til tiltak for å ha god cybersikkerhet. Nøkkelinformanten forklarte:

> Det er jo for det har vært den første store sektoren som har vært digitalisert, hvor det har blitt lagt mye penger i IT, og hvor sikkerhet har vært en del av reguleringsmyndigheten. Det har jo vært en viktig del av det. Hadde ikke finanstilsynet vært så opptatt med informasjonssikkerhet, som IKT-forskriften er, så hadde det ikke vært det samme og det er jeg overbevist om. (NI1).

Flere av informantene i dette studiet har trukket frem at reguleringene gjennom PSD2 og økende konkurranse i betalingsformidling er faktorer som kan påvirke cybersikkerhet. I dag går den teknologiske utviklingen hurtig. Trenden man ser i utvikling av nye applikasjoner for betalingsformidling, som kan påvirke cyber-risiko, er økende. Frykten er at sikkerhet kan gå på bekostning av å holde følge med konkurransen i markedet. Tross denne frykten, oppleves regulering og rapportering som noe positivt av informantene i dette studiet, noe som også støttes opp av dokumentene. Regulering og rapportering påvirker også organisasjoner gjennom å stille nye krav og legge nye føringer, som i sin tur bidrar til organisatoriske endringer.

5.3.3 Organisatoriske endringer

Hvordan risikostyring har endret seg, kan ikke separeres fra hvilke endringer som har skjedd organisatorisk i finanssektoren. En av informantene trakk frem at finanssektoren i Norge er kjent for et utstrakt samarbeid i møte med ulike trusler, og at samarbeidet startet allerede på tidlig 2000-tallet. «Det interessante her er at det skaper en samarbeidskultur som følger bankvesenet gjennom hele utviklingen» (NI1). Dette samarbeidet har i senere tid blir formalisert, og Finanstilsynet (2016) har rost foretakene for å ha etablert gode samarbeidsarenaer og informasjonskanaler. Opprettelsen av NF CERT i 2014 er et formalisert samarbeid, ikke bare mellom norske virksomheter, men også mellom de skandinaviske landene.

I takt med digitaliseringen av finanssektoren, med fordelene og utfordringene de har brakt med seg, har det tvunget organisasjonene til å endre seg. Finanssektoren har alltid vært opptatt av sikkerhet og av å sikre sine verdier. For finanssektoren er tap som følge av cyber-hendelser ofte veldig synlige, og en del av oppgavene til bankene er å beskytte pengene til kundene.

Dersom noen skal rane en bank kan de gjøres via det digitale domenet. Dette krever at bankene beskyttes digitalt. Flere informanter og dokumenter nevner at cybersikkerhet har beveget seg fra datarommet i kjelleren opp til konsernledelsen i øverste etasje. En av informantene som tidligere hadde jobbet i bank forklarte at lederes holdning til cybersikkerhet for 10 år siden var dårlig, men i 2019 opplevde informanten dette annerledes. Informanten forklarte: «det er en helt annen bevissthet på ledelses- og styrenivå enn de hadde før, og det er en helt annen kobling. Det er en tettere kobling på cyber- og IT-sikkerhet enn det var før opp mot ledelse og styre» (TM3). Videre sa han: «de er genuint redde for at cyber-trusler kan påvirke og gi negative konsekvenser for virksomheten» (TM3). Frykten som ledere har utviklet for cyber-trusler henger antageligvis sammen med de ulike cyber-angrepene som har rammet andre sektorer, samt hvilke alvorlige konsekvenser det vil gi for finanssektoren.

Risikoerkjennelse

I lys av finanstilsynet sine ROS-analyser som startet allerede i 2002 har erkjennelsen og bevisstheten for risiko knyttet til IKT vært tilstede i snart to tiår, selv om trusselen i dag sammenlignet mot 2002 er helt annerledes. Det visser likevel at enkelte deler av finanssektoren allerede i 2002 erkjente farene knyttet til IKT og digitalisering, og at de ble tatt

på alvor. Uttalelsene til informantene tyder på at det har vært en erkjennelse i finanssektoren over hvor viktig cybersikkerhet har blitt. Det er en erkjennelse av hvilken risiko cyber representerer. En av informantene forklarte: «men det er jo den erkjennelsen, sånn som når Rune Bjerke uttalte i DN for en tid tilbake går ut og sier at neste finanskrise kan bli trigget av en cyberhendelse». (NI1). At risiko blir erkjent hos ledere er helt sentralt for å sette fokus i hele virksomheten, og finansvirksomheter må forstå at de er en digital virksomhet i kraft av at finanssystemet er heldigitalisert.

En annen informant trakk dette frem: «man har fått flyttet det opp til at erkjennelsen av at når Rune Bjerke sier 'vi er en IT-bedrift' så er det å skjønne at man har en digital virksomhet og man må ha det mindsettet, der har det skjedd mye på 10 år.» (NI2). Det trekkes frem i dokumentene at det er virksomhetens ledere som må godkjenne risiko knyttet til bruk av cyber, og da er det en forutsetning at de erkjenner hvilken risiko cyber-risiko representerer.

Erkjennelsen av at cyber-risiko kan gi ringvirkninger på tvers av virksomheten, har vært sentral. En av informantene trakk frem at cyber-risiko kan være en operasjonell risiko, som kan gi finansiell risiko i form av økonomiske tap eller sanksjoner fra tilsynsmyndigheter dersom man ikke har tilstrekkelig cybersikkerhet. Videre ble det forklart: «så er det jo andre (risikoer) tilknyttet renomme-risiko, og kanskje, vet ikke om jeg vil dra inn markedsrisiko temaer, men mulig at det er en form for markedsrisiko» (TM4).

Dernest syntes erkjennelsen av at cyber-risiko kan påvirke omdømmet å være helt sentralt, og det blir nevnt av flere informanter. I Norge er finanssektoren avhengig av tillit fra kunder og samarbeidspartnere, og cyber-risiko kan påvirke denne tilliten. En informant forklarte:

> Det handler om tillit, for det er utrolig viktig å ha tillit fra kunder og myndigheter. Har du ikke det så har du ikke en business, sant. Man vil jo ikke sette pengene sine inn i en bank som ikke har god sikkerhet – har de flere hendelser eller dårlig sikkerhet så får du jo ikke kunder. Det er jo for penger er noe folk har et veldig, hva skal man si, et veldig bevisst forhold til. Så du vil ikke gi dem til noen du ikke stoler på. (TM3).

Det er helt avgjørende for banker at cybersikkerheten er på et nivå der kunder, samarbeidspartnere og myndigheter har tillit til at det er på et akseptabelt sikkerhetsnivå. Som en annen informant sa: «hvis jeg ikke kan stole på at banken har kontroll på innskuddene

mine så er jo det veldig veldig alvorlig» (TM1). Tapet av omdømme kan være så betydelig at det påvirker hele forretningsdriften. Denne erkjennelsen har vært viktig for at man skal iverksette tiltak og håndtere risikoen eller mitigere den til et akseptabelt nivå. En av informantene knyttet motivasjonen for forebygging opp mot omdømmet og sa: «det betyr at tapet på 20 millioner på nettbank er uproblematisk, men omdømme og tilliten til de tjenestene er helt 'devestating'. Derfor har man vært så ekstremt aggressiv, det er en primær motivasjon» (NI1). Motivasjonen basert på erkjennelsen har vært sentral for å sette fokus på problemet. Fokus bidrar i sin tur til å øke bevisstheten i virksomhetene.

Fokus

Ettersom cybersikkerhet har blitt noe som påvirker en hel virksomhet, er det sentralt at det er likt fokus hos alle i en virksomhet, og at det er bevissthet rundt risikoen. En organisatorisk endring er at bevisstheten omkring ansvar legges til virksomhetsledere. Departementet skriver «virksomhetsledere er ansvarlig for å foreta risikovurderinger, og på bakgrunn av dette gjennomføre tilstrekkelige tiltak» (Departementene, 2019, s.13). Tidligere har det også vært en virksomhetsoppgave, men denne har ofte blitt delegert nedover i en organisasjon eller utkontraktert til leverandører. «For 10-15 år siden var svært få interessert i IT-sikkerhet, det var bare et nødvendig onde» forklarte en informant (TM3). En annen informant sa: «for 10-15 år siden var IKT-sikkerhet noe man la til IKT-avdelingen, og jeg tenker at i 2019 så er det et tema på styrenivå» (NI2). Begge disse uttalelsene viser til at ledere har et helt annet fokus på temaet i dag, og at det ansees som en utfordring som må tas på alvor. Dette alvoret er tett knyttet opp til erkjennelsen av at cyber-domenet medfører endringer i sårbarhet og risiko, som i sin tur påvirker risikobildet.

En av driftsleverandørene fortalte at: «det har etterhvert blitt slik at fokuset er helt annerledes i forhold til sikkerhet. Det er jo det trusselbildet som vi ser, og så ser vi at kunder er mye mer fokusert på sikkerhet, så det er jo en temmelig stor forskjell» (DL2). Bevisstheten kan også skyldes økt oppmerksomhet fra myndighetsorganer, slik som finanstilsynet. Den pliktige rapporteringen av IKT-hendelser er et virkemiddel for å skape fokus hos virksomhetene, og det har gitt tydelig effekt hevder flere av informantene. Dette rettes ikke kun mot risikoer, men også mot hvilke tiltak som er og burde iverksettes.

Gjennom økt bevissthet fører det til iverksettelse av risikoreduserende tiltak, og et vanlig tiltak er å skape bevissthet hos ansatte. Gjennom såkalt «awareness-training» (bevissthets-trening) blir ansatte opplyst om hvilke trusler de kan bli utsatt for, og hvilke risikoer det medfører dere virksomhet og i noen tilfeller seg selv. Informantene opplevde bevissthet som «veldig viktig» og at det må være en del av den «etablerte strategien» (SE1). Videre nevntes det at bevissthets-treningen burde skje hyppig, «løpende drypp for ting går fort i glemmeboken» (TM4). Det er helt sentralt at man har bevisste ansatte i møte med cyber-risikoer. Som belyst i kapittel 5.2 kan menneskelige feil knyttes mot organisatoriske føringer, da organisatoriske føringer påvirker hvordan mennesker forholder seg til cybersikkerhet og hvordan man samhandler med cyber-domenet. Videre har dette fokuset bidratt til å øke ressursene som brukes på it-sikkerhet. «Man ser at kostnaden knyttet til IT-sikkerhet også øker generelt» sa en av systemeierne (SE1), det knyttes opp mot endring i risiko og at bevissthet og fokus tydeliggjør behovet for ressurser i møte med risikoen.

«Jeg opplever at det er et veldig paradigmeskift i forhold til sikkerhets/IT-fokus» sa en av informantene (NI1). Dette «paradigmeskiftet» kan relateres til samfunnsutviklingen for øvrig, og må ses i lys av ledelse. Ledelse og ledere har en sentral rolle i å sette fokuset, og en ny leder kan endre en hel virksomhet sitt fokus på sikkerhet. Dette har vært tilfelle hos en av driftsleverandørene, og følgende ble forklart:

> Vi har fått en ny konsernsjef nå som har et helt annet fokus på det enn forgjengeren. Mye mer fokus. Så det er jo bygget opp en egen sikkerhetsdivisjon som da har et ansvar på tvers av selskapet. Det går på at de skal serve alle disse forretningsområdene med sikkerhetstjenester som skal være en bunnpanne for selskapet for å håndtere det som er en av angrepsvektorene som vi må forholde oss til. Så det er en viktig rolle. (DL1).

Dette eksempelet er ett av flere, og som nevnt tidligere oppfattet informantene at først når cybersikkerhetsutfordringene er erkjent hos ledelsen, bidrar det til å sette fokus for så å skape bevissthet på tvers av virksomhetene. Under intervjuene ble informantene spurt hva som kjennetegner god IKT-sikkerhet i en virksomhet, og selv om svarene var noe varierende nevnte alle at ledelse, organisatoriske forhold og topp-bunn forankring. En informant sa: «sikkerhet er ikke noe kun en organisatorisk enhet skal drive med, men alle skal drive med» (SE2). Dersom alle i en organisasjon skal drive med det, er det en forutsetning at ledelse ser

dette som et prioritert område og at alle ledd i organisasjonen blir gjort bevisste. Endringen i tilnærming til cybersikkerhet kan ses på som en modningsprosess. Neste seksjon vil ta for seg nettopp dette.

5.3.4 Cybersikkerhet som en modningsprosess

I løpet av bare det siste tiåret har det skjedd enorme teknologiske utviklinger og innovasjoner, som har påvirket finanssektoren. Fremvoksende FinTech (finansiell teknologi) løsninger endrer betalingsformidling, skaper nye muligheter og nye utfordringer. Utviklingen av cybersikkerhet kan ses som en modningsprosess, hvor man kontinuerlig utvikler og lærer mer om terrenget man befinner seg i. En av informantene fortalte «jeg tenker at måten næringen jobber med dette (cybersikkerhet) på har blitt profesjonalisert, og man har lært.» (NI2).

I Norges Bank sin rapport på finansiell stabilitet og finansiell infrastruktur er det gjort noen svært interessante funn. Ettersom denne oppgaven har undersøkt utviklingen av cyber-risiko de siste 10 årene ble det gjort et søk av ordet «cyber» i alle publiseringene. Dette for å kartlegge når Norges Bank vektla dette som faktorer som påvirker den finansielle stabiliteten og finansielle infrastrukturen i Norge. Resultatet fra søket er presentert i tabellen under:

	Antall ganger «cyber» blir nevnt:	
Årstall	Finansiell Stabilitet	Finansiell Infrastruktur
2009-2015	0	0
2016	0	16
2017	16	28
2018	12	48

Tabell 4: Ordsøk av antall ganger "cyber" nevnes

Kilde: Norges Bank, 2009a-2018a; Norges Bank, 2009b-2018b.

Som tabellen indikerer, er det lite oppmerksomhet dedikert til cyber frem til 2016, noe som tyder på at bevissthet overfor risikoen knyttet til cyber-domenet har endret seg betydelig. Det kan ses i lys av at digitalisering i finanssektoren og utviklingen av truslene har vært en gradvis prosess, og modningen i bevissthet har dermed fulgt den gradvise endringsprosessen. Modningen for cybersikkerhet i finansvirksomheten står i motsetning til kritikken NSM gir norske virksomheter. NSM kritiserer norske virksomheter i forbindelse med kompetanse og innsats for å minske cyber-risikoen (2018b). Finanstilsynets tiltak og økende fokus på cyber

tyder derimot på at finansvirksomhetene har modnet sin styring av cyber-risiko. Selv om finanstilsynet i 2015 etterlyste og fremhevde behovet for bevisstgjøring og opplæring for å motstå digitale angrep, har det vært viktig å følge cyber-risiko i finanssektoren. Ettersom det har blitt innført et strengt rapporteringsregime på IKT-hendelser, tyder det at finanssektoren er et av de virksomhetsområdene som er langt fremme både i kompetansebygging og innsats for å minske og håndtere cyber-risiko. Rapportering av hendelser til myndighetene tyder på at oppmerksomheten på cybersikkerhet har vært stabilt økende det siste tiåret, og cybersikkerhet har blitt en del av sikkerhetskulturen. Funnene fra dokumentene viser derimot at problematikken ligger i at cyber-truslene er økende.

Flere av informantene kritiserer de nasjonale trussel- og risikovurderingene ved å poengtere at det ikke rettes stor nok oppmerksomhet mot problematikk knyttet til cyber-risiko. Det nevnes blant annet at oppmerksomheten som dedikeres til cybercrime på det nasjonale nivå er langt mindre enn oppmerksomheten som dedikeres fra næringslivet (NI2). Dette funnet syntes å være interessant da det demonstrerer et tydelig gap mellom nasjonale dokumenter og refleksjoner fra finanssektoren. Det tyder på at finanssektoren sin oppmerksomhet og bevissthet på risikoen synliggjør et modenhetsnivå som er lengre foran enn andre sektorer. En av informantene sa «finanssektoren er jo langt fremme på dette her. Det er en veldig moden sektor» (TM3). Opprustningen av sikkerhetsorganisasjoner de siste årene viser også til en modning. En av informantene nevnte dette i forhold til endring i tilnærming for å styre risiko, han forklarte:

> Hva må de gjøre? Risikovurdering og internkontroll, risikovurdering og interkontroll. Det er jo det som er løsningen på alt, og det gjør jo egentlig at man bare pusher flere organisasjoner til å gjøre det, altså bygge en stor sikkerhetsorganisasjon slik de store norske bankene har gjort. (NI1).

Virksomhetene i finanssektoren har vært nødt til å bygge opp både proaktive og reaktive kapasiteter for å holde et sikkerhetsnivå som er tilfredsstillende i møte med risikoene. Det har vært et økende fokus på slik beskyttelse i tråd med en betydelig økt risiko for å bli rammet. Ettersom modningen har vært såpass betydelig i forhold til tilnærmingen til cybersikkerhet er det helt naturlig at det brukes ressurser på å bygge robusthet. En informant sa «jeg tenker at finanssektoren har den robustheten den selv lager» (NI2). Robustheten har følgelig blitt styrket, eksemplifisert i tiltakene virksomheter og myndigheter har gjort.

5.3.5 Oppsummering

Det er utfordrende å definere i hvilken grad risikostyring har endret seg, men det er åpenbart at det har skjedd en del forandringer for risikostyringen av cyber-risiko i sektoren. Tilnærmingen til sikkerhet har endret seg som følge av økt forståelse av cybersikkerhet. Etterhvert som man har blitt mer kjent med risikobildet har behovet for kartlegging av trusselaktører vist seg. Det krever høy kompetanse for å kartlegge, forstå og holde følge med endringene, og den risikobaserte tilnærmingen til sikkerhet og risikostyring fremstår som helt avgjørende. Det fører videre til de organisatoriske endringene som har forekommet i sektoren. Sammen med erkjennelsen av omfanget cyber-risikoen representere for virksomheter, har det ført til bevissthet blant ledelse og nedover i organisasjoner. Videre er ledelsens forståelse for cyber-risiko betydningsfullt for at det skal bli iverksatt risikoreduserende tiltak. Risikostyringen for cyber-risiko kan ses i sammenheng med utviklingen av cybersikkerhet som en modningsprosess. I denne modningsprosessen har organisasjoner erfart og lært, og dette har ført til tiltak og organisatoriske endringer som har resultert i endringer i risikostyring.

6. Drøfting

I dette kapittelet løftes blikket fra det spesielle til det generelle. De empiriske funnene redegjort for i kapittel 5, vil bli diskutert opp mot teorien som ble presentert i kapittel 3. Tidligere forskning vil også bli inkludert i drøftingen der det er relevant, da tidligere forskning kan støtte opp om både teori og empiri. Strukturen i kapittelet følger forskningsspørsmålene, i likhet med kapittel 5. Drøftingen leder opp til problemstillingen som omfatter hele denne oppgaven, nemlig hvorfor cyber-risiko i finanssektoren har utviklet seg de siste 10 årene? Dette spørsmålet vil bli besvart i kapittel 7, konklusjon.

6.1 Hvordan har cyber-truslene mot finanssektoren utviklet seg de siste 10 årene?

Empirien viser at cyber-truslene mot finanssektoren har hatt en voldsom utvikling det siste tiåret. Funnene fra dokumentstudiet skisserer et økende og stadig mer utfordrende trusselbilde mot finanssektoren. Hvert år siden 2011 har det kommet en ny form for cyber-trussel eller metode for å gjennomføre cyber-angrep, hvilket demonstrerer hvor omfattende cyber-domenets trusler er. Det kommer særlig frem i lys av angrepsmetodikk og trusselaktører, samt et skifte i hvem som angripes. Trusselaktørens utvikling er en av de fremste cyber-truslene mot sektoren og utviklingen må ses i lys av hvem trusselaktøren er, motivasjon og kapabilitet. Fra empirien er det særlig fem utviklingstrekk som er bekymringsfulle, det er: 1) profesjonalisering, 2) økende kompleksitet-, sofistikert og avanserte angrep, 3) uoversiktlighet, 4) rask utvikling, og 5) økende ressurser blant trusselaktører.

Utvikling og økende trussel

Som belyst gjennom empirien har cyber-truslene mot finanssektoren utviklet seg enormt de siste 10 årene. Finanssektoren er et system som består av flere systemer og komponenter, og som på et vis kan betraktes som et høyteknologisk system. I et høyteknologisk system hevder blant annet LaPorte og Consolini (1991) at det er mulig å forebygge systemulykker. Systemulykker kan forårsake trusler som krever at man organiserer seg slik at man kan holde funksjonalitet selv om det forekommer alvorlige uønskede hendelser. Dersom en trussel forsøker å skape en uønsket hendelse, vil det være viktig at man har et pålitelig system og en pålitelig organisasjon. Teorien om høy pålitelige organisasjoner (HRO) kan omsettes når man undersøker hvordan trusselbildet har utviklet seg, også i forhold til trusselaktører og opplevelsen av at truslene har økt. Rosness et al (2004) trekker frem at organisatorisk redundans kan forhindre at et system bryter sammen som et resultat av uønskede hendelser.

En av informantene nevner redundans ved at man bygger inn sikkerhetsmekanismer som forhindrer en trussel i å ødelegge eller spre seg i systemet. Det handler om å ha flere lag med sikkerhet (Rosness et al., 2004). Når man har flere lag med sikkerhet vil man, i følge Perrow (1984), øke kompleksiteten i systemet. I teorien om normale ulykker (NAT) hevdes det at et system som er tett koblet og preget av komplekse interaksjoner, slik som finanssektoren, på et gitt tidspunkt vil bli utsatt for en alvorlig ulykke. Fordelen ved å bygge inn redundans som en sikkerhetsmekanisme kan dermed bli en ulempe i lys av Perrow (1984) sin teori om normale ulykker. Dette vil bli diskutert videre i kapittel 6.2.

Weick og Sutcliffe (2007) skriver at årvåkenhet (mindfullness) handler om å ha evnen til å oppdage og håndtere uventede hendelser, og at det krever at man er oppmerksom på systemet man opererer i og med. De fem utviklingstrekkene som skildres i empirien vitner om at fokuset på cyber-trusler er høyt og at finanssektoren er svært årvåkne i møte med både et skiftende trusselbilde og trusselaktører. Empirien er samstemt når det gjelder utviklingstrendene, og det står liten tvil om at trusselbildet er krevende for finanssektoren. Det kan tenkes at en av årsakene til at finanssektoren har etablert en årvåkenhet for truslene, er konsekvenspotensialet det har mot deres verdier. Det nevnes gjennomgående i empirien at finanssektoren, både i dag og historisk, har vært veldig bevisst på hvilke verdier de forvalter. Det krever at finanssektoren består av pålitelige organisasjoner som er i stand til å tilpasse seg dynamiske trusler og sårbarheter som følge av digitaliseringen.

Konsekvensene vil kunne ramme finanssektoren på ulike måter. For eksempel kan forretningsforstyrrelser gi direkte og kortsiktige effekter som kan håndteres ved at organisasjonen omstiller seg, mens et datainnbrudd trolig vil kun påvirke den eller de virksomhetene som blir utsatt for angrepet (Bouveret, 2018). Bouveret (2018) sin forståelse av datainnbrudd hos en virksomhet kan problematiseres. Dette fordi en hendelse i et system kan gi ringvirkninger på andre systemer, derav er det behov for å ha systemer som raskt kan omstille seg, og hvor beslutninger kan tas for å håndtere uønskede hendelser (Bouveret, 2018). Hendelsen som rammet Maersk i 2016 (se vedlegg 8) demonstrerer at et angrep på cyber-domenet kan gi dramatiske konsekvenser for en ulykkes utenforstående parter, jamfør Perrow (1984). Maersk var en utenforstående part og et «tilfeldig» offer for cyber-angrepet som var ment å ramme Ukraina.

Trusselaktører: motivasjon, kapabilitet og utvikling

I kapittel 3 ble begrepet trussel forklart som en årsak til en uønsket hendelse (Budmundrud et al., 2015; NS5814:2008), hvor kapasitet til og intensjon for å forårsake en hendelse med formål om å skade eller ødelegge. Slik cyber-trusler skildres i empirien må de forstås i lys av et «security»-perspektiv. Det er begrunnet i at truslene er både er tilsiktede og har som intensjon å påføre skade eller ødeleggelse (Bohom et al., 2016). På en side kan de ulike sikringstiltakene som har blitt iverksatt for å håndtere truslene forklare hvorfor det ikke har forekommet noen alvorlige systemulykker. På den andre siden kan sikringstiltakene forklare hvorfor trusselaktørene har utviklet sine metoder (Pietre et al., 2010). Det trekkes nemlig frem at sikringstiltak kan virke mot sin hensikt ved å føre til at trusselaktører finner nye metoder for å gjennomføre sine handlinger (Engen et al., 2016).

Basert på empirien kan man skissere ulike scenario og plassere dem inn i trefaktormodellen. De følgende scenarioene tar i bruk «security»-perspektivet, hvor trussel referer til en tilsiktet hendelse. Basert på funnene er det to fremtredende trusselaktører mot finanssektoren: fremmede stater og organiserte kriminelle. Fremmede stater og organiserte kriminelle blir brukt som en samlebetegnelse for en rekke ulike trusselaktører og grupperinger, eksempelvis er både Kina og Russland trusselaktører, men de refereres til under betegnelsen «fremmede stater». Utviklingstrekkene som har blitt trukket frem i empirien vitner om at risikoen for at trusselaktørene klarer å gjennomføre et vellykket angrep har økt. De «to» trusselaktørene har ulike formål med å angripe finanssektoren ved at de er på jakt etter ulike verdier. Sårbarhetene kan knyttes opp mot svakheter i teknologi, manglende sikringstiltak og barrierer som følge av utviklingen blant trusselaktørene som fører til organisatoriske svakheter og utnyttelse av teknologi, for å nevne noen.

Scenario 1 blir dermed følgende: Russland (trusselaktør) gjennomfører en omfattende etterretningsoperasjon i den norske finanssektoren hvor de henter ut sensitiv informasjon (verdi) som bryter med sikkerhetsmålene knyttet opp mot konfidensialitet, integritet og tilgjengeligheten for informasjonen. Dette blir gjort ved å utnytte et systems sårbarhet gjennom skreddersydd spyware som blir liggende i systemet over lengre tid uten å bli detektert. Risikoen vil kunne kvantifiseres ved å se på Russland sine kapasiteter og motivasjoner for å gjennomføre et angrep, og en sårbarhetsanalyse av finanssektorens systemer og tiltak. Dersom det er gode detekteringssystemer som oppdager spyware eller

forsøk på å infiltrere et system, kan det være mulig å forhindre angrep ved å redusere sårbarhet og risikoen vil bli lavere.

Scenario 2 er følgende: En organisert gruppe kriminelle (trusselaktør) har flyttet sin kriminelle virksomhet over til cyber-domenet og utgjør dermed trusselaktøren mot finanssektoren. Denne grupperingen lykkes i å gjennomføre et omfattende DDoS-angrep på en av de mindre bankene i den norske finanssektor, som en avledningsmanøver for å infiltrere et betalingssystem for å observere hvordan transaksjoner blir gjennomført. Etter å ha observert transaksjonsflyt og hentet ut kundeopplysninger er de i stand til å «hacke» seg inn i nettbanken til kunder hvor det opprettes falske transaksjoner til en norsk skall-konto, som så viderefører pengene ut av landet. Verdien de er ute etter er penger, og sårbarheten de utnytter er mindre organisasjoners begrensede evne til å detektere og håndtere et cyber-angrep. Slik utnyttes de sårbarhetene mindre banker har gjennom lavere teknisk kompetanse og færre ressurser dedikert til cybersikkerhet. I dette scenario vil tilgjengeligheten av økonomiske verdier kompromitteres, samt integriteten til systemet.

De to scenarioene belyser hvilken nytte trefaktormodellen kan gi, ved at man kan gjøre subjektive vurderinger som videre kan kvantifiseres ved tilgjengelige data. I finanssektoren er det viktig at de ikke utelukkende er bevisste på trusler, men også på verdier og sårbarheter. En sårbarhetsanalyse vil derfor være viktig når man skal iverksette sikringstiltak. Underveis i studien kommer det frem at finanssektoren er særlig utsatt for APT og CEO-svindel, og at det antas å være fordi sektoren er nært knyttet til en svært ettertraktet verdi – penger og informasjon. Det gir mye av forklaringen på hvorfor sektoren opplever et økt trusselnivå og hvorfor det stadig forekommer nye fremgangsmåter for å angripe. Det kan i sin tur knyttes opp mot at evnen til å redusere og avdekke sårbarheter henger etter trusselaktørenes evner, teknologi og ferdighet. Dette illustreres gjennom konkurransen for å få ut nye tjenester, ved at det er viktigere å henge med i markedet enn å vurdere risikoen knyttet til ny teknologi. Empirien viser at markedskonkurranse for nye tjenester og applikasjoner kan gå på bekostning av sikkerheten, og dette kan bli utnyttet av trusselaktørene. Trusselaktører kan dermed dra fordel av sårbarhetene i ny teknologi når den lanseres på markedet.

Delkonklusjon

I lys av diskusjonen ført over, ønsker jeg å trekke frem at truslene mot finanssektoren har blitt mer konkrete og spisset mot finanssektoren det siste tiåret. Charles Perrow sin teori om

normale ulykker, bidrar til å belyse at finanssektorens interaksjoner og koblinger gjør at trusselaktørene kan forårsake enda større ulykker med større konsekvenspotensiale forutsatt at de lykkes i sine forsøk. High Reliability Theory utdyper hvor viktig det er at finanssektoren organiserer seg på en slik måte at potensielle trusler ikke er i stand til å forårsake storulykker, selv om de lykkes i å kompromittere en del av systemet. Ved å ha en organisasjon som preges av årvåkenhet, omstilling og resiliens, kan dermed finanssektoren møte truslene, selv om de er i konstant utvikling. Cyber-truslene burde ikke forstås som et problem kun forårsaket av utenforstående, men bør også ses i lys av de organisatoriske rammene som finnes i sektoren.

I lys av bevisstheten omkring truslene man kan bli utsatt for, vil det være naturlig at organisasjoner fatter sikringstiltak for å hanskes med risikoen som trusselaktører utgjør. Trefakormodellen kan bidra til å skape forståelse for scenariotenkning ved å angi hvilke trusler, verdier og sårbarheter som kan påvirke risiko. Det fører videre til at man erkjenner hvilken trussel ulike farer i systemet kan gi for cyber-risikoen. Dersom man utelukkende fokuserer på sikringstiltak, kan det føre til at organisasjoner unngår å inkludere andre viktige faktorer gjennom sin risikostyringsstyringsprosess. Risikostyringsprosessen vil bli diskutert i kapittel 6.3

6.2 På hvilken måte påvirker cyber-farer finanssektorens cyber-risiko?

I kapittel 3 redegjøres det for ulike tilnærminger til risiko. Risiko kan handle om potensiale for at en gitt trussel vil utnytte sårbarhetene til et sett av verdier som fører til skade (ISO 27005: 2018). Risiko kan også forstås som kombinasjonen av sannsynlighet og konsekvens, beheftet med en viss form for usikkerhet (Aven, 2015). Gjennom trefaktormodellen kan risiko handle om en trussels kapasitet og intensjon til å forårsake skade. Cyber-risiko må derfor vurderes i lys av trusler, farer og sårbarheter knyttet til bruk av cyber-domenet i finanssektoren, samt hvilke kapasiteter som eksisterer for at trusler og farer materialiseres. Det forstås som en del av sektorens operasjonelle risiko ettersom risikoen er knyttet til sektorens evne til å operere og være i drift. Hvilken påvirkning cyber-farer har på sektorens cyber-risiko gir ikke et entydig svar, da det må ses i sammenheng med hvilken forståelse man har for terminologien og hva som betegnes som en fare.

Ulik forståelse av terminologi

At det eksisterer ulike forståelser for terminologi knyttet til cyber og IKT, samt forståelser for cyber-risiko, -trusler og -farer har utmerket seg i dette studiet. Dette har kommet frem både gjennom dokumentstudiet og dybdeintervjuene. Selv om det virker som det utgjør en lav sikkerhetsmessig risiko, kan det gi utslag i hvilke tiltak som gjøres for å minske potensielle risikoer som særlig farer kan føre til. Det kan begrunnes med at risiko kan bli kommunisert utydelig og uklart. Renn (2008) belyser at risikokommunikasjon er en viktig del av risikostyringsprosessen da det bidrar til å skape forståelse for risiko. Dersom det tas i bruk ulike begreper og ulik forståelse for begrepene, kan risikokommunikasjonen bli utydelig, som i sin tur kan påvirke risikostyring negativt (Renn, 2008). Det krever at man har lik forståelse for hva de ulike begrepene innebærer, hvilket de empiriske funnene fra dette studiet bestrider. Empirien viser at det er stor forvirring i sektoren og at risikokommunikasjon og begreper rundt cyber-risiko og cyber-farer er uklar.

Studiet avdekket først og fremst ulike forståelser for begrepene cyber og IKT. I noen tilfeller blir begrepene brukt som synonymer, mens begrepene i andre tilfeller henviser til forskjellige konsepter. Ulikheten i begrepsforståelser er noe som informantene oppfatter som forvirrende. I tillegg har flere av informantene utfordringer med å forklare hvorfor det differensieres mellom begrepene, og hvor de ulike forståelsene kommer fra. I kapittel 5.2 ble det skrevet at informanter forstår cyber-hendelser som tilsiktede hendelser, mens IKT-hendelser referer til både tilsiktede og utilsiktede hendelser. Det er interessant i forhold til «safety» og «security»-perspektivene, særlig ettersom teori og forskning belyser hvor viktig det er å ha en felles forståelse for risiko og sikkerhet (Aven og Krohn, 2013; Dahl, 2000; Armour, 2016).

Empirien demonstrerer at det også er ulike oppfatninger for hva som er en cyber-trussel, en cyber-fare og en cyber-risiko. I finanssektoren er de uønskede hendelsene vanligvis knyttet til operasjonelle hendelser, heller enn sikkerhetshendelser (Finanstilsynet, 2018). Likevel, er fokuset hos informantene på de tilsiktede hendelsene og man kan hevde at risikoforståelsen blir dominert av et fokus på intenderte hendelser. Noe av forklaringen på dette kan være informantenes bakgrunn og deres tilnærming til trusler som faller inn i «security»-perspektivet, der trusler er tilsiktet. Det betyr at kompetansen informantene besitter, påvirker deres risikoforståelse (Armour, 2016; IRGC, 2017). Dokumentene bidrar på sin side til å belyse hvordan farer kan ha en negativ effekt på risiko. Aven (2015) forstår risiko som de

potensielle avvik som kan gi konsekvenser for måloppnåelse, og at det er usikkerhet knyttet opp mot konsekvensene. Hvorvidt avvikene er intenderte eller uintenderte, inkluderes ikke i risikoforståelsen. For å skape en mer helhetlig forståelse for den totale cyber-risikoen i sektoren, kunne det vært formålstjenlig å anvende både «safety»-, og «security»-perspektivet når man skal kommunisere og skape forståelse for cyber-risiko.

Videre bidrar empirien til å kategorisere farene som kan gi cyber-risiko. Kompleksitet, avhengighet, utkontraktering, konsentrasjonsrisiko og nedetid trekkes frem som farer som kan øke cyber-risikoen. Fra et «safety»-perspektiv, kan de omsettes i trefaktormodellen og kan betraktes som trusler (NS5814:2008; NS5830:2012). Man kan videreføre scenariotenkningen fra kapittel 6.1 for å omsette farer i et tredje scenario. Scenario 3 er knyttet til «safety»-perspektivet, og trusler blir erstattet med farene som truer finanssektoren. Verdiene blir både penger (økonomiske verdier) og informasjon, men vil ha størst potensiale til å ramme økonomi, eksempelvis finansiell stabilitet. Det skjer gjennom at farene som kompleksitet og avhengighet kan forårsake, blir materialisert gjennom at systemet blir så komplekst satt sammen og avhengig av en underleverandør grunnet utkontraktering, at sårbarhetene blir vanskelige å detektere og håndteres. I sin tur kan det føre til at finansiell stabilitet (verdi) svekkes og tilgjengelighet reduseres og i verste fall kompromitteres.

Farer

Kompleksiteten handler ikke primært om teknologien, men også om metodene som brukes for å ramme finanssektoren. I lys av Perrow (1984) sin teori om normale ulykker er finanssektoren et helhetlig system, preget av tette koblinger og komplekse interaksjoner. En cyber-hendelse, tilsiktet eller utilsiktet, kan føre til katastrofale konsekvenser (Paté-Cornell et al., 2018). Kompleksiteten som skapes i systemene, vanskeliggjør håndteringen av cyber-truslene, og de blir vanskelige å detektere. Selv om konsekvensene på kortsikt ikke fører til tap av liv og helse, kan truslene ha potensiale til å ramme den finansielle stabiliteten i Norge (jamfør Sikkerhetsloven §1.5, 2019). Det finnes flere eksempler som demonstrerer at for eksempel barrierer kan være en kompleksdrivende faktor. Perrow (1984) bruker Three Mile Island-ulykken for å belyse hvordan sikkerhetsmekanismer og barrierer kan øke kompleksitet i systemer og gi motsatt virkning. Det var også tilfelle under Piper Alpha ulykken i 1988. Årsaken til Piper Alpha-ulykken knyttes mot en sikkerhetsmekanisme som var designet for å forhindre at sjøvannspumpene startet automatisk, dette hadde motsatt effekt under Piper Alpha-ulykken, noe som resulterte i at flere ble drept (Harford, 2011). Knyttet opp mot cyber-

risiko kan prinsippene knyttet til redundans, kompleksitet og avhengighet trekkes frem som faktorer som kan føre til at konsekvensene ved en systemulykke blir svært alvorlige. Det er prinsippene i Perrow (1984) sin teori som er omsettelige til finanssektoren i lys av cyber-risiko.

Gjennom digitalisering har finanssektoren blitt mer avhengig av teknologiske systemer og digitale prosesser – det vil si at sektoren har gjort seg mer avhengig av cyber-domenet. Cyber-domenet består i sin tur av komplekse interaksjoner som svært ofte er i tidskritiske operasjoner, og det er tette koblinger som øker systemets avhengighet. Kompleksitet blir forårsaket av flere faktorer, og i empirien trekkes redundans, lange interaksjonskjeder, integrasjon, teknologi, aktører og metoder frem som noen faktorer som kan forårsake mer kompleksitet i et system. Årsaken til at et cyberangrep blir en normal ulykke er at det er den mest komplekse teknologien det interageres med og skaper avhengigheter i finanssektoren og samfunnet forøvrig. På grunn av de tidskritiske operasjonene som skal til for å holde liv i teknologien, samt den gjensidige avhengigheten mellom ulike infrastrukturer, kan alvorlige cyber-hendelser og cyber-angrep betraktes som normale ulykker.

Fra kompleksitet trekkes farene som kan forårsakes av utkontraktering frem. I lys av Perrow's teori ville man kunne hevde at utkontraktering vil gjøre et allerede komplisert system enda mer komplekst. Verdikjeden utvides, og man legger til et ekstra ledd – som fordrer at sikkerhetsnivået er på samme nivå på tvers av ulike organisasjoner.

Tilhengere av HRT vil argumentere for at finanssektoren ikke nødvendigvis vil bli utsatt for en ulykke, selv om det finnes svakheter hos underleverandørene. Dette er fundert på argumentet om at man kan ha en pålitelig organisasjon basert på upålitelige komponenter (Aven et al., 2004). Det fordrer at man har tydelig fordeling av ansvar, men også at ansatte på tvers av ulike virksomheter er bevisste på hvilke feil som kan oppstå, for så å raskt håndtere dem. Weick og Sutcliffe (2007) sitt argument knyttet til årvåkenhet kan øke bevisstheten for hvilke feil som kan oppstå. Feil som kan forårsakes av utkontraktering kompenseres for ved at finanssektoren organiseres på en måte som håndterer ulykker. Eksempelvis vil en organisasjon som er resilient ha evnen til å takle motstand og opprettholde sin funksjon selv om den møter uventede hendelser (Hollnagl, 1973). Resiliens kan sees i sammenheng med proaktivitet slik Sutcliffe og Vogus (2007) gjør. Det betyr at dersom finanssektoren evner å tilpasse seg uventede og utfordrende forhold som de kan rammes av som følge av

utkontraktering, vil det gjøre dem i stand til å håndtere slike forhold, men også styrke sektoren på lang sikt. I finanssektoren knyttes utkontraktering og konsentrasjonsrisiko sammen selv om de også forstås som to ulike farer.

Konsentrasjonsrisikoen i finanssektoren er et omdiskutert tema, og en av informantene hevder det er en filosofisk diskusjon. Konsentrasjonsrisiko vil henge sammen med hvilken tilnærming man har til risiko og sikkerhet, og hvilken tilnærming man har til styring. I lys av denne diskusjonen vil NAT hevde at desentralisering er en faktor som øker kompleksitet ved å inkludere flere aktører, som dermed øker sjansen for at ulykker kan oppstå. HRO vil på den andre side trekke frem styrkene ved å ha en sentralisert tilnærming, men understreker samtidig betydningen av å ha muligheten for spontan omstilling for å unngå ulykker (Sutcliffe & Vogus, 2007). Konsentrasjonsrisiko kan dermed være både en fare og en faktor som styrker systemet.

Avhengighet kan relateres til nedetid. Går man 20 år tilbake representerte ikke nedetid en like stor fare fordi avhengigheten av cyber-domenet på den tiden ikke var like stor. Avhengighet kan betraktes som en årsak til nedetid, men også ved at avhengigheter mellom systemer og annen infrastruktur kan øke konsekvensene forårsaket av nedetid. Konsekvensene som nedetid kan forårsake i finanssektoren er store, og nedetid i et system kan gi utslag i andre systemer. Påskehendelsen i 2011 er et god eksempel på dette. Perrow (1984) hevder at teknologi ikke kun bør forstås som rene teknologiske systemer, men også som menneskelige konstruksjoner. Menneskelige konstruksjoner kan relateres til de nye teknologiene som blir tatt i bruk i finanssektoren, og risikoene kan være store. Finanstilsynet trakk i 2014 frem at risikoen i finanssektoren var størst i tilknytning til endringer i system, infrastruktur og organisasjoner, og disse endringene forekommer oftest gjennom teknologisk utvikling. Et teknologisk system blir i dag ikke utviklet av seg selv, men utviklet og videreutviklet av mennesker. Derfor må nedetid også forstås i lys av menneskers interaksjon med teknologi, hvor nedetid kan være en konsekvens av menneskelige feil.

Mennesker – en sårbarhet, fare og trussel?

Innenfor sikkerhetsfagfeltet har menneskelige feil blitt problematisert av en rekke anerkjente teoretikere (Perrow, 1994; Reason, 1997), og ulykker kan ofte ikke isoleres fra menneskelig atferd. I NAT, HRT og IRGC-rammeverket er mennesket en viktig komponent, og som en av

informantene presiserte kommer man ikke bort fra menneskelig aktivitet. I dette studiet blir mennesket betraktet som en kilde til feil, en sårbarhet, en fare og som en potensiell trusselaktør. Mennesker har dermed en avgjørende rolle i finanssektoren. Det er mennesker som interagerer med teknologi og cyber-domenet. Som kapittel 5.2 trakk frem, kan mennesket gjennom uintendert handling forårsake store uønskede hendelser, samtidig som de selv kan bli offer for bedrageri og svindel.

Delkonklusjon

Teori bidrar til å belyse hvordan farer har en sentral påvirkning på cyber-risikoen i finanssektoren. Farer og trusler vil alltid ha potensiale til å påvirke risiko, selv om fokuset ofte legges på trusler heller enn farer. Til tross for at forståelsen for hvilken risiko farer kan representere er varierende, er det godt belegg for å påstå at farene som har blitt identifisert i dette studiet kan ha en negativ effekt på cyber-risikoen i finanssektoren. Dersom risikokommunikasjonen er utydelig angående hvilken risiko farer utgjør, slik som det virker som i dag, kan det i verste fall føre til uønskede hendelser. Både tidligere forskning og teori belyser at mennesket påvirker risiko og at mennesker kan betraktes som en sårbarhet, en trussel og en fare. I dette studiet blir menneskelig handling sett i lys av lureri og svindel, og det er utvilsomt at menneskene som interagerer med teknologi i finanssektoren kan spille en avgjørende rolle for systemets grad av funksjon. Selv om finanssektoren er digitalisert, er den avhengig av menneskelig aktivitet for å opprettholdes. Teorien utdyper at feil og ulykker ikke kan reduseres til et enkelt menneske, men heller må ses på som organisatoriske svakheter. Neste seksjon vil inkludere dette drøftingspunktet, i lys av organisatoriske endringer.

6.3 Hvordan har risikostyring endret seg for cyber-risiko?

Risikostyring forklares av Aven (2015) som den målrettede aktiviteten en virksomhet legger ned for å styre risiko. En del av risikostyringsprosessen inkluderer at man bestemmer hvilke risikoer som er akseptable og hvilke som ikke er det (Aven et al., 2017). Den endringen som finanssektoren har opplevd i forhold til cyber-trusler og cyber-farer, viser at det har vært forandring i hvordan cyber-risiko styres og håndteres. Eksempelvis har det blitt innført flere tiltak for å minske risikoen. Informanter forklarer utviklingen av cyber-trusler og cyber-risiko som årsaken til at styringen har måttet endre seg.

Utvikling og endring i risikostyringsprosessen

IRGC-rammeverkets ulike steg (se figur 3: IRGC-modellen) kan øke forståelsen for hvordan tilnærmingen til risikostyring og cybersikkerhet har endret seg i finanssektoren (IRGC, 2017). Gjennom en kontinuerlig prosess, som skissert av Renn (2008), har finanssektoren sett behovet for å endre tilnærmingen til cybersikkerhet. Den tradisjonelle tilnærmingen til farer og trusler omfavner ikke hvordan cyber-risiko utartes (Myles et al., 2015). Det faktum at risikostyringsprosessen har blitt utvidet fra kun å omfatte avdekking og respons, til også å omfavne identifikasjon, beskyttelse, avdekking og tilbakestilling, kan tolkes som bevis på store endringer bare de siste 10 årene.

Dernest trekker IRGC-rammeverket frem at risikostyring er en inkluderende prosess der man både skaper forståelse for risiko og fatter styringstiltak for å hanskes med risikoen (Renn, 2008; SRA, 2018). Det oppfordres videre til at risikostyring er en prosess som må forstås gjennom fire hovedsteg. Disse stegene kan relateres til endringene som har skjedd i finanssektorens styring av cyber-risiko de siste 10 årene. Utviklingen av cyber-domenets betydning i finanssektoren har ført til at man har samlet inn og utviklet kunnskap knyttet til cyber-risikoen. Armour (2016) påstår at det er kritisk at organisasjoner tilpasser seg et miljø som er i konstant forandring, og kun gjennom dynamisk læring og forbedring kan cyber-risiko styres. En av hovedutfordringene for risikostyring hevdes å være nettopp det å samle inn og utvikle kunnskap om risikoforhold (Renn, 2008). Det kan ytterligere problematiseres gjennom de ulike forståelsene for hva som er en risiko, en trussel og en fare. Som det fremgår av empirien er det sprikende forståelser for begreper blant informanter og dokumenter. For å kunne styre sikkerhet på en helhetlig måte, hevder Dahl (2000) at det er avgjørende at man har en felles forståelse av risiko. Det betyr at ulik forståelse og mangelfull kunnskap kan påvirke risikostyringsprosessen negativt. Styringsprosessen kan bli negativt påvirket ettersom misforståelser og enighet kan oppstå når det ikke eksisterer en konvergent forståelse eller tilnærming til risikoen som skal styres. Armour (2016) trekker også frem at ledelse og konsernstyre må forstå og akseptere risiko, hvilket fordrer at risikoforståelsen er lik.

Organisatorisk samarbeid påvirker cybersikkerhet

Det er utfordringer knyttet til iverksettelse av tiltak som reduserer, kontrollerer og styrer risiko. Gjennom organisatoriske endringer og erkjennelse av risiko gjennom å samle inn og å utvikle kunnskap, har finanssektoren iverksatt flere tiltak for styre å cyber-risiko. Tiltakene

som nevnes i empirien er både for virksomheter i finanssektoren, men også for finanssektoren som helhet. IKT-forskriften, NIS-direktivet og den nye sikkerhetsloven har alle flere fellesnevnere, hvor en er at de foreslår spesifikke tiltak for å kontrollere risiko slik at man har et akseptabelt sikkerhetsnivå. Videre er opprettelsen av Nordic Financial CERT i 2014 et tiltak for å detektere, forebygge og håndtere cyber-trusler, som i sin tur påvirker cyber-risikoen. Samarbeidskulturen som belyses i empirien, bidrar til at virksomheter er mer informert i forhold til risiko og sårbarheter. IRGC (2017) trekker frem at gjennom samarbeid og videreutvikling av cybersikkerhet vil organisasjoner fortsette å dra nytte av teknologien samtidig som de opererer i et trygt (safety) og sikkert (security) miljø.

Virksomhetene i finanssektoren har valgt å samarbeide heller enn å konkurrere i møte med utfordringene knyttet til cybersikkerhet. På den måten kan synergieffektene på tvers av virksomhetene bli utnyttet, særlig i lys av informasjonsdeling og utarbeidelse av gode praksiser for håndtering. Man kan hevde at et slikt samarbeid bidrar til å skape en åpen og kunnskapsbasert kultur. Det gjør at sektoren bærer preg av Reason (1997) sin konseptualisering av en informert kultur. Finanssektoren har en rapporterende kultur i lys av den pliktede rapporteringen til finanstilsynet. I tillegg kan man betrakte kulturen som lærende ettersom utviklingen av trusler og farer fordrer at forsvarsverk blir oppdatert som følge av økt kompetanse og kunnskap – som i sin tur fører til læring. Den fleksible kulturen muliggjør endringer slik at organisasjoner er resiliente i møte med cyber-domenet (Weick & Sutcliffe, 2007). Endringene finanssektoren har gjennomgått ved å formalisere samarbeidet og øke ressurser som brukes på å håndtere cyber-hendelser vitner om at finanssektoren tilpasser seg og forsøker å være fleksibel i møte med et dynamisk risikobilde. Dette støttes opp av Antonacci (2018) som oppfordrer til samarbeid på tvers av landegrenser for å møte og håndtere cyber-trusler.

Styring av cyber-risiko som en modningsprosess

Renn (2008) hevder at risiko må kommuniseres tydelig, involvere flere interessenter og inkludere kontekst i risikovurderinger. I empirien nevnes det at man kan se dette som en modningsprosess, hvor finanssektoren år for år har modnet sin tilnærming. Gjennom denne modningen har organisasjoner forsøkt å tilpasse seg et klima som er i konstant utvikling (Armour, 2017). Rosness et al. (2004) hevder at organisatorisk redundans består av både en strukturell og en kulturell dimensjon. Dette er også i samsvar med sektorens tilnærming til styring av risiko, noe som også reflekteres i modningsprosessen sektoren har gjennomgått det

siste tiåret. Formaliseringen av samarbeidet og et utstrakt samarbeid gjennom EØS-regulering og ny nasjonal strategi er viktige tiltak for å hanskes utfordringene.

Modningen speiles ved at cyber-risiko på et nasjonalt nivå har mottatt mer oppmerksomhet og risikoen knyttet til cyber har blitt tydeligere kommunisert. Gjennom å involvere flere interessenter som NSM og PST i ROS-analyser knyttet til finanssektoren styrkes forståelsen av risiko. Ettersom finanssektoren er en av Norges kritiske samfunnsfunksjoner samt avhengig av annen kritisk infrastruktur, er det avgjørende at de risikoer som truer funksjonaliteten blir tatt på alvor. Myles et al. (2015) påstår at et cyberangrep mot kritisk infrastruktur har kapasiteten til å forstyrre et helt land. Med bakgrunn i denne kunnskapen kreves det både regulatoriske og organisatoriske tiltak for å forhindre angrep på kritisk infrastruktur påvirker samfunnskritiske funksjoner. Det bidrar til å forklare årsaken for at nasjonale risikoer knyttet til cyber, og særlig cyber-trusler, må inkluderes når finanssektoren kartlegger risikolandskapet gjennom ROS-analyser. Renn (2008) trekker inn hvordan såkalte «cross-cutting aspects» har stor innflytelse på risikostyringsprosessen, og at man gjennom kommunikasjon, involvering av interessenter og inkludering av den sosiale kontekst for risiko, er et viktig steg. Inklusjon av eksperter bidrar til å øke kunnskap hos ledere, noe som i sin tur fører til at ledere har tilstrekkelig kunnskap om cyber-risikoer for å best mulig styre dem (Armour, 2017).

Risikostyring for cyber-risiko har i løpet av det siste tiåret gått fra å være et tema som fikk tildelt ressurser, dog uten at det eksisterte særlig bevissthet knyttet til tematikken, til å bli en av finanssektorens største bekymringer. Informantene belyste at sikkerhet angår alle i en organisasjon. Dette er også i tråd med Myles et al. (2015) som fremhever at cyber-risiko ikke er et IKT-problem, men et styringsproblem. Risikoen krever at ledelsen og styret i en virksomhet er aktivt engasjert i hvordan dette skal håndteres. Funn fra empirien demonstrerer også at lederskap er en viktig faktor for at risikoen blir tatt på alvor, og at cybersikkerhet har blitt løftet opp til å være av relevans på organisasjoners styrenivå. Armour (2016) skriver at ledere selv må sørge for å ha tilstrekkelig informasjon om cyber-risiko for at organisasjoner skal være motstandsdyktige. Ved å heve sikkerhet og sørge for at ledere er informerte om risikobildet, er virksomhetene i bedre stand til å stå imot og håndtere trusler og farer dersom de materialiseres.

Delkonklusjon

Virksomhetene i finanssektoren har blitt mer motstandsdyktige gjennom fokus på organisatorisk resiliens og -robusthet, og dette bidrar til bedre håndtering cyber-hendelser. Organisatorisk resiliens og -robusthet har blitt ytterligere styrket av samarbeidet på tvers av sektoren. Modningsprosessen i sektoren kan hevdes å være tydelig da funn viser at det ikke har forekommet alvorlige hendelser som påvirker sektorens tilgjengelighet, konfidensialitet eller integritet det siste tiåret. Det har vært forekommet sikkerhetshendelser av mindre omfang og ingen som klassifiseres som alvorlige.

At finanssektoren har modnet sin tilnærming til sikkerhet, og følgende endringer for styring, tyder på at kunnskap og forståelse har økt i sektoren det siste tiåret. Dette kan ikke separeres fra de nasjonale trendene og den økte bevisstheten i samfunnet angående potensielle risikoer knyttet til cyber-domenet. Som en nødvendighet har risikostyringen endret seg slik at finanssektoren skal være i stand til å sikre sine verdier. Dersom ledelse og organisasjoner ikke hadde sett behovet for å endre sine tiltak og prosedyrer i forbindelse med digitalisering ville de trolig, som belyst av informantene, mistet både tillit, troverdighet og konsesjonsrett til å drive sin virksomhet. Likevel må det påpekes at funn i denne studien viser at det ikke bare er det siste tiåret tilnærming til styring har endret seg. Behovet for endring har eksistert helt siden starten av digitaliseringsprosessen som respons på det endrede trussel- og risikobildet.

7. Konklusjon

Dette kapittelet avslutter denne avhandlingen. Kapittelet vil bidra til å besvare problemstillingen som har drevet frem avhandlingen. Problemstillingen som besvares er følgende:

Hvorfor har cyber-risiko i finanssektoren utviklet seg de siste 10 årene?

Oppgavens problemstilling gir rom for flere svar, og det er helt tydelig et sammensatt årsaksbilde. Forklaringen på utviklingen av cyber-risiko i finanssektoren må ses i sammenheng med en rekke faktorer og årsaker. Dernest er det viktig å trekke frem at selv om særlig cyber-trusselen har økt, har det også ført til bevissthet og risikoreduserende tiltak. Cyber-truslene som har blitt nevnt gjennom denne oppgaven pekes ut som en viktig årsak for hvorfor cyber-risikoen har utviklet seg det siste tiåret. Videre har faren knyttet til nedetid en betydelig effekt på cyber-risikoen i sektoren. Det er kartlagt flere årsaker for cyber-risikoens utvikling gjennom denne studien, følgende ansees å være av særlig relevans:

- Cyber-risiko har utviklet seg som følge av et finanssystem som er digitalisert. Digitaliseringen har ført til at flere av finanssystemets verdier er tilgjengelige gjennom cyber-domenet.
- Det må understrekes at cyber-risiko har fått fart og retning også av utviklingstrekk på nasjonalt nivå, eksempelvis gjennom tilstrømningen av ny teknologi, innovasjon og konkurranse.
- Kompleksitet i finanssystemets infrastruktur, systemer og organisasjoner bidrar til å øke cyber-risiko ved å skape avhengigheter til og imellom infrastrukturer og systemer som i sin tur skaper lange og komplekse verdikjeder.
- Konsekvensene og alvorlighetsgraden av en uønsket hendelse, tilsiktet eller ikke-tilsiktet, har økt. Det fører til at cyber-trusler og cyber-farer representerer en større total cyber-risiko. Dette er særlig aktuelt dersom man betrakter risiko i lys av tre-faktormodellen (trussel, verdi og sårbarhet).
- Cyber-truslene påvirker cyber-risikoen negativt gjennom de identifiserte utviklingstrekkene, det er følgende: profesjonalisering av trussel-aktører, mer avanserte og komplekse angrepsmetoder, et mer uoversiktlig aktørbilde, økte kapabiliteter og økte ressurser.

- Fremmede stater og organiserte kriminelle utgjør en betydelig større trussel i 2019 enn i 2009. Disse trusselaktørene er de aktørene som truer sektoren mest.
- Sårbarhetene er dynamiske og må ses i sammenheng med utviklingen i trussel- og risikobildet. Derimot viser funn at det er færre sårbarheter i teknologien som benyttes i det finansielle systemet i dag enn tidligere, hvilket har en positiv effekt på cyber-risikoen.
- Utkontraktering er en årsak som må inkluderes i utviklingen av cyber-risiko. Det har på en side bidratt til å skape risiko gjennom økt konsentrasjonsrisiko, mens det på den andre siden har hatt en positiv effekt i forhold til økt kompetanse og håndtering av risiko.
- Gjennom regulering og rapportering har virksomheter i finanssektoren blitt «tvunget» til å ta stilling til cyber-risiko, samt gjøre tiltak og redusere uakseptabel risiko. Det har ført til en god sikkerhetskultur knyttet til cyber, hvor særlig rapportering og læring har vært sentrale komponenter.
- Tilnærmingen til cyber-risiko har endret seg vesentlig, og håndteres mer profesjonelt av finanssektoren i 2019 enn i 2009. Det begrunnes i erkjennelsen av risikoen og økt fokus på cybersikkerhet. Endring i bevissthet har i sin tur ført til stadig mer omfattende tiltak og økt forsvarsevne.
- Økt fokus på cybersikkerhet har en positiv effekt på cyber-risiko da finanssektoren inkluderer både tilsiktede (trusler) og ikke-tilsiktede (farer) hendelser som sine topp-risikoer. Dette har ført til en endring i tilnærmingen til styring. Styringsmetodikken har utviklet seg fra «forhindre, håndter»» til «forutse, forhindre, håndter, gjenopprett».
- Synergieffektene av samarbeid og informasjonsdeling synes å være svært viktig når man undersøker hvorfor cyber-risiko har utviklet seg. Videreføring og formalisering av samarbeidskulturen i finanssektoren har hatt en positiv effekt på cyber-risiko i finanssektoren.

Med formålet å undersøke hvorfor cyber-risiko har utviklet seg, kan funn i denne studien peke mot en negativ utvikling for risikoen gjennom økte trusler, dynamiske sårbarheter og at flere verdier flyttes over på cyberdomenet. Likevel er dette en svært forenklet forklaring da de negative utviklingstrendene ikke kan sees isolert fra finanssektorens innsats for å forebygge og håndtere risiko.

Finanssektoren i Norge er en moden sektor når det kommer til å ivareta cybersikkerhet og sine (digitale) verdier. Utfordringene er flere og finanssektoren har selv tatt en rekke viktige initiativ for å hanskes med dem. Videre har det de siste par årene ikke vært noen alvorlige hendelser i finanssektoren i form av cyber-hendelser, selv om aktiviteten på cyberdomenet har økt. Det tyder på at finanssektoren har hatt en positiv utvikling i sin cyber-risiko, til tross for at trussel, verdi og konsekvens har økt. Utfordringen knyttes til at dersom det først skjer en større uønsket hendelse, tross lav sannsynlighet, kan konsekvensene være katastrofale.

7.1 Forslag til videre forskning

Denne avhandlingen har belyst noen utfordringer knyttet til tematikken, med særlig fokus på bank- og finansområdet. I en forlengelse av studiet oppfordres det til at myndighetene gjennomfører en større studie knyttet til digitaliseringen av samfunnet. Cyber-domenet påvirker nærmest alle grunnleggende nasjonale funksjoner, og det er manglende kartlegging av hvilke konsekvenser frafall av cyber-domenet kan gi for samfunnet forøvrig. Det er et behov for å kartlegge hvordan samfunnet kan skape og opprettholde robusthet i møte med teknologiske fremskritt og innovasjoner. Digitalisering og teknologisk utvikling gjennomsyrer vårt samfunn og skjer med enorm hastighet, og i et sikkerhetsfaglig perspektiv er det essensielt å etterstrebe forståelse både for fordelene og ulempene dette medfører.

8. Litteraturliste

Al Jezeera. (2018, 24. Mai). Hacked: The Bangladesh Bank Heist. Hentet fra https://www.aljazeera.com/programmes/101east/2018/05/hacked-bangladesh-bank-heist-180523070038069.html

Andersen, S. S. (2006). Aktiv informantintervjuing. *Norsk statsvitenskapelig tidsskrift, 22*, 278-298

Antonacci, P. (2018). The cyberthreat facing the financial services industry. *Cyber Security, 2*(2), 106-113.

Aven, T. (2015). *Risikostyring. Grunnleggende prinsipper og ideer* (2.utg). Oslo: Universitetsforlaget.

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

Aven, T., & Krohn, B.S. (2013). A new Perspective on how to understand, assess and manage risk and the unforseen. *Reliability Enginerring and system Safety, 121*, 1-10.

Aven, T., Røed, W., & Wiencke, H.S. (2017). *Risikoanalyse* (2.utg). Oslo: Universitetsforlaget.

BankAxept. (2019). «Om oss». Hentet fra: https://bankaxept.no/om-oss/

Berger, P.L & Luckmann, T. (2000). Den samfunnsskapte virkelighet. Oslo: Fagbokforlaget.

Berry, A., Homan, J., & Eitzman, R. (2017). WannaCry Maleware Profile. Hentet fra https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html

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

Bits. (2019). «Om bits». Hentet fra: https://www.bits.no/om-bits/

Boholm, M., Möller, N., & Hansson, S.E. (2016). The concept of risk, safety and security: applications in everyday langauge. *Risk Analysis. 36*(2), 320-338. DOI: 10.1111/risa.12464

Bouveret, A. (2018). IMF working paper: Cyber Risk for the Financial Sector: A framework for Quantitative assessment. Hentet fra: https://www.imf.org/en/search#q=Cyber%20Risk%20for%20the%20Financial%20Sector%3A%20A%20Framework%20for%20Quantitative%20Assessment%2C%20WP%2F18%2F143%2C%20July%202018%20&sort=relevancy

Blaikie, N. (2010). *Designing social research: The logic of anticipation* (2. Utg). Cambridge: Polity Press.

Busmundurd, O., Maal, M., Kiran, J.H., & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. (FFI rapport 00923/ 2015). Hentet fra https://www.ffi.no/no/Rapporter/15-00923.pdf

Brewster, T. (2017, 28. Juni). 3 things you dan do to stop 'NotPetya' Ransomeware wrecking your PC. *Forbes.* Hentet fra https://www.forbes.com/sites/thomasbrewster/2017/06/28/three-things-you-can-do-to-stop-notpetya-ransomware-wrecking-your-pc/#5066ab9177b0

Cebula, J.J., & Young, L.R. (2010). A taconomy of Operational Cyber Secutiry Risks (Technical Note CMU/SEI-2010-TN-029). *Software Engeenering Institute*.Varnegie Mellon Unviersity. Hentet fra: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.204.4058&rep=rep1&type=pdf

Christensen, J. (2019, 20. Mars). Så mye har andre cyberangrep kostet. *Dagens næringsliv.* Hentet fra https://www.dn.no/industri/morten-landro/aon/hydro/sa-mye-har-andre-cyberangrep-kostet/2-1-569510

Deloitte. (2018). Ny sikkerhetslov og NIS-direktivet. Hentet fra: https://www2.deloitte.com/no/no/pages/legal/articles/sikkerhetslov-januar-2019.html

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

Departementene. (2012). *Nasjonal strategi for informasjonssikkerhet*. Hentet fra https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

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

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

Engen, O.A. (2002). Rethoric and Realities: *The NORSOK programme and Technical and Organisational Change in the Norwegian Petroleum Industrial Complex*. (Doktoravhandling). Universitetet i Bergen, Bergen.

Engen, O. A. H., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E. & Pettersen, K. A. (2016). *Perspektiver på samfunnssikkerhet*. Oslo: Cappelen Damm Akademisk.

Eling, M, & Wirfs, J.H. (2016). «Cyber Risk: too Big to Insure? Risk Transfer Options for a Mercurial Risk Class». *Institute of Insurance Economics*, University of St. Gallen. Hentet fra https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf

Etterretningstjenesten. (2011). *Fokus 2011*. Hentet fra: https://forsvaret.no/fakta_/ForsvaretDocuments/FOKUS-2011.pdf

Etterretningstjenesten. (2018). *Fokus 2018*. Hentet fra:

https://forsvaret.no/fakta_/ForsvaretDocuments/fokus2019_web.pdf

Evry. (2018). «DNB forlenger avtale med EVRY». Hentet fra:

https://www.evry.com/no/media/artikler/dnb-forlenger-avtale-med-evry/

Finanstilsynet. (2009). Risiko- og sårbarhetsanalyse (ROS) 2008. Hentet fra

https://www.finanstilsynet.no/contentassets/3c6c6351c2d34d66a71c15fab2ea2ef2/ros-analyse-2008.pdf

Finanstilsynet. (2010). Risiko- og sårbarhetsanalyse (ROS) 2009. Hentet fra

https://www.finanstilsynet.no/contentassets/aca94b50517845fbbb8bb8987d31f7ee/ros-analyse-2009.pdf.pdf

Finanstilsynet. (2011). Risiko- og sårbarhetsanalyse (ROS) 2010. Hentet fra

https://www.finanstilsynet.no/contentassets/9d595e9bd079449bb34b91b5e7f9d6e1/ros_analyse_2010.pdf

Finanstilsynet. (2012). Risiko- og sårbarhetsanalyse (ROS) 2011. Hentet fra

https://www.finanstilsynet.no/contentassets/98f605c0caec4b048009cf6568ea10df/ros-analyse_2011.pdf

Finanstilsynet. (2013). Risiko- og sårbarhetsanalyse (ROS) 2012. Hentet fra

https://www.finanstilsynet.no/contentassets/3d535fe2ebd3448e8918a7cb1fb2954f/ros_analyse_2012.pdf

Finanstilsynet. (2014). Risiko- og sårbarhetsanalyse (ROS) 2013. Hentet fra

https://www.finanstilsynet.no/contentassets/8f1b3764099e494197de0f9a2f19c1c7/ros-analyse_2013.pdf

Finanstilsynet. (2015). Risiko- og sårbarhetsanalyse (ROS) 2014. Hentet fra

https://www.finanstilsynet.no/contentassets/2d10ae0298b94dee888d47148280cfca/ros_analyse_2014.pdf

Finanstilsynet. (2016). Risiko- og sårbarhetsanalyse (ROS) 2015. Hentet fra

https://www.finanstilsynet.no/contentassets/c14bf3f349d24321b5096f5a8161ea7b/risiko_og_sarbarhetsanalysen_2015.pdf

Finanstilsynet. (2017). Risiko- og sårbarhetsanalyse (ROS) 2016. Hentet fra

https://www.finanstilsynet.no/contentassets/63187295c2b345f895523e54ee408783/risiko-og-sarbarhetsanalyse-2016.pdf

Finanstilsynet. (2017b). Tilsyn med IT og betalingstjenester. Hentet fra:

https://www.finanstilsynet.no/tema/tilsyn-med-it-og-betalingstjenester/

Finanstilsynet. (2018). Risiko- og sårbarhetsanalyse (ROS) 2017. Hentet fra

https://www.finanstilsynet.no/contentassets/b9cb0cab82304c4498a1562a002bafce/risiko--og-sarbarhetsanalyse-2017.pdf

Finanstilsynet. (2019). Risiko- og sårbarhetsanalyse (ROS) 2018. Hentet fra

https://www.finanstilsynet.no/contentassets/a92eb0d064a94bcfa0b8d862936af02e/risiko--og-sarbarhetsanalyse-2018.pdf

Friedman, S., (2016). Taking cyber risk management to the next level - lessons learned from the front lines at Financial institutions. *Deloitte insights*, Juni. Hentet fra: https://www2.deloitte.com/tr/en/pages/risk/articles/cyber-risk-management-financial-services-industry.html

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

International Organization for Standardization (ISO) and International Electrotechnical Comisson (IEC). (2018). 27005. Information technology, security techniques, information security risk management

International Risk Governance Council. (2017). IRGC Risk Governance Framework. Hentet fra: https://irgc.org/risk-governance/irgc-risk-governance-framework/

Johannesen, A., Christoffersen, L., & Tufte, P. A. (2011). *Forskningsmetode for økonomiskadministrative fag* (3.Utg). Oslo: Abstrakt forlag.

Justis- og beredskapsdepartementet. (2016). NIS-direktivet. (EØS-notat, 16.12.2016). Hentet fra https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/

Justis- og beredskapsdepartementet. (2017). *IKT-sikkerhet – Et felles ansvar*. (Meld.St.38, 2016-2017). Hentet fra https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/

Halsør, M., Skille, Ø.B., Olsson, S.V., Vartdal, Å., & Døvik, O. (2019). Granskere: Kina hacka norsk selskap (NRK, 06.02.2019). Hentet fra: https://www.nrk.no/urix/granskarar_-kina-hacka-norsk-selskap-1.14418026

Hannemyr, G. (2015). *Digitale medier: teknologi, anmeldelser & samfunn* (3. Utg). Oslo: Universitetsforlaget

Harford, T. (2011). What we can learn from a nuclear reactor? *Financial Times*. Hentet fra: https://www.ft.com/content/cea7b256-1def-11e0-badd-00144feab49a

Havnes, H. (2014, 08. Juli). Norgs Bank Angrepet. *Dagens Næringsliv.* Hentet fra: https://www.dn.no/norges-bank/kriminalitet/norges-bank-angrepet/1-1-5146381

Kitten, T. (2016, 25.April). Bangladesh Bank Heist: Lesson learned. *Bank Info Security.* Hentet fra https://www.bankinfosecurity.com/bangladesh-bank-heist-lessons-learned-a-9064

Hollnagl, E., Woods, D.D., & Levenson, N. (2006). Resilience Engineering. Concept and percepts. London: Ashgate.

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *Cyber risk, market failures, and financial stability.* (IMF working paper 185/ 2017). Hentet fra https://www.cybersecitalia.it/wp-content/uploads/2017/10/wp17185.pdf

Hydro. (2019). Oppdatering på cyberangrepet 12. April. Hentet fra: https://www.hydro.com/no-NO/media/news/2019/oppdatering-pa-cyberangrepet-12.-april/

Langø, H.-I., & Sandvik, K. B. (2013). Cyberspace og sikkerhet. *Internasjonal politikk*, ss. 221-228.

La Porte, T., Consolini P.M. (1991). Working in Practice Byt Not in Theory: Theoretical Challenges of «High Reliability Organizations». *Journal of Puclic Administration Research and Theory, 1*(1), 19-47

Myles, D., Lee, A., Thomas, Z., & Meager, L. (2015). Cyber-attacks: financial stability's newest threat. *International Financial Law Review, 10*(12). Hentet fra http://web.a.ebscohost.com.ezproxy.uis.no/ehost/detail/detail?vid=4&sid=c8d2a340-1d4b-4c5a-852e-5e86b91e8e27%40sdc-v-sessmgr02&bdata=JnNjb3BlPXNpdGU%3d#AN=110282562&db=bth

Nasjonal Sikkerhetsmyndighet. (2009). *Cybersikkerhet* (Årsmelding 2009). Hentet fra https://www.nsm.stat.no/globalassets/rapporter/arsrapporter/nsm-arsmelding-2009.pdf

Nasjonal Sikkerhetsmyndighet. (2010). *Sikkerhetskultur* (Årsmelding 2010). Hentet fra https://www.nsm.stat.no/globalassets/rapporter/arsrapporter/arsmelding-nsm-2010web.pdf

Nasjonal Sikkerhetsmyndighet. (2011). *Grunnsikring* (Årsmelding 2011). Hentet fra https://www.nsm.stat.no/globalassets/rapporter/arsrapporter/arsmelding_nsm_2011_video.pdf

Nasjonal Sikkerhetsmyndighet. (2012). *Nye utfordringer, større ambisjoner* (Årsmelding 2012). Hentet fra https://www.nsm.stat.no/globalassets/rapporter/arsrapporter/arsmelding_nsm_2011_video.pdf

Nasjonal Sikkerhetsmyndighet. (2013). *Nasjonal sikkerhetsmyndighet er Norges ekspertorgan for informasjons- og objektsikkerhet* (Årsrapport 2013). Hentet fra https://www.nsm.stat.no/globalassets/rapporter/arsrapporter/nsm-arsrapport-2013.pdf

Nasjonal Sikkerhetsmyndighet. (2014). *Årsrapport 2014 – Økt risiko – styrket beredskap*. Hentet fra https://www.nsm.stat.no/globalassets/rapporter/arsrapporter/nsm-arsrapport-2014.pdf

Nasjonal Sikkerhetsmyndighet. (2015). *Helhetlig IKT-risikobilde 2015.* Hentet fra https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf

Nasjonal Sikkerhetsmyndighet. (2016). *Helhetlig IKT-risikobilde 2016.* Hentet fra https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2016_web_enkel.pdf

Nasjonal Sikkerhetsmyndighet. (2017). *Helhetlig IKT-risikobilde 2017.* Hentet fra https://www.nsm.stat.no/globalassets/rapporter/helhetlig_ikt-risikobilde_2017_orig_enkeltsider_low.pdf

Nasjonal Sikkerhetsmyndighet. (2018a). *Risiko 2018: Verdifulle individer, verdifull infrastruktur, verdifulle virksomheter*. Hentet fra: https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf

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

Norges Bank. (2009a). *Finansiell stabilitet*. Hentet fra: https://static.norges-bank.no/contentassets/c8ec155e77664d5c9b90a4d1f3554bc2/finstab_2_09.pdf?v=03/09/2017123512&ft=.pdf

Norges Bank. (2010a). *Finansiell stabilitet*. Hentet fra: https://static.norges-bank.no/contentassets/41dd5224da3849b789e63decf275ed2b/finansiell_stabilitet_2_10.pdf?v=03/09/2017123145&ft=.pdf

Norges Bank. (2011a). *Finansiell stabilitet*. Hentet fra: https://static.norges-bank.no/contentassets/a172ceac26fe4fee9321bf946a377653/finstab_2-11.pdf?v=03/09/2017123505&ft=.pdf

Norges Bank. (2012a). *Finansiell stabilitet*. Hentet fra: https://static.norges-bank.no/contentassets/c3fb0df0495146ac9b3969588ce38d4e/fs_212_no.pdf?v=03/09/2017123513&ft=.pdf

Norges Bank. (2013a). *Finansiell stabilitet*. Hentet fra: https://static.norges-bank.no/contentassets/2820fd5cb02340d894a44cf8c0c49ee5/finansiell_stabilitet_rapport_2013.pdf?v=03/09/2017123459&ft=.pdf

Norges Bank. (2014a). *Finansiell stabilitet*. Hentet fra: https://static.norges-bank.no/contentassets/0834e5b22d7f4e908172d45ec3dfdd8b/finansiellstabilitet_2014_www.pdf?v=03/09/2017123536&ft=.pdf

Norges Bank. (2015a). *Finansiell stabilitet*. Hentet fra: https://static.norges-bank.no/contentassets/3d9dbb79d1a64063a0f94fef9ac58178/finansiellstabilitet_2015.pdf?v=03/09/2017123359&ft=.pdf

Norges Bank. (2016a). *Finansiell stabilitet*. Hentet fra: https://static.norges-bank.no/contentassets/ab1612d0f7aa45a8976ce687bcf25620/finansiell_stabilitet_2016.pdf?v=03/09/2017123539&ft=.pdf

Norges Bank. (2017a). *Finansiell stabilitet – sårbarhet og risiko*. Hentet fra: https://static.norges-bank.no/contentassets/f3a45cb94d334c4cb619cc549952d553/fs_rapport_2017.pdf?v=11/02/2017091701&ft=.pdf

Norges Bank. (2018a). *Finansiell stabilitet – sårbarhet og risiko*. Hentet fra: https://static.norges-bank.no/contentassets/1afe861c5f1c43afaf61fb57082e7c7a/fs2018_rapport.pdf?v=11/23/2018133919&ft=.pdf

Norges Bank. (2009b). *Årsrapport om betalingssystem 2009*. Hentet fra: https://www.norges-bank.no/globalassets/upload/publikasjoner/betalingssystem/aarsrapport_betalingssystem_2009.pdf

Norges Bank. (2010b). *Årsrapport om betalingssystem 2010*. Hentet fra: https://static.norges-bank.no/contentassets/31b4184fcea74550b9c681a47dc85a32/ars_betalingssystem_2010.pdf?v=03/09/2017123311&ft=.pdf

Norges Bank. (2011b). *Årsrapport om betalingssystem 2011*. Hentet fra: https://static.norges-bank.no/contentassets/fa04d2dd6f94487c9a563bf8f69839ac/betalingssystemet2011.pdf?v=03/09/2017123232&ft=.pdf

Norges Bank. (2012b). *Årsrapport om betalingssystem 2012*. Hentet fra: https://static.norges-bank.no/contentassets/56415e186ed442a681fd7315ad66f26e/betalingssystem_2012_o.pdf?v=03/09/2017123320&ft=.pdf

Norges Bank. (2014b). *Finansiell infrastruktur*. Hentet fra: https://static.norges-bank.no/contentassets/96010276ae49476e8405ccbf6600009b/finansiell_infrastruktur_2014_2.pdf?v=03/09/2017123527&ft=.pdf

Norges Bank. (2015b). *Finansiell infrastruktur*. Hentet fra: https://static.norges-bank.no/contentassets/93262fdabe724e6a802de39299985502/finansiell_infrastruktur_2015.pdf?v=03/09/2017123202&ft=.pdf

Norges Bank. (2016b). *Finansiell infrastruktur*. Hentet fra: https://static.norges-bank.no/contentassets/316597d288d24ec8b23a8befaf1567c1/finansiell_infrastruktur_2016.pdf?v=03/09/2017123443&ft=.pdf

Norges Bank. (2017b). *Finansiell infrastruktur*. Hentet fra: https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Finansiell-infrastruktur---rapport/finansiell-infrastruktur-2017/

Norges Bank. (2018b). *Finansiell infrastruktur.* Hentet fra: https://static.norges-bank.no/contentassets/234480bf59cf4c02a5b2f7b18c97008f/finansiell_infrastruktur_2018.pdf?v=05/25/2018091305&ft=.pdf

Norsk senter for Informasjonssikring. (2017). Trusler og trender 2017-18. Hentet fra https://norsis.no/wp-content/uploads/2017/12/tt17-18_web_endelig_v2.pdf

NOU 2000: 24. (2000). *Et sårbart samfunn – utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Oslo: Justis- og beredskapsdepartementet.

NOU 2006: 6. (2006). *Når sikkerhet er viktigst – Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.* Oslo: Justis- og beredskapsdepartementet.

NOU 2015: 13. (2015). *Digital sårbarhet – sikkert samfunn – beskytte enkeltmennesker og samfunn i en digitalisert verden*. Oslo: Justis- og beredskapsdepartementet.

NOU 2018: 14. (2018*). IKT-sikkerhet i alle ledd – organisering og regulering av nasjonal IKT-sikkerhet*. Oslo: Justis- og beredskapsdepartementet.

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

Paté-Cornell, E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis, 38*(2), 226-24. DOI: 10.1111/risa.12844

Perrow, C. (1984). *Normal Accidents – living with high risk technologies.* New York: Basic books

Politiets sikkerhetstjeneste. (2009). *Trusselvurdering 2009*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2009/

Politiets sikkerhetstjeneste. (2010). *Trusselvurdering 2010*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2010/

Politiets sikkerhetstjeneste. (2011). *Trusselvurdering 2011*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2011/

Politiets sikkerhetstjeneste. (2012). *Trusselvurdering 2012*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2012/

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

Politiets sikkerhetstjeneste. (2014). *Trusselvurdering 2014*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2014/

Politiets sikkerhetstjeneste. (2015). *Trusselvurdering 2015*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2015/

Politiets sikkerhetstjeneste. (2016). *Trusselvurdering 2016*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2016/

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

Politiets sikkerhetstjeneste. (2018). *Trusselvurdering 2018*. Hentet fra: https://www.pst.no/trusselvurdering-2018/

Politiets sikkerhetstjeneste. (2019). *Trusselvurdering 2019*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2019/

PWC. (2018a). *Cybercrime Survey 2018*. Hentet fra https://www.pwc.no/no/publikasjoner/cybercrime-survey.html

PWC. (2018b*). The Anxious Optimist in the Corner Office* (Global CEO-survey 2018). Hentet fra https://www.pwc.no/no/publikasjoner/pwc-global-ceo-survey-2018.pdf

Reason, J. (1997). *Managing the risks of organizational accidents*. London: Ashgate

Regjeringen. (2019). Revidert betalingstjenestedirektiv – PSD2. (Direktiv 2015/2366, PSD2). Hentet fra https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2013/okt/revidert-betalingstjenestedirektiv---psd-2.-/id2434721/

Renn, O. (2008). *Risk Governance – coping with Uncertainty in a Complex World*. London: Taylor & Francis LTD

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R.K., & Herrera, I.A. (2004). *Organisational Accidents and Resilient Organisations: Five Perspectives*. Trondheim: SINTEF

Schwarts, M.J. (2018, 16. Januar). NotPetya: From Russian Intelligence, With Love. *Bank Info Security.* Hentet fra https://www.bankinfosecurity.com/notpetya-from-russian-intelligence-love-a-10589

Sikkerhetsloven. (2019). Lov om nasjonal sikkerhet (LOV-2018-06-01-24). Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-01-24#KAPITTEL_1

Skuterud, E. (2003). *Sikring av forretningskritiske systemer*. Hentet fra https://www.magma.no/sikring-av-forretningskritiske-systemer

Solhaug, B. (2014, Juni). *Hva er cyberrisiko?* Innlegg presentert ved Seminar om cyberrisiko, Sintef. Hentet fra http://heim.ifi.uio.no/~ketils/kst/Seminars/20140618-CyberriskHvaSlagsRiskErDetOgHvaErKonsekvenseneForAnalyseOgTesting/Foredrag/140618_solhaug.pdf

Society of Risk Analysis. (2018). Society for Risk Analysis glossary. Hentet fra https://sra.org/sites/default/files/pdf/SRA%20Glossary%20-%20FINAL.pdf

Statista. (2019). Global digital population as of January 2019. Hentet fra: https://www.statista.com/statistics/617136/digital-population-worldwide/

Standard Norge, NS 5814. (2008). Krav til risikovurderinger.

Standard Norge, NS 5830. (2012). Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – terminologi.

Standard Norge, NS 5832. (2014). Samfunnsikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse.

Starner, T. (2015). Cyber Risk Models Remain Elusive. [Forsidebilde]. Hentet fra https://riskandinsurance.com/cyber-risk-models-remain-elusive/

Sutcliffe, K.M & Vogus, T.J. (2007, Oktober). *Organizational Resilience: Towards a theory and research agenda*. Innlegg presentert på IEEE International Conference on Systems, Man and Cybernetics. Hentet fra https://www.researchgate.net/publication/220756654_Organizational_Resilience_Towards_a_Theory_and_Research_Agenda

Tjora, A. (2012). Kvalitative forskningsmetoder i praksis. Oslo: Gyldendal.

Vipps. (2019). «Om oss». Hentet fra https://www.vipps.no/om-oss

Weick, K., & Sutcliffe, K. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty.* California: Jossey Bass

Wernersen, C. % Omland, E. (2017, 13. Mai). NSM – Største dataangrepet verden har sett. *NRK.* Hentet fra https://www.nrk.no/norge/nsm_-_-storste-dataangrepet-verden-har-sett-1.13515221

World Economic Forum. (2015). *The global Competitiveness Report 2015-2016*. Hentet fra: http://www3.weforum.org/docs/gcr/2015-2016/Global_Competitiveness_Report_2015-2016.pdf

Øyvann, S. (2017, 8. November). Tapte nær 2,5 milliarder på cyberangrep. *Computerworld.* Hentet fra http://www.cw.no/artikkel/datasikkerhet/tapte-naer-25-milliarder-pa-cyberangrep

Vedlegg

Vedlegg 1: Dokumenter

Utgivelsesår	Utgiver	Tittel
2018	Etterretningstjenesten	Fokus 2018
2011	Etterretningstjenesten	Fokus 2011
2009	Nasjonal sikkerhetsmyndighet	Cybersikkerhet - Årsmelding 2009
2010	Nasjonal sikkerhetsmyndighet	Sikkerhetskultur - Årsmelding 2010
2011	Nasjonal sikkerhetsmyndighet	Grunnsikring - Årsmelding 2011
2012	Nasjonal sikkerhetsmyndighet	Nye utfordringer – større ambisjoner - Årsmelding 2012
2013	Nasjonal sikkerhetsmyndighet	Nasjonal sikkerhetsmyndighet er Norges ekspertorgan på informasjons- og objektsikkerhet - Årsrapport 2013
2014	Nasjonal sikkerhetsmyndighet	Økt risiko – styrket beredskap - Årsrapport 2014
2015	Nasjonal sikkerhetsmyndighet	Helhetlig IKT-risikobilde 2015
2016	Nasjonal sikkerhetsmyndighet	Helhetlig IKT-risikobilde 2016
2017	Nasjonal sikkerhetsmyndighet	Helhetlig IKT-risikobilde 2017
2018a	Nasjonal sikkerhetsmyndighet	Et sikkert digitalt Norge – IKT-risikobilde 2018
2018b	Nasjonal sikkerhetsmyndighet	Risiko 2018: Verdifulle individer, verdifulle

Utgivelsesår	Utgiver	Tittel
		virksomheter, verdifull infrastruktur
2009	Politiets sikkerhetstjeneste	Trusselvurdering
2010	Politiets sikkerhetstjeneste	Trusselvurdering
2011	Politiets sikkerhetstjeneste	Trusselvurdering
2012	Politiets sikkerhetstjeneste	Trusselvurdering
2013	Politiets sikkerhetstjeneste	Trusselvurdering
2014	Politiets sikkerhetstjeneste	Trusselvurdering
2015	Politiets sikkerhetstjeneste	Trusselvurdering
2016	Politiets sikkerhetstjeneste	Trusselvurdering
2017	Politiets sikkerhetstjeneste	Trusselvurdering
2018	Politiets sikkerhetstjeneste	Trusselvurdering
2015	Justis- og beredskapsdepartementet	NOU 2015: 13 Digital sårbarhet – sikkert samfunn
2018	Justis- og beredskapsdepartementet	NOU 2018: 14 IKT-sikkerhet i alle ledd
2006	Justis- og beredskapsdepartementet	NOU 2006:6 Når sikkerhet er viktigst – beskyttelse av landet kritiske infrastrukturer og kritiske samfunnsfunksjoner.
2017	Justis- og beredskapsdepartementet	IKT-sikkerhet – et felles ansvar (Mld. St. 38: 2016-2017)
2019	Direktoratet for sikkerhet og beredskap	Krisescenario 2019
2009a	Norges Bank	Finansiell stabilitet
2010a	Norges Bank	Finansiell stabilitet
2013a	Norges Bank	Finansiell stabilitet
2014a	Norges Bank	Finansiell stabilitet
2015a	Norges Bank	Finansiell stabilitet
2016a	Norges Bank	Finansiell stabilitet

Utgivelsesår	Utgiver	Tittel
2017a	Norges Bank	Finansiell stabilitet – sårbarhet og risiko
2018a	Norges Bank	Finansiell stabilitet – sårbarhet og risiko
2009b	Norges Bank	Årsrapport om betalingssystem 2009
2010b	Norges Bank	Årsrapport om betalingssystem 2010
2011b	Norges Bank	Årsrapport om betalingssystem 2011
2012b	Norges Bank	Årsrapport om betalingssystem 2012
2014b	Norges Bank	Finansiell infrastruktur
2015b	Norges Bank	Finansiell infrastruktur
2016b	Norges Bank	Finansiell infrastruktur
2017b	Norges Bank	Finansiell infrastruktur
2018b	Norges Bank	Finansiell infrastruktur
2018	Næringslivets sikkerhetsråd (NSR)	Mørketallsundersøkelsen 2018
2018	Norsk senter for informasjonssikring (NorSiS)	Trusler og trender 2016-17
2019	Departementene	Nasjonal strategi for digital sikkerhet
2012	Departementene	Nasjonal strategi for informasjonssikkerhet
2009	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2008
2010	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2009
2011	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2010

Utgivelsesår	Utgiver	Tittel
2012	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2011
2013	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2012
2014	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2013
2015	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2014
2016	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2015
2017	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2016
2018	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2017
2019	Finanstilsynet	Risiko og sårbarhetsanalyse (ROS) 2018
2018	PwC	Cyber-survey 2018
2018	PwC	CEO-suervey 2018

Tabell 5: Dokumenter brukt i dokumentsudiet

Vedlegg 2: Aktører i det norske betalingssystemet

Betalingssystem	Funksjonsbeskrivelse	Systemeier	Driftsleverandør	Tilsynsmyndighet
Interbanksystem				
Norges Banks oppgjørssystem	Oppgjør med endelig virkning mellom banker, mellom banker og staten	Norges Bank	Evry ASA	Nasjonal sikkerhetsmyndighet
NICS	Bankenes felles avregningssystem for norske kroner (Bits, 2019).	Bits AS	Nets Norge Infrastruktur AS	Norges Bank
Private oppgjørsbanks-systemer	Oppgjør mellom norske bankers massebetalinger. Fører opp transaksjoner mot bankers oppgjørskontoer	DNB Bank ASA, Sparebank 1 SMN, Danske Bank, NUF,	Evry ASA	Norges Bank
System for betalingstjenester				
Nettbanksystem	Nettbaserte betalingsoverføringer og transaksjoner. Opererer ut ifra selvbetjeningsprinsipp, slik at forbruker og virksomheter minsker kostnader og effektiviserer bruk.	DNB Bank ASA, Sparebank 1 SMN, Balder Betaling AS, Sbanken ASA, Danske Bank NUF,	Evry ASA, SDC A/S (storebrand)	Finanstilsynet
BankAxept, BankID, Vipps	Betalingsløsninger mellom person, bedrift, netthandel, faktura og betaling i butikk. Utvikler og forvalter betalingsprodukter for banker	Vipps AS	Nets Norge Infrastruktur AS	Finanstilsynet

Tabell 6: Aktører i betalingssystemet.

Vedlegg 3: Informanter

Kode	Kodebeskrivelse	Erfaring
TM1	Tilsynsmyndighet informant 1	10 års erfaring med tilsyn av IKT-tjenester og IKT-system i finanssektoren.
TM2	Tilsynsmyndighet informant 2	35 års erfaring med IKT og IT-sikkerhet, herunder tilsynsvirksomhet, utredninger og implementering av forskrifter og lovverk i virksomhet
TM3	Tilsynsmyndighet informant 3	20 års erfaring med IKT og IT-sikkerhet, herunder tekniske systemer, tilkobling til nett, hendelseshåndtering, sikkerhetsarkitektur.
TM4	Tilsynsmyndighet informant 4	30 års erfaring fra finanssektoren og IT. Primært erfaring fra betalingsformidling og bank-området.
SE1	Systemeier informant 1	2 års erfaring (tekniker)Ansvarlig for cyber-security response and detect team. Arbeider med hendelseshåndtering av tilsiktede hendelser, samt strategi for å motstå angrep i en stor bank
SE2	Systemeier informant 2	Erfaring fra NSM og PST, samt leder for hendelseshåndtering i nåværende stilling.
DL1	Driftsleverandør informant 1	30 års erfaring, jobber med levering av driftstjenester til finanssektoren.
DL2	Driftsleverandør informant 2	15 års erfaring, jobber med sikkerhetsløsninger i driftstjenester til finanssektoren.
N1	Nøkkelinformant informant 1	23 års erfaring fra sektoren. Erfaring fra PST, bank og konsulentvirksomhet
N2	Nøkkelinformant informant 2	20 års erfaring. Erfaring fra Sparebanker og banksystemet knyttet til IKT og IT, samt cyber sikkerhetshendelseshåndtering nasjonalt nivå
N3	Nøkkelinformant informant 3	20 års erfaring fra finanssektoren og utbygging/implementering av digitale sikkerhetsløsninger.
N4	Nøkkelinformant informant	Dataingeniør med 5 års erfaring fra konsulentbransjen. Spesialisert inn mot tilsiktede cyber-angrep
N5	Nøkkelinformant informant 5	Oppga ikke bakgrunnsinformasjon annet enn utdanning: statsviter.

Kode	Kodebeskrivelse	Erfaring
N6	Nøkkelinformant informant 6	Oppga ikke bakgrunnsinformasjon annet enn utdanning: siviløkonom.
N7	Nøkkelinformant informant 7	Oppga ikke bakgrunnsinformasjon annet enn utdanning: siviløkonom.

Tabell 7: Informant-beskrivelse

Vedlegg 4: Intervjuguide

INTERVJUGUIDE

1. Introduksjonsspørsmål.
Kan du først fortelle om din bakgrunn og erfaring knyttet til IKT-sikkerhet/cybersikkerhet og finanssektoren?

2. IKT-forståelse
Hva legger du i begrepet operasjonell risiko?
Hva legger du i begrepet IKT-risiko?
Hva er forskjellen på IKT-sikkerhet og cybersikkerhet?
Hva kjennetegner god IKT-sikkerhet i en virksomhet?

3. Trusselbildet
Kan du fortelle om trusselbildet mot finanssektoren i 2018/9?
    Hvem er trusselaktørene?
    Hva er deres motivasjon?

4. Cyber-trussel/angrep:
Er det høy Cyber-risiko i finanssektoren?
→Hva er en Cyber-trussel mot finanssektoren?
→Hva er et IKT-angrep/cyber-angrep i finanssektoren?

5. Nasjonal sikkerhetsmyndighet, E-tjenesten og politiets sikkerhets tjeneste trekker frem etterretningsvirksomhet som en av de største truslene for nasjonen, på hvilken måte er denne trusselen overførbar til finanssektoren?

6. NSM trekker også frem cyberkriminalitet som, sammen med etterretningsvirksomhet, en av de største truslene. Hvorfor er cyberkriminalitet et problem for finanssektoren?

7. I Norges Bank sin rapport om finansiell infrastruktur 2018, trekkes det frem at det er en høy konsentrasjonsrisiko i finanssektoren. Hva er konsentrasjonsrisiko?
    Hvorfor er konsentrasjonsrisikoen høy?
    Hvilke konsekvenser kan konsentrasjonsrisiko gi?
    Kan denne risikoen minskes?

8. Rapporten nevner også utkontraktering. Hvordan vil du beskrive risiko tilknyttet til utkontraktering av IKT-tjenester?
    Hvorfor kan utkontrakterings svekke robusthet og gi økt sårbarhet?

9. Det skjer raske teknologiske fremskritt i dagens samfunn, hvordan påvirker teknologiske utvikling-, og innovasjon finanssektoren sin robusthet?

10. Finanstilsynet sine ROS-analyser viser at kompleksitet i system, men også hendelser øker. Hvordan forstås kompleksitet knyttet til IKT-sikkerhet i finanssektoren?

11. Både interbankssytem og system for betalingsoverføringer er digitalisert i Norge, på hvilken måte skaper det en avhengighet til annen kritisk infrastruktur?

12. Rapportering:
Hvordan rapporteres uønskede IKT-hendelser?
Rapporteres alle uønskede hendelser?
Fører uønskede hendelser til endring i praksis?
Tror du praksisen for rapportering av uønskede hendelse lik i finanssektoren?

13. Sårbarhet
Vi gjennomgikk noen trusler tidligere, Hvilke sårbarheter er tilknyttet disse truslene?
På hvilken måte kan teknologisk utvikling føre til endring i finanssektoren sine sårbarheter?

14. Betalingssystemet:
Både Norges Bank og finanstilsynet beskriver den norske finansielle infrastruktur som effektiv og robust, hvilke faktorer kan påvirke systemets
→Effektivitet
→Robusthet?

15. I 2009 ble det rapportert 115 uønskede IKT-hendelser til finanstilsynet, mens i 2017 ble det rapportert 190 uønskede hendelser. Hvordan tolker du disse tallene?

16. Kan du tenke på noen konkrete endringer i trusselbilde de siste 10årene?

17. Hvorfor oppleves trusselen for IKT-hendelser som større i 2019 enn i 2009?

Vedlegg 5: Samtykkeerklæring

Samtykkeerklæring

I forbindelse med min masteroppgave i samfunnssikkerhet ved Universitetet i Stavanger, skal jeg gjennomføre flere intervjuer. Oppgaven omhandler utviklingen av IKT-trusler i finanssektoren de siste 10 årene. Formålet med studien er å belyse hvordan utviklingen har påvirket risiko, sårbarhet og risikostyring i sektoren. For å avgrense oppgaven er «lov om betalingssystem» anvendt, og har bidratt til å generere et logisk utvalg av informanter. Utvalget er representanter fra betalingsoverføringer (interbanksystem og system for betalingsoverføringer) og er representert gjennom tilsynsmyndighet, driftsleverandør og systemeiere.

Konfidensialitet etterstrebes, og jeg benytter NSD sine retningslinjer for oppbevaring av sensitive opplysninger. For å kunne gjengi troverdige data og gjøre en grundig analyse av funn, er det ønskelig å benytte opptak i intervjuet. Dette er for å unngå distraksjon av å måtte ta notater, samt å kunne delta aktivt i samtalen. Opptaket vil kun bli lytte til av meg, og så snart det har blitt transkribert vil det bli slettet.

For å sikre konfidensialitet vil alle informanter og foretak bli anonymisert, og informanter vil bli omtalt som «TM-informant A» (tilsynsmyndighet-informant). På denne måten sikrer jeg at opplysningene blir behandlet anonymt. Dersom det er ønskelig kan i dere få muligheten til å godkjenne teksten og sitat som brukes i oppgaven før den leveres.

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

.....	.....
Alvhild Skjelvik	Respondent
Masterstudent i Samfunnssikkerhet	
Universitetet i Stavanger	

Vedlegg 6: Beskrivelse av angrepsmetoder

Tjenestenektangrep: blokkerer tilgang til en side gjennom å overbelaste systemet med falske tilkoblingsforespørsler, slik at systemet ikke klarer å respondere på legitime forespørsler. Det er den vanlisgte formen for angrep på websider. Et angrep vil forhindre legitime brukere å få tilgang til siden. Det er vanligvis gjort gjennom å «overloade» systemet med mer tilgang enn den er i stand til å håndtere.

Trojansk hest: Software som fremstår som gyldig og sikker med et tydelig formål, som i realiteten har et ondsinnet og kriminelt formål.

Orm: Et virus som kan spre uten menneskelig aktivitet.
Maleware: Skadelig programvare med ondsinnet programvare
Spyware: Software som overvåker datamaskiner og bruken av datamaskiner.
Kryptoware: Er det samme som virus

Ranseomware: også referert til som løspengevirus, utpressingsvare – er en skadelig programvare som krypterer deler av innholdet på en datamaskin. Formålet er å gjøre det utilgjengelig slik at man kan kreve løsepenger. Dersom man blir utsatt for et ransomewareangrep vil innholdet mest sannsynlig bli kryptert og krever en krypteringsnøkkel for å gjennopprette tilgang.

Phishing: Den digitale versjonen av å snoke etter informasjon, jamfør fisking av informasjon.

Spear-phishing: En variant av phishing hvor man på forhånd har samlet informasjon for å øke kredibilitet og troverdighet hos en angripers mål. Det er en mer tilpasset metode for phishing som rettes mot spesifikke mål som for eksempel bedrifter.

Zero days-angrep: Et angrep som utnytter en sårbarhet som bli avdekket i et systems software. Det betyr at sårbarheten blir utnyttet før den bli fikset/håndtert av eieren.

Vannhullsangrep: Spredning av skadevare fra et tilsynelatende ufarlig nettsted. Det kan være gjennom å utnytte et hull i et populært nettsted, for å spre skadevare.

Tredjepartsangrep: Et angrep på en verdikjede, hvor man eksempelvis angriper en leverandør for å ramme andre virksomheter.

Påvirkningsoperasjoner: Tilsynelatende usynlige operasjoner ved spredning av informasjon, falske opplysninger og falske nyheter for å påvirke oppfatningen til målet i ønsket retning.

Informasjonslekkasje: Uønsket spredning eller avdekking av sensitiv informasjon.

RAT: Remote access trojan: en software som gir administratorrettigheter til et datasystem gjennom en fjern nettverksforbindelse. RAT vil vanligvis bli installert uten at offeret er klar over det, og vil ta i bruk andre virus for å skjule operasjonene for offeret.

Fysiske implantater: Et implantat som for eksempel en USB blir koblet til en harddisk, datamaskin eller annet teknisk system og sprer så skadevare eller henter ut konfidensiell informasjon.

Vedlegg 7: Ordsøksanalyse

Finanstilsynet	
Årstall	Antall ganger cyber nevnes
2009	2
2010	8
2011	0
2012	1
2013	4
2014	10
2015	6
2016	8
2017	12
2018	16

Tabell 8: Ord-søk "cyber" i Finanstilsynets ROS-analyser 2009-2018

Vedlegg 8: Beskrivelse av tidligere cyber-angrep og cyber-hendelser

Påskehendelsen:

Våren 2011 fikk den norske finanssektoren svært store problemer da telenettet var nede. Det oppsto et problem når EDB ergo group (Evry) fikk problemer i sine systemer som følge av en oppgradering. Det førte til at både betalingsterminaler og uttak i minibanker fikk problemer, og til at flere transaksjoner ble doblet. Videre skapte det store tidsforsinkelser som førte til at det ikke var mulig å gjennomføre transaksjoner slik som vanlig (Finanstilsynet, 2012).

Bangladesh-hendelsen:

I februar 2016 ble sentralbanken i Bangladesh utsatt for et cyber -angrep gjennom SWIFT nettverket for å overføre nesten 1 milliard amerikanske doller fra «federal reserve bank of New York» til en konto tilhørende Bangladesh (Kitten, 2016). I SWIFT systemet la hackere inn 35 falske instruksjoner for overføring, hvor 5 var vellykkete og overførte 101 millioner dollar, hvor 20 millioner spores til Sri Lanka og 81 millioner til Filipinene. FRB New York stoppet de andre transaksjonene grunnet mistanke om et cyber-angrep (Al Jazeera, 2018).

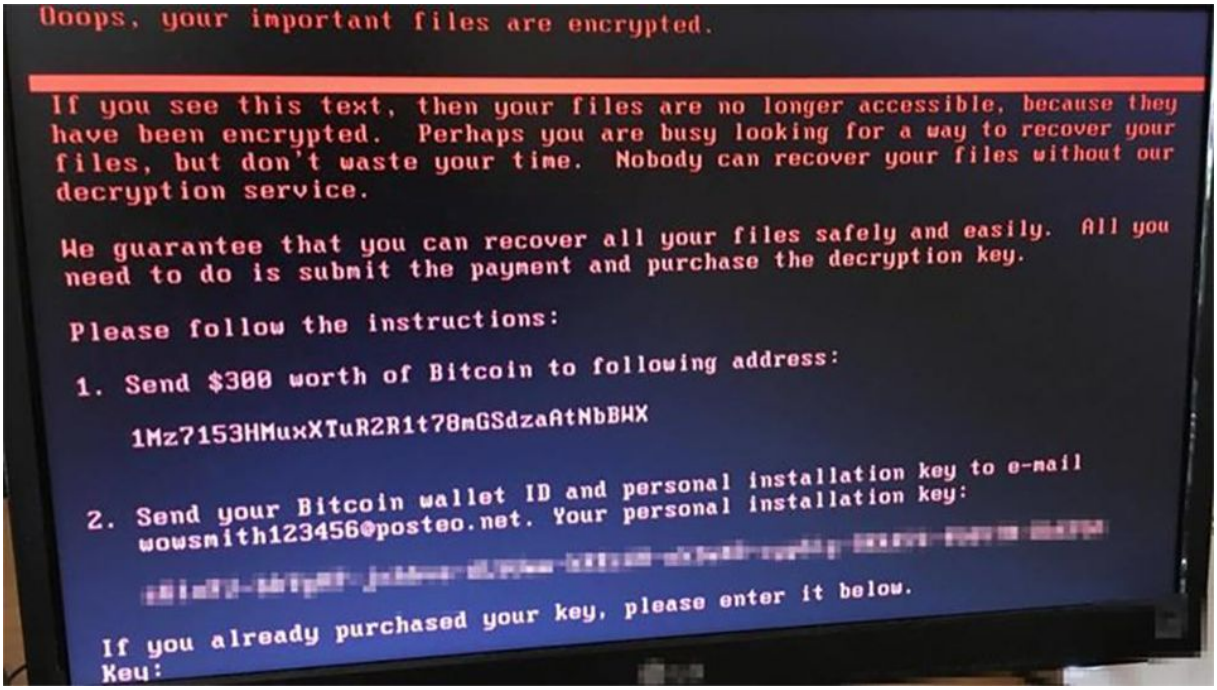
Wannacry:

Virset Wannacry (også kjent som WCry og WanaCryptor) er selvforplantende løspenge-skadevare, som en kryptoorm, som spredde seg i interne nettverk og over det offentlige Internettet ved å utnytte sårbarheter i Microsoft sine servere Message Block Protocol (Berry, Homan & Eitzman, 2017). Viruset består av to særegne komponenter, en som gir skadevaren funksjonalitet og en som gjør at den kan spre seg selv (Berry et al., 2017). Skadevaren krever 300 USD eller 600 USD for å dekryptere systemet. Angrepet rammet en rekke land, og i Norge ble helse-sektoren hardt rammet. Det førte til avlyste operasjoner og avtaler ettersom helsepersonell ikke fikk tilgang til system med personopplysninger. Flere private norske virksomheter og eliteserieklubber ble også rammet. Helsesystemet i England og Skottland, samt russiske myndigheter var også blant de som ble angrepet. NSM sa i 2017 at det var det største dataangrepet de noensinne hadde sett (Wernersen og Omland, 2017).

Figur 9: Varsling om WannaCry

NotPetya:

27. Juni 2017 startet et massivt cyber-angrep som rammet 64 land. Petya er et kryptert løspengevirus, som rettes mot microfost Windows systemer for å gjennomføre operasjoner som krypterer en harddisk sitt fil system og forhindrer windows fra å reboote. Samtidig krever det at brukeren av systemet betaler en sum i bitcoin (kryptovaluta) for å få tilgang til systemet igjen. NotPetya var varianten av viruset som ble brukt i 2017, og startet i Ukraina. Det var ukrainske selskap som først rapporterte om angrepet, og det antas at ukrainske selskap og statlige virksomheter var hovedmålet med angrepet. Ukrainias sentralbank ble hardt rammet, og man antar at det var et politisk motivert angrep mot Ukrainia ettersom det rammet Ukraina på deres nasjonaldag. Det var rettet mot energi og strøm forsyning, buss stasjoner, bensinstasjoner, flyplasser og banker. Hovedflyplassen i Kiew og atomkraftverket i Tsjernobyl ble angrepet. (Brewster, 2017; Schwartz, 2018)



Figur 10: Varsling om NotPetya

Maersk- hendelsen:

A.P Møller- Mærsk var en av selskapene som ble hardt rammet av NotPetya. Viruset lammet Mærsk sine systemer, som gjorde at det oppsto store vanskeligheter med å motta bestillinger samt 76 lasteterminaler i 59 land måtte stenge midlertidig over flere dager. Det anslås at Mærsk tapte mellom 2.1-2.5 milliarder norske kroner som følge av angrepet (Øyvann, 2017; Christensen, 2019).