DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram/spesialisering: Samfunnssikkerhet	Vårsemesteret 2023 Åpen / ~~Konfidensiell~~
Forfatter: Ferdinand Hauge	
Fagansvarlig ved UiS: Riana Steen Veileder:	
Tittel på oppgaven: Å kunne betale eller ikke kunne betale, det er spørsmålet: Om den norske finansielle infrastrukturens beredskapsevne for betalingsterminaler Engelsk tittel: To be able to pay or not be able to pay, that is the question: On the Norwegian financial infrastructure's emergency preparedness capabilities for payment terminals	
Studiepoeng: 30	
Emneord: Samfunnssikkerhet, beredskap, resiliens, DRMG, krise, pengesikkerhet, betaling, finans, betalingsterminal, kortterminal, samarbeid, STIP, reserveløsning, betalingskort	Sidetall: 107 + vedlegg/annet: 22 (129 totalt) Oslo, 14.06.2023

Å KUNNE BETALE ELLER IKKE KUNNE BETALE, DET ER SPØRSMÅLET

Om den norske finansielle infrastrukturens beredskapsevne for betalingsterminaler

Ferdinand Hauge

Masteroppgave i samfunnssikkerhet

Universitetet i Stavanger

VÅR 2023

2023

Å kunne betale eller ikke kunne betale, det er spørsmålet: Om den norske finansielle infrastrukturens beredskapsevne for betalingsterminaler

Ferdinand Hauge

Forsidemontasjen er laget ved hjelp av følgende kilder: Ja til kontanter (2022), Nave m.fl. (2022), Oakley (2016), PayJunction Team (2019), Solli (2022) og Trondsen (2006).

Forord

Denne oppgaven markerer slutten på min toårige masterutdanning i samfunnssikkerhet ved Universitetet i Stavanger og i den forbindelse ønsker jeg å takke de som muliggjorde det.

Takk til universitetet og instituttet for utdanningsopplegget deres og takk til alle gruppemedlemmene jeg samarbeidet om prosjektoppgaver med. En stor takk rettes også til Riana Steen, som gjorde en glimrende jobb med å dytte meg i riktig retning og hele tiden kom med konkrete forslag til hvordan oppgaven kunne forbedres.

Jeg skulle ønske jeg kunne takke informantene som bidro til oppgaven ved navn, men hensynet til personvern forhindrer meg fra å gjøre det. Dere skal vite at jeg er takknemlig for at dere tok dere tid til å hjelpe meg og at dere alle var så vennlige og behjelpelige som dere var. Personen jeg var i kontakt med hos Finanstilsynet, som hjalp meg med å rette inn mine forespørsler til de relevante aktørene, fortjener også en takk. Det samme gjør min far, Egil Hauge, Tommy Skjervold og alle jeg var i kontakt med underveis som hjalp meg videre i prosessen og som gjorde det de kunne for å få meg i dialog med de rette personene i utvalgte organisasjoner.

Bestefaren min, Tormod Arnold Hovda, tok på seg å stå for utgiftene til husleie og mat det halvannet året jeg var bosatt i Stavanger. En stor takk til ham! Samtidig sto mormoren min, Wilma Helene Hovda, nok en gang for deler av utgiftene til pensumlitteratur. En takk til min mor, Linda Hovda, som tok på seg å være korrekturleser og husvert for meg det siste semesteret.

Takk også til mine to andre besteforeldre. Erik Johannes Hauge som hele veien har vist interesse for fremdriften og Haldis Ellinor Valton Rasch, som dessverre døde høsten 2021. Og takk til Reidar Arvid Rasch som var med på flere gåturer i Stavanger-området via telefon, samt min bror Espen Hauge som også utviste stor interesse for mitt ve og vel.

Den største takken går også denne gangen til den norske skattebetaleren. Uten dere ville dette ikke vært mulig.

Ferdinand Hauge

Oslo, 13. juni 2023

Sammendrag

16. mai 2022 ble norske betalingsterminaler rammet av en feil. Noen butikkjeder klarte ikke å motta betaling med betalingskort. Det førte til stor offentlig oppmerksomhet og mange medieoppslag. På det tidspunktet vurderte jeg allerede å skrive om betalingsterminaler, men den hendelsen avgjorde saken. Hensikten med oppgaven er å undersøke beredskapsevnen den norske finansielle infrastrukturen har for betalingsterminaler og vurdere om den kan forbedres ved hjelp av resiliens. Det førte til følgende problemstilling:

«Hvordan kan anvendelse av konsepter og metoder innen resiliens forbedre finanssektorens beredskapsevne for betalingsterminaler?»

Oppgaven benytter seg av Darwin Resilience Management Guidelines (DRMG), som ble utviklet for å bidra til en mer effektiv krisehåndtering. Jeg gjør bruk av tre av retningslinjenes kapabilitetskort for å studere hvordan samarbeidet fungerer mellom finanssektorens aktører og hvordan de innretter beredskapen sin i forbindelse med betalingsterminaler. Basert på de utvalgte kapabilitetskortene utviklet jeg en intervjuguide som ble brukt i datainnsamlingen. Totalt deltok fem organisasjoner tilknyttet verdikjeden for betalingsterminaler i studien. Funnene viser at finanssektoren i liten grad bruker konsepter og metoder innen resiliens i sikkerhetsarbeidet. Med et økende sikkerhetsfokus i finansbransjen som følge av de siste års hendelser ligger det til rette for at resiliens kan spille en viktig rolle for å forbedre beredskapsevnen i tiden som kommer. Ikke bare for betalingsterminaler, men også i den finansielle infrastrukturen som helhet.

Abstract

Norwegian payment terminals were struck by an error on the 16th of May 2022. Some retail chains were unable to receive payment by card. It led to massive public attention and many media reports. At the time I was already considering writing about payment terminals, but this event closed the deal. The purpose of the thesis is to investigate the emergency preparedness capabilities the Norwegian financial infrastructure has for payment terminals and assess whether it can be improved by resilience. This led to the following thesis question:

"How can utilization of concepts and methods in resilience improve the financial sector's emergency preparedness capabilities for payment terminals?"

The thesis uses Darwin Resilience Management Guidelines (DRMG), which was developed to contribute to more effective crisis management. I use three of the guidelines' Capability Cards to study how the cooperation between the financial sector's actors works and how they arrange their emergency preparedness associated to payment terminals. I developed an interview guide based on the chosen Capability Cards which was used in the data gathering. Five organizations with a relation to the value chain of payment terminals participated in the study. The findings show that the financial sector uses concepts and methods in resilience to a small degree in their safety work. With an increasing safety focus in the financial industry because of events over the last years resilience may play an important role in improving the emergency preparedness capabilities in the time to come. Not only for payment terminals, but also for the whole financial infrastructure.

Forkortelser

BFI Beredskapsutvalget for finansiell infrastruktur. Opprettet i 2000 for å samordne beredskapsarbeidet mellom aktørene i finanssektoren. Ledes av Finanstilsynet.

BIDBAX BankID BankAxept. Et eget selskap for løsningene BankID og BankAxept ble etablert i 2022.

CC Capability Card (kapabilitetskort). Viser til kapabilitetskortene som brukes i DRMG.

DRMG Darwin Resilience Management Guidelines. Et sett med retningslinjer utviklet for å bistå organisasjoner og andre aktører med å forbedre sikkerhetsarbeidet ved hjelp av resiliens.

DSB Direktoratet for samfunnssikkerhet og beredskap. Opprettet i 2003 som følge av sammenslåinger mellom Direktoratet for brann- og elsikkerhet og Direktoratet for sivilt beredskap. DSB er underlagt Justis- og beredskapsdepartementet.

EMP Elektromagnetisk puls. Elektriske forstyrrelser som kan skade elektrisk utstyr.

FFI Forsvarets forskningsinstitutt. Et tverrfaglig forskningsinstitutt grunnlagt i 1946 og underlagt Forsvarsdepartementet.

NAOB Det Norske Akademis ordbok. En løpende oppdatert digital ordbok som publiseres på oppdrag fra Kulturdepartementet.

NFCERT Nordic Financial Computer Emergency Response Team. En ideell organisasjon som støtter opp om og bistår den nordiske finansindustrien i forbindelse med cyberangrep og andre tilsiktede cyberhendelser. Eies av sine medlemmer i finanssektoren. Nesten alle aktører i den kritiske finansielle infrastrukturen i Norge, Danmark og Island er medlemmer, så vel som omkring 90 prosent i Finland. Har også medlemmer i Sverige.

NTNU Norges teknisk-naturvitenskapelige universitetet. Et universitet med hovedsete i Trondheim og campuser i Ålesund og Gjøvik. Ble grunnlagt i 1996 etter en sammenslåing av seks institusjoner for forskning og høyere utdanning i Trondheim.

NSM Nasjonal sikkerhetsmyndighet. Et norsk direktorat underlagt Justis- og beredskapsdepartementet som ble grunnlagt i 2003.

PCI DSS Payment Card Industry Data Security Standard. En informasjonssikkerhets-standard brukt i forbindelse med betalingskort.

PIN Personal Identifaction Number (personlig identifiseringsnummer). En kode som er ment å verifisere at betalingskortet brukes av rette vedkommende.

ROS-analyse Risiko- og sårbarhetsanalyse.

QSA Quality Security Assessment. En systematisk gjennomgang av rutiner, arbeidsprosesser, teknikk og lignende for å kontrollere at ting fungerer som tiltenkt.

SBS Sivilt beredskapssystem. Er sammen med Beredskapssystem for forsvarssektoren del av Nasjonalt beredskapssystem, som skal sikre sivil-militær koordinering.

SINTEF Selskapet for industriell og teknisk forskning ved Norges tekniske høgskole. Et norsk forskningsinstitutt grunnlagt i 1950. Er tilknyttet NTNU.

SLA Service Level Agreement (servicenivåavtale). En avtale mellom en tjenestetilbyder og en kunde.

STIP Stand-in processing. Et kredittbasert system som slår inn hvis betalingsterminalen ikke oppnår kontakt med banken innen få sekunder.

TRL Technology Readiness Level. En skala fra 1 til 9 som måler teknologimodenhet. Skalaen indikerer hvor langt teknologien har kommet i utviklingen og hvilken dokumentasjon som finnes for dens ytelse.

Definisjoner

Beredskap «Tiltak for å forebygge, begrense eller håndtere uønskede hendelser og kriser» (Lunde, 2019, s. 38 & 43).

Betalingstjeneste «[E]n tjeneste med meldeplikt eller krav om særskilt tillatelse etter finansforetaksloven, og som omfatter en eller flere av følgende forretningsaktiviteter:

a. innskudd og uttak av kontanter på en konto
b. aktiviteter som kreves for å forvalte en konto
c. betalingstransaksjoner, herunder overføring av betalingsmidler på en konto som gjennomføres ved
    1. direktebelastninger iverksatt av betalingsmottakeren, herunder direkte engangsbelastninger
    2. bruk av betalingskort eller lignende
    3. betalerens instruksjon om kontobetalinger, herunder faste betalingsoppdrag
d. gjennomføring av betalingstransaksjoner som er nevnt i bokstav c med betalingsmidler som er omfattet av en kredittmulighet (kredittgrense)
e. utstedelse av betalingsinstrumenter og innløsning av betalingstransaksjoner
f. overføring eller mottak av betalingsmidler uten kontoavtale
g. betalingsfullmakttjenester
h. kontoinformasjonstjenester» (Finansavtaleloven, 2020, § 1-5, første ledd).

Krise «[E]n hendelse som kan resultere i store forstyrrelser i den finansielle infrastrukturen. Med store forstyrrelser menes bortfall av en tjeneste som fører til at (større deler av) befolkningen ikke har tilgang til nødvendige betalingsmidler, økonomisk aktivitet og handel stopper opp og/eller finansiell stabilitet trues» (BFI, 2016, s. 5).

Resiliens «[E]t uttrykk for hvordan folk, alene eller sammen, håndterer hverdagssituasjoner – store og små – ved å tilpasse ytelsen deres etter forholdene. En organisasjons ytelse er resilient hvis den kan fungere som nødvendig under både ventede og uventede forhold (endringer/forstyrrelser/muligheter)» (Hollnagel, 2018, s. 14-15).

Risiko «[E]t uttrykk for konsekvens/utfall av uønskede hendelser og usikkerhet assosiert med hendelser og utfall» (Njå m.fl., 2020, s. 46).

Samfunnssikkerhet «Samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger» (Meld. St. 10 (2016-2017), s. 19).

Sort svane «En overraskende ekstremhendelse relativt til ens kunnskap» (Aven og Thekdi, 2022, s. 51).

Sårbarhet «[M]anglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin tilstand eller funksjon etter hendelsen. Manglende evne relateres til vår usikkerhet om fremtiden» (Njå m.fl., 2020, s. 52).

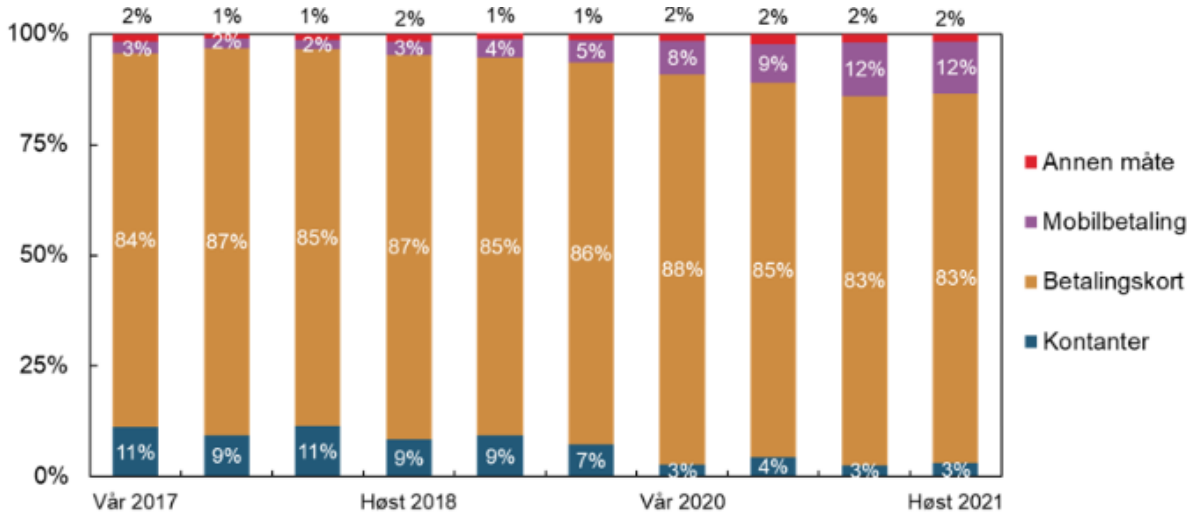
Innholdsfortegnelse

Figurer

Tabeller

1 Introduksjon

De siste tiårene har betalingsvanene endret seg markant i Norge. I 1993 sto kontanter for 85 prosent av betalingene, mens kortbetalinger utgjorde 13 prosent. De siste to prosentene ble betalt ved hjelp av sjekk. Majoriteten av betalinger ble utført med kontanter frem til omkring årtusenskiftet, samtidig som at kortbetalingene fikk stadig sterkere fotfeste. I 2007 ble 76 prosent av betalingene på utsalgssteder gjennomført som kortbetalinger. Mot slutten av 2021 var andelen kortbetalinger på 83 prosent. Det var en svak nedgang fra noen år tidligere, men var likevel fortsatt den dominerende betalingsmåten. En nevneverdig endring som har skjedd i løpet av de senere årene, er at kortbetalingene i større grad blir kontaktløse. Det vil si at kortbetalingen gjennomføres uten å dra kortet gjennom eller sette det inn i betalingsterminalen med tilhørende inntasting av PIN-kode. I 2017 ble nesten alle kortbetalinger utført ved at kortet fysisk ble satt inn i terminalen, men andelen kontaktløse betalinger utgjorde omkring 80 prosent av transaksjonene under fem år senere. Figur I viser utviklingen i betalingsmetoder mellom 2017 og 2021 (hentet fra Åmås, 2021). Mens kontantbruken falt ytterligere som følge av koronapandemien og påfølgende smittevernhensyn våren 2020, har samtidig bruken av mobilbetalinger økt en del i femårsperioden som er illustrert i figuren. Mobilbetalinger viser til tjenester som Vipps, Coopay og Apple Pay (Ibid.).



Figur I. Betalingsmåter ved handel på utsalgssted.

Selv om det er mulig at vi ser starten på betalingskortenes nedgangstider, slik kontantenes storhetstid nærmet seg slutten på 1990-tallet, er det uansett et faktum at flesteparten av

betalingene som gjennomføres på utsalgssteder i Norge skjer i en betalingsterminal ved bruk av et betalingskort. Betalingskort viser til debet-, kreditt- og faktureringskort. Inntil videre vil betalingsterminaler med andre ord spille en viktig rolle i det norske samfunnet.

I takt med at kontantbruken har blitt redusert, har også bruken av dem blitt tema for diskusjon. Skal butikker og andre utsalgssteder være pålagt å motta kontanter som betaling? Ifølge norsk lovgivning er kontanter et tvunget betalingsmiddel (Norges Bank, 2020), men hvorvidt dette egentlig er tilfellet har blitt trukket i tvil, deriblant av jusprofessor Hans Fredrik Marthinussen (Jensen, 2019). Høsten 2022 sendte regjeringen et forslag som skal styrke retten til bruk av kontanter ut på høring med svarfrist 19. desember 2022 (Regjeringen, 2022). I det denne oppgaven skrives er forslagets utfall uvisst. Det er for så vidt ikke av spesiell betydning for oppgaven, men er heller ment å illustrere hvordan den nåværende situasjonen for betalingsmidler er her til lands og bidrar dermed til å danne oppgavens bakteppe.

1.1 Bakgrunn

En årsak til at regjeringen ønsker å forsterke retten til å bruke kontanter er beredskapshensyn. 16. mai 2022 førte en intern IT-feil hos tjenesteleverandøren Nets til at mange betalingsterminaler ikke fungerte. Resultatet var lange køer ved minibanker hvor folk tok ut kontanter for å få unnagjort de siste innkjøpene i forkant av nasjonaldagen inntil feilen ble rettet og systemet var tilbake i normal drift senere samme dag (Fallmyr m.fl., 2022). Dette var en feil som førte til store problemer i enkelte betalingsterminaler og vanskeliggjorde folks innkjøp. Det er verdt å minne om at 17. mai 2022 var den første nasjonaldagsfeiringen etter at koronapandemien var offisielt avblåst og det er grunn til å tro at folk av den grunn ønsket å feire litt ekstra. Siden både enkelte dagligvarebutikker og Vinmonopolet var blant de rammede (se f.eks. Kvatningen m.fl., 2022; og Fallmyr m.fl., 2022), kan man med andre ord fastslå at timingen for feilen var langt fra optimal. Lignende hendelser, hvor betalingsterminaler er ute av drift av diverse årsaker, vet vi dessuten at kan skje fra tid til annen, selv om det sjelden er av samme størrelsesorden som 16. mai 2022. Personlig var jeg ikke berørt av hendelsen 16. mai 2022, men jeg har erfaring med en lignende hendelse i julehandelen for en del år siden. Det problemet var langt mer lokalt og rammet kun et fåtall butikker. Den gangen ble jeg reddet av at jeg hadde umiddelbar tilgang til kontanter.

Selv om det foreløpig ikke har inntruffet en hendelse som har ført til langvarig bortfall av betalingsterminaler, fordrer det likevel spørsmålet om hvorvidt samfunnet egentlig er godt nok forberedt på en situasjon hvor det ikke er mulig å betale ved hjelp av betalingskort.

Samtidig som vi har hatt hendelser som demonstrerer, om enn mildt, hva konsekvensene av bortfall av betalingsterminaler kan bli, samt regjeringens ønske om å styrke kontantenes rolle i det norske samfunnet, deriblant av beredskapshensyn, er det andre stemmer som tar til orde for å skrote kontantene permanent og gå fullt og helt over til elektroniske og digitale betalingsmetoder, kortbetalinger inkludert. De som argumenterer for dette standpunktet, viser blant annet til at kontanter bidrar til å underbygge en svart økonomi (Sættem, 2016) og at det blir billigere for kundene dersom man slipper å forholde seg til ekstraarbeidet kontanter medfører for bedriftene (Malm og Resvoll, 2022). I april 2023 foreslo Regnskap Norge at det skal være opp til hver enkelt bedrift å avgjøre hvorvidt de ønsker å motta kontantbetaling. Forslaget fikk støtte fra Virke, som representerer handels- og tjenestenæringen (De Rosa, 2023). Norges Bank jobber samtidig med et prosjekt for å finne ut om det skal innføres digitale sentralbankpenger, som er allment tilgjengelige elektroniske penger utstedt av sentralbanken på samme måte som kontanter utstedes av Norges Bank i dag, i Norge i fremtiden (Norges Bank, 2022a). Kina var den første store økonomien i verden som introduserte en digital valuta da de startet et prøveprosjekt i 2019 (Conrad, 2022). Jeremy Fleming, lederen for det britiske etterretningsorganet Government Communications Headquarters (GCHQ), som har ansvaret for signaletterretning og informasjonssikkerhet, advarte i oktober 2022 om at Kina kan bruke den digitale valutaen til å overvåke innbyggerne sine og delvis omgå eventuelle internasjonale sanksjoner (Fleming, 2022). Advarselen bidrar til å fremheve det etiske aspektet ved debatten. Kan avhengighet av elektroniske og digitale betalingsformer medføre innskrenket personvern? Og kan myndighetene straffe bestemte innbyggere ved å fryse tilgangen deres til betalingsmidler? I februar 2022 erklærte kanadiske myndigheter unntakstilstand da en omfattende demonstrasjon bidro til å sperre deler av hovedstaden Ottawa. Dermed fikk myndighetene frosset enkelte av demonstrantenes tilgang til deres egne bankkontoer, som var ment å fremskynde demonstrasjonens avslutning (Vieira og Monga, 2022).

Hensikten min er ikke å ta stilling til denne debatten, men å vise at oppgaven trer inn på et felt hvor det allerede er en større diskusjon og som potensielt medfører viktige etiske spørsmål, som kan få konsekvenser for den fremtidige samfunnssikkerheten. Med andre ord oppfatter jeg oppgavens tematikk som tidsrelevant. Ikke minst fordi en eventuell overgang til kun elektroniske og digitale betalingssystemer vil kreve stor stabilitet i systemenes ytelsesevne i og med at manuelle reserveløsninger, som kontanter, i så fall vil være utilgjengelige.

Som hendelsen 16. mai 2022 viste er betalingsterminaler viktige for at samfunnet skal fungere. Uten tilgang på betalingsmidler blir det vanskelig å få kjøpt varer og tjenester. I et samfunnssikkerhetsperspektiv er det innkjøp av nødvendighetsvarer som har størst betydning.

Med nødvendighetsvarer menes mat, drivstoff og medisiner. Jeg kommer tilbake til betalingsterminaler som en del av den kritiske infrastrukturen i Norge i kapittel 2.

1.2 Problemstilling og tilhørende forskningsspørsmål

Betalingsterminaler er fortsatt den mest brukte betalingsmåten i Norge og er dermed en sentral del av vår pengesikkerhet. Som jeg viser i kapittel 2, er dessuten betalingsterminaler definert som en kritisk infrastruktur. Når vi i tillegg vet at systemet fra tid til annen opplever forstyrrelser av varierende grad, mener jeg det er viktig å undersøke hvorvidt det er mulig å forbedre beredskapen for systemet. Jeg tar sikte på å gjøre det ved hjelp av perspektiver på resiliens. Derfor legger jeg følgende problemstilling til grunn for denne oppgaven:

«Hvordan kan anvendelse av konsepter og metoder innen resiliens forbedre finanssektorens beredskapsevne for betalingsterminaler?»

For å nærme meg et svar på problemstillingen, laget jeg tre forskningsspørsmål med den som utgangspunkt:

1. Hvordan legger aktørene i finanssektoren til rette for å fremme felles forståelse på tvers av organisasjonene i forbindelse med beredskapen for betalingsterminaler?
2. Hvordan fungerte det interorganisatoriske samarbeidet mellom aktørene i finanssektoren under bortfallet av betalingsterminalene 16. mai 2022 og hvilken lærdom trakk de ut av det?
3. Hvordan innretter finanssektorens aktører beredskapen for betalingsterminaler?

Hensikten er at forskningsspørsmålene skal hjelpe meg med å besvare problemstillingen.

1.3 Avgrensning

Den ovennevnte problemstillingen og de tre tilhørende forskningsspørsmålene forteller ingenting om hvordan jeg har tenkt til å ta i bruk resiliens for å komme nærmere en løsning. En avgrensning er nødvendig for å spisse oppgaven ytterligere.

Det er flere tilnærmingsmåter til resiliens som kunne vært mulige å bruke for dette formålet, men i denne sammenhengen falt valget på å benytte DARWIN Resilience

Management Guidelines (DRMG). Det er et sett med retningslinjer for hvordan man kan bruke resiliens for å forbedre sikkerheten og effektivisere krisehåndteringen. DRMG forklares nærmere i kapittel 3, og som det fremgår der vil mitt fokus være på punktene som gjelder det å støtte koordinering og synkronisering av fordelte oppgaver og styring av adaptiv kapasitet. Andre aspekter for å forbedre beredskapen ved hjelp av resiliens og DRMG faller utenfor denne oppgavens rammer. Grunnen til at jeg valgte å fokusere på nettopp disse er fordi jeg vurderte det som lettere og mer sannsynlig å få god informasjon å basere oppgaven på. Siden det er mange sider ved den finansielle infrastrukturen generelt og betalingsterminaler spesielt som kan være i bedriftenes interesse å holde skjult for offentligheten, valgte jeg temaer jeg antok aktørene var villige til å dele informasjon om.

Jeg legger til grunn at oppgaven kun omfatter den finansielle infrastrukturen i Norge. Hvordan beredskapen for betalingsterminaler er organisert i andre land faller utenfor denne oppgavens rammer. I enkelte tilfeller vil det likevel være aktuelt å vise til internasjonale standarder eller andre utenlandske normer, men det vil i så fall kun være for å kontekstualisere tilstanden i den norske finanssektoren.

I forlengelsen av det, dukker også spørsmålet om hvilke aktører i den norske finanssektoren oppgaven skal ta utgangspunkt i. Den norske finansielle infrastrukturen er bygd opp av en rekke aktører. Beredskapsutvalget for finansiell infrastruktur (BFI), som jeg introduserer nærmere i kapittel 3.1.3, består for eksempel av femten medlemsorganisasjoner. Dessuten vil en transaksjon som utføres ved hjelp av en betalingsterminal inkludere flere aktører før den eventuelt godkjennes og gjennomføres. Den prosessen forklares overflatisk i kapittel 2.3. Poenget mitt her er at det må gjøres en avgrensning med tanke på hvilke aktører som involveres og som følgelig skal danne grunnlaget for oppgaven. Jeg valgte å kontakte aktører som på en eller annen måte er involvert i betalingsterminalenes verdikjede og som har innsikt i beredskapsarbeidet som foregår internt i bedriften og i samarbeid med øvrige aktører. Samtidig søkte jeg å få dekket de fleste prosessene tilknyttet en transaksjon via betalingsterminal. Dermed er det empiriske grunnlaget for oppgaven avgrenset til å se på aktører som er direkte involvert i prosessen eller som har sentrale roller i den finansielle infrastrukturen. Alle selskapene jeg var i kontakt med har fast medlemskap i BFI, selv om ikke alle mine kontaktpersoner var representert der. Det betyr at diverse støttefunksjoner, som strøm og telekommunikasjon, ikke dekkes av denne oppgaven, selv om det også kunne vært en mulig retning. Det var riktignok ett unntak til dette. Jeg ønsket å komme i kontakt med en aktør innen mobilbetaling. Årsaken er at disse aktørene må regne med å få et økt press på sine nettverk hvis

betalingsterminaler av en eller grunn er ute av funksjon. Det viste seg dessverre ikke å være mulig, men dette forklares likevel nærmere og drøftes kort i henholdsvis kapittel 5 og 6.

Basert på den ovennevnte redegjørelsen er det verdt å understreke at jeg ønsket å få et innblikk i hele prosessen som er relevant for betalingsterminaler. Det betyr at jeg i liten grad var i kontakt med aktører som står for de samme tjenestene i prosessen. For eksempel var jeg kun i kontakt med en aktør som er ansvarlig for betalingskortenes funksjonalitet, selv om det på det norske markedet er flere som tilbyr den tjenesten. Jeg valgte å avgrense oppgaven på denne måten for å få et så helhetlig bilde som mulig på den tiden jeg hadde til rådighet i løpet av vårsemesteret 2023.

Med det i mente, er det på sin plass å redegjøre for hvordan oppgaven er strukturert og bygd opp.

1.4 Struktur og oppbygning

Tabell I. Oppgavens struktur og oppbygning.

Fokusområde	
1) Innledning	Kapittelet introduserer oppgavens bakgrunn og tema, for deretter å presentere problemstillingen og de tilhørende forskningsspørsmålene. Det inkluderer også en avgrensning av oppgaven og en beskrivelse av dens struktur og oppbygning.
2) Kontekst	Oppgavens kontekst forklares. Det redegjøres kort for betalingsmidlenes historiske utvikling fra oldtiden til i dag, hva samfunnets kritiske funksjoner er og hvordan betalingsterminaler er en del av dem, hvordan en betalingsterminal fungerer og et utvalg sårbarheter ved betalingsterminaler.
3) Teori	I denne delen presenteres den relevante teorien. Det er en gjennomgang av teorier om beredskap, krisefaser, resiliens og DRMG.
4) Metode	Forskningsmetoden som er tatt i bruk i arbeidet med oppgaven beskrives og vurderes. Hensikten er å redegjøre for oppgavens reliabilitet og validitet, samt at den etterlever bestemte etiske prinsipper.
5) Presentasjon av empiri	De empiriske funnene som ble gjort under datainnsamlingen legges frem systematisert på bakgrunn av forskningsspørsmål.
6) Drøfting	Her knyttes empirien sammen med det teoretiske grunnlaget. Forskningsspørsmålene diskuteres og drøftes.
7) Konklusjon	I konklusjonen presenteres et svar på problemstillingen på grunnlag av drøftingen rundt de tre forskningsspørsmålene i det foregående kapittelet.
8) Referanseliste	Det siste kapittelet inneholder en oversikt over alle referansene som ble brukt i form av en litteraturliste.

1.5 Oppsummering

I dette kapittelet introduserte jeg betalingsterminaler som tema for oppgaven og presenterte oppgavens problemstilling og tilhørende forskningsspørsmål. Det ble også foretatt en avgrensning av oppgaven og oppgavens struktur og oppbygning ble lagt frem i form av en tabell.

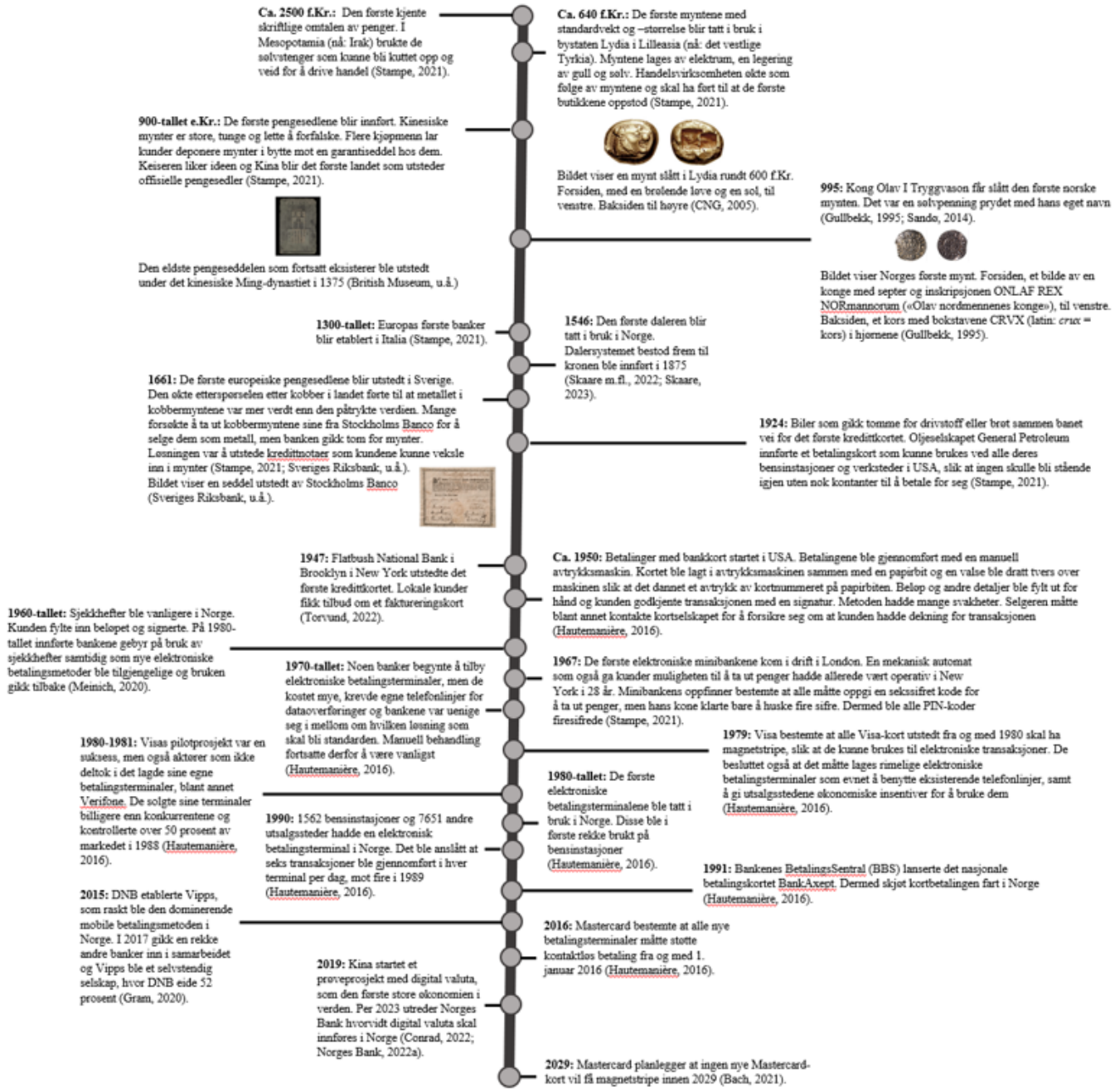
Neste kapittel setter betalingsterminalene inn i en større historisk og samfunnsmessig kontekst.

2 Kontekst

I dette kapittelet ser jeg nærmere på betalingsterminaler i et historisk og samtidig perspektiv. Jeg starter med å redegjøre kort for den historiske utviklingen til betalingsmidler fra omkring 2500 f.Kr. frem til i dag. Deretter forklarer jeg hva det som kalles samfunnets kritiske funksjoner går ut på og hvordan betalingsterminaler er en del av dem. Videre gir jeg en indikasjon på hvordan betalingsterminaler faktisk fungerer i normal drift, før jeg avslutter med en oversikt over hvilke sårbarheter de har. Men først unner vi oss altså et historisk overblikk over betalingsmidlenes utvikling.

2.1 Betalingsmidlenes historiske utvikling

Mennesker har brukt betalingsmidler for å gjøre opp for seg i omkring 4500 år. Dette var en innovasjon som gjorde at man ikke trengte å frakte med seg noe å gjennomføre en byttehandel med, uansett om det var varer, dyr eller noe annet. Dermed holdt det å ha med seg mindre gjenstander som man var enige om at hadde en gitt verdi. I løpet av de 4500 årene som har gått siden sølvstenger ble brukt som betalingsmiddel i Mesopotamia, har en rekke nye betalingsmidler sett dagens lys. Under følger en oversikt over betalingsmidlenes historiske utvikling. Den er ikke ment å være utfyllende, men heller å gi en oversikt over noen av høydepunktene i norsk og internasjonal historie. Hovedvekten er lagt på den historiske utviklingen de siste hundre årene. Plasseringen til punktene som angir årstall er satt slik de er for å gjøre figuren mest mulig kompakt og oversiktlig. Den må ikke forstås som et forsøk på en korrekt grafisk fremstilling av tidsforløpet mellom de ulike hendelsene.



Figur II. Betalingsmidlenes historiske utvikling.

Det som kanskje er mest fremtredende i betalingsmidlenes historie, er hvor viktige de har vært for samfunnsutviklingen over hele verden. Derfor er det ikke overraskende at penger er en del av det som defineres som samfunnets kritiske funksjoner i Norge.

2.2 Samfunnets kritiske funksjoner

I Meld. St. 10 (2016-2017), *Risiko i et trygt samfunn*, defineres samfunnssikkerhet som:

> Samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger (s. 19).

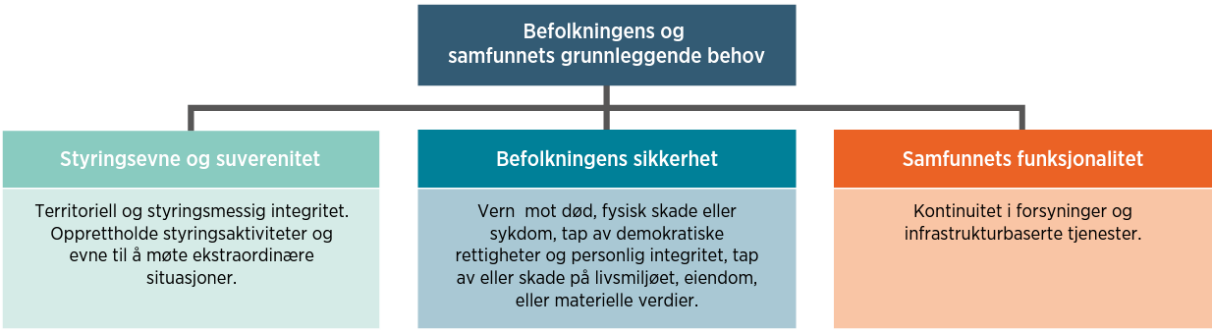
Med andre ord defineres samfunnssikkerhet som de tiltakene man iverksetter for å beskytte bestemte verdier og funksjoner som setter liv og helse i fare, uavhengig av hva som forårsaker den uønskede hendelsen. Definisjonen identifiserer imidlertid ikke hvilke grunnleggende verdier og funksjoner den omfatter eller hva som kreves for at en verdi og/eller funksjon skal inkluderes i den. En utdypning av samfunnets kritiske funksjoner ble utarbeidet av Direktoratet for samfunnssikkerhet og beredskap (DSB) på oppdrag fra Justis- og beredskapsdepartementet i 2016. I den fremgår det at en samfunnsfunksjon er kritisk dersom befolkningens og samfunnets grunnleggende behov blir truet som følge av dens bortfall. Behovene inkluderer tilgang på mat, vann, varme, trygghet med mer. (DSB, 2016, s. 27). Dette må dessuten skje innen en syvdagersperiode. Hvis funksjonens bortfall ikke truer grunnleggende behov i løpet av syv døgn, blir den ikke karakterisert som kritisk (Njå m.fl., 2020, s. 15). Totalt er det identifisert fjorten kritiske samfunnsfunksjoner fordelt på tre kategorier: Styringsevne og suverenitet, befolkningens sikkerhet og samfunnets funksjonalitet.

Styringsevne og suverenitet er funksjonene som danner de grunnleggende rammebetingelsene for ivaretakelsen av de øvrige samfunnsfunksjonene. Det innebærer blant annet opprettholdelse av territoriell integritet og en overordnet evne til å møte og håndtere ekstraordinære situasjoner (DSB, 2016, s. 28).

Befolkningens sikkerhet er de funksjonene som først og fremst har en direkte betydning for samfunnets evne til å ta hånd om befolkningens grunnleggende sikkerhet. Deres hovedhensikt er å fungere som et vern mot død, fysisk skade eller sykdom, tap av eiendom og materielle verdier osv. (Ibid.).

Samfunnets funksjonalitet handler om de funksjonene som fortrinnsvis har en indirekte betydning for samfunnets evne til å sørge for befolkningens grunnleggende sikkerhet. Dette er forskjellige former for forsyninger og infrastrukturbaserte tjenester. Disse funksjonene er viktige for borgernes trygghet og svikt kan forårsake uro, bekymring og vanskeligheter i dagliglivet (Ibid.).

Figur III viser en oversikt over innholdet i de forskjellige kategoriene (hentet fra Ibid.).



Figur III. Kategorier av samfunnsfunksjoner.

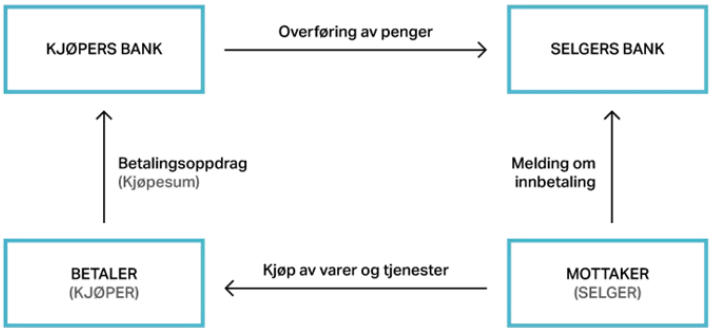
Feil i og bortfall av en funksjon kan medføre feil i og bortfall av andre funksjoner og på tvers av kategoriene. Årsaken er at enkelte funksjoner henger sammen med andre. Det er altså en grad av avhengighet enten mellom dem eller fra den ene funksjonen til den andre. En feil i et system som fører til en feil i et annet system er kjent som en kaskadefeil. For eksempel avhenger mange systemer av satellittbaserte tjenester. Bortfall av satellitter vil skape utfordringer for blant annet telekommunikasjon og betalingstransaksjoner (Brekke, 2013, s. 98-99). Selv om jeg i denne oppgaven først og fremst ser på et bestemt aspekt av en bestemt funksjon i en bestemt kategori, er det verdt å poengtere at de finansielle tjenestene også avhenger av at andre samfunnskritiske funksjoner er i virksomhet for selv å fungere normalt.

Det er syv funksjoner som utgjør kategorien samfunnets funksjonalitet: forsyningssikkerhet, vann og avløp, finansielle tjenester, kraftforsyning, elektronisk kommunikasjon, transport og satellittbaserte tjenester. Hver enkelt funksjon har også tilhørende kapabiliteter. Det vil si det samfunnet må planlegge for å opprettholde nesten uavhengig av hva som måtte inntreffe (DSB, 2016, s. 28). Kapabilitetens funksjonsevne knyttes til deres kontinuitet, sikkerhet og beredskap. Kontinuitet viser til evnen til å opprettholde en tjeneste eller leveranse når en uønsket hendelse inntreffer. Sikkerhet handler om evnen til å opprettholde et akseptabelt sikkerhetsnivå på steder som kan forårsake, eller brukes for å forårsake, skade på samfunnsverdier som liv og helse. Beredskap er evnen til å iverksette planlagte tiltak i ekstraordinære situasjoner (Ibid., s. 29). Jeg kommer tilbake til en mer detaljert forklaring på hva beredskap er i neste kapittel.

I denne oppgaven er det finansielle tjenester, som er en kategori tilhørende samfunnets funksjonalitet, som er temaet. Denne funksjonen har tre kapabiliteter knyttet til seg: finansmarkedet, finansielle transaksjoner og betalingsmidler (Ibid., s. 82). Ettersom finansmarkedet skal være i stand til å sørge for at kapital formidles på en sikker måte både nasjonalt og på tvers av landegrenser (Ibid., s. 84), faller den utenfor oppgavens rammer.

Finansielle transaksjoner viser til de forskjellige måtene penger kan overføres på. Det kan for eksempel være bankoverføringer og bruk av kontanter. Den viktigste funksjonen er å tilrettelegge for at elektroniske transaksjoner mellom banker, både nasjonalt og internasjonalt, muliggjøres (Ibid., s. 85). Det betyr at heller ikke denne kapabiliteten er innenfor oppgavens rammer. Betalingsmidler inkluderer kontanter, elektroniske betalingsinstrumenter, giro, kontobetaling med mer. For å opprettholde samfunnets funksjonalitet, er det nødvendig at befolkningen til enhver tid har tilgang til nødvendige betalingsmidler. Hvis det svikter, vil de kunne medføre konsekvenser for innbyggernes tilgang på mat og andre viktige varer (Ibid.), som igjen kan resultere i forskjellige former for sosial uro. Eksempler på elektroniske betalingsinstrumenter inkluderer debet- og kredittkort, bank- og kredittoverføringer, kryptovaluta (European Central Bank, 2021, s. 3) og betalingsapper (Finanstilsynet, 2016). Betalingsterminaler er dermed en del av denne kapabiliteten og følgelig også av samfunnets kritiske funksjoner.

For at tilgangen på betalingsmidler skal opprettholdes og samfunnets normale funksjon ivaretas, skal betalingssystemet og øvrig økonomisk infrastruktur overvåkes av Norges Bank. Norges Bank skal også bidra til beredskapsløsninger (Sentralbankloven, 2019, § 3-3 (2)). Et betalingssystem defineres i § 1-1 i Betalingssystemloven (1999). som et system «for overføring av midler med formelle og standardiserte ordninger og felles regler for behandling, avregning eller oppgjør av betalingstransaksjoner.» Dette inkluderer betalingsterminaler. En illustrasjon av hvordan et betalingssystem fungerer, er å finne i Figur IV (hentet fra Finanstilsynet, 2016).



Figur IV. Oversikt over et betalingssystem.

Figuren viser hvordan kjøp av varer og tjenester, for eksempel ved bruk av en betalingsterminal, gjennomføres i praksis. Kjøperen overfører penger til sin egen bank, som overfører pengene til bankkontoen selgerens bank har registrert hos Norges Bank. Selgerens bank får en melding om

innbetalingen og overfører beløpet til selgerens konto. For at dette skal være så effektivt som mulig, har bankene i Norge inngått avtaler seg imellom.

At det er et krav om beredskapsløsninger i forbindelse med betalingsterminaler, fremgår mer direkte i Forskrift om systemer for betalingstjenester (2019). Forskriften pålegger alle betalingstjenestetilbyderne å gjennomføre risiko- og sårbarhetsanalyser (ROS-analyser) når en ny betalingstjeneste lanseres, ved hendelser eller hvis det utføres endringer som har betydning for sikkerhetsnivået, jfr. § 2, første ledd. Paragrafens øvrige ledd stadfester krav om tilgang på systemer og kontrollmekanismer for operasjonell og sikkerhetsmessig risiko, samt effektive fremgangsmåter for hendelseshåndtering. I tillegg pålegges alle betalingstjenestetilbydere årlig å rapportere til Finanstilsynet om både operasjonell- og sikkerhetsrisiko tilknyttet betalingstjenestene. Videre skal alle betalingstjenestetilbydere etablere tiltak på bakgrunn av ROS-analysene for at betalingstjenesten skal ha en sikker ytelse, også ved å sørge for dens tilgjengelighet (§ 4). Definisjonen på hva en betalingstjeneste er, finnes i Finansavtalelovens (2020) § 1-5, første ledd:

> Med *betalingstjeneste* menes i denne loven en tjeneste med meldeplikt eller krav om særskilt tillatelse etter finansforetaksloven, og som omfatter en eller flere av følgende forretningsaktiviteter:
>
> a. innskudd og uttak av kontanter på en konto
> b. aktiviteter som kreves for å forvalte en konto
> **c. betalingstransaksjoner, herunder overføring av betalingsmidler på en konto som gjennomføres ved** (forfatterens uthevning)
>   1. direktebelastninger iverksatt av betalingsmottakeren, herunder direkte engangsbelastninger
>   2. **bruk av betalingskort eller lignende** (forfatterens uthevning)
>   3. betalerens instruksjon om kontobetalinger, herunder faste betalingsoppdrag
> d. gjennomføring av betalingstransaksjoner som nevnt i bokstav c med betalingsmidler som er omfattet av en kredittmulighet (kredittgrense)
> e. utstedelse av betalingsinstrumenter og innløsning av betalingstransaksjoner
> f. overføring eller mottak av betalingsmidler uten kontoavtale
> g. betalingsfullmakttjenester
> h. kontoinformasjonstjenester

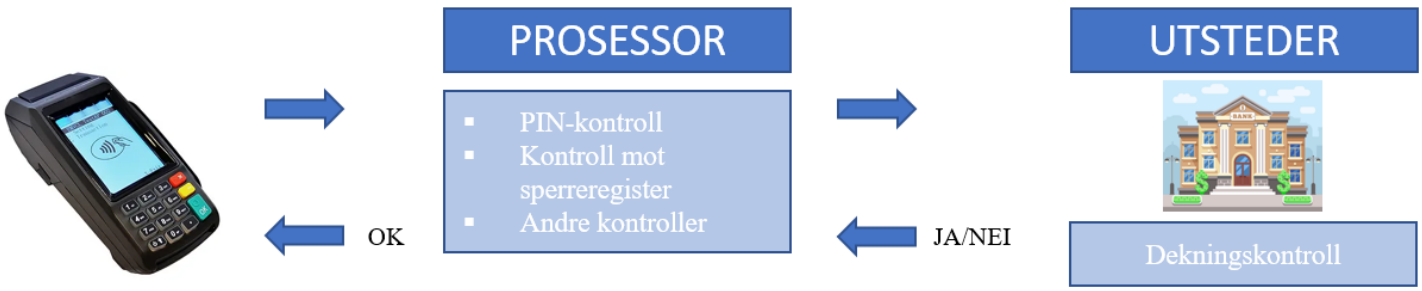
For å utføre betalingstjenester i Norge må foretaket være lovlig godkjent som bank, kredittforetak, betalingsforetak, e-pengeforetak, opplysningsfullmektig eller finansieringsforetak. Enkelte utenlandske aktører, som godkjente kredittinstitusjoner, har også

tillatelse til å utføre betalingstjenester i Norge, i henhold til Finansforetakslovens (2015) § 2-3, første og andre ledd.

Det betyr at kun godkjente institusjoner kan utføre betalingstjenester, herunder også betalingskort som benyttes i betalingsterminaler, og at disse er pålagt å utføre ROS-analyser og eventuelt iverksette beredskapstiltak for å ivareta sikkerheten. De må også overlevere en samlet vurdering til Finanstilsynet, som har ansvaret for å føre oppsyn med og vurdere hvorvidt tiltakene som tas for å ivareta sikkerheten er tilstrekkelige. Med andre ord er det krav om at betalingstjenestetilbyderne skal ha en form for beredskap i driften, deriblant for betalingsterminaler. Det fordrer spørsmålet om hvilke sårbarheter en betalingsterminal har, men la oss først undersøke hvordan en betalingsterminal fungerer når alt virker som det skal.

2.3 Hvordan en betalingsterminal fungerer

Hvordan et betalingssystem fungerer viste jeg i Figur IV ovenfor. Her flyttes fokuset over på selve betalingsterminalen og hvordan den fungerer når man utfører et varekjøp i butikken. Den følgende redegjørelsen er forenklet og tar utgangspunkt i at hele transaksjonsflyten gjennomføres uten problemer. Hvordan beredskapen er innordnet for å håndtere at det er noe feil i transaksjonsflyten som forhindrer den fra å fungere som normalt, kommer jeg tilbake til i kapittel 5.



Figur V. Forenklet transaksjonsflyt ved bruk av betalingsterminaler.

Figur V er basert på informasjon innhentet fra informanter og tegnet på bakgrunn av en lignende modell som en av informantene delte med meg. Illustrasjonsbildene er hentet fra Vodacom (2023) og Freepik (2023).

For å forklare figuren gjennomfører vi et tenkt varekjøp og betaler med et betalingskort i en betalingsterminal. Uansett om vi setter kortet fysisk inn i terminalen eller bruker det kontaktløst er det de samme mekanismene som er i sving. I dette tilfellet setter vi kortet inn i

terminalen. Den ønsker da en verifisering på at vi har tillatelse til å bruke kortet og ber om dets PIN-kode. Etter at vi har tastet inn koden utføres det en kontroll for å sjekke at den stemmer. Prosessoren utfører også en rekke andre kontroller. For eksempel kontrolleres det at kortet er gyldig og ikke er sperret for bruk. Et eksempel på en sperremekanisme er regionsperre, som gjør kortet ubrukelig i områder valgt av kortets eier. Når kontrollene knyttet til selve kortet er utført og godkjent, sendes informasjonen videre til den institusjonen som har utstedt kortet vårt. Hos banken sjekkes det om vi har tilstrekkelig med penger på kontoen hvis vi betaler med et debetkort eller om vi har tilgjengelig kreditt dersom vi betaler med et kredittkort – en såkalt dekningskontroll. Hvis vi har penger til å gjennomføre varekjøpet vil banken informere terminalens programvare om at det er dekning for kjøpet og transaksjonen godkjennes deretter av terminalen. Terminalen gir uttrykk for at kjøpet er godkjent, for eksempel ved å lyse grønt, og vi har betalt for varen. Hele prosessen er unnagjort i løpet av få sekunder.

Det er veldig enkelt forklart hva som skjer når man betaler med kort i butikken. Neste spørsmål blir hvilke aktører som er involvert i denne prosessen. Uten at det eksplisitt ble nevnt, antyder forklaringen ovenfor at mer enn én aktør må være involvert i transaksjonen for at kjøpet skal være vellykket. Under følger en kort forklaring av hvem som er involvert. Heller ikke denne fremstillingen er utfyllende og aktørene som nevnes er eksempler på hvem som er involvert i de forskjellige prosessene.

Butikken vi er i har en avtale med en leverandør av betalingsterminaler. Det finnes mange forskjellige leverandører på det norske markedet. Blant de største leverandørene her til lands finner vi Nets, Verifone, Zettle, Bambora og SumUp. De står for den fysiske terminalen og dens innmat.

Betalingskortet vi bruker for å kjøpe varen er utstedt av en finansinstitusjon, som oftest en bank. De fleste betalingskortene i Norge kommer med BankAxept, men ikke alle. I tillegg er det vanlig at kortene også er av typen Visa eller Mastercard. Det gjør kortene mulige å bruke utenfor Norges grenser, ettersom BankAxept utelukkende er laget for å fungere i Norge. I en norsk terminal vil terminalen som hovedregel lese av BankAxept først. Dersom kortet ikke har BankAxept eller hvis BankAxept av andre årsaker er skrudd av, vil transaksjonen gå gjennom Visa eller Mastercard. Bildene under er eksempler på hvordan kortene kan se ut når de kommer med både BankAxept og Visa eller Mastercard. De fysiske betalingskortene i Norge produseres ikke av den som står oppført som utsteder. Det er en tredjepart som produserer dem på oppdrag for utstederen. Bedrifter som Tietoevry og Nets produserer betalingskort i Norge.

Bildene viser eksempler på betalingskort med støtte for hhv. BankAxept og Mastercard (til venstre) og BankAxept og Visa (til høyre). Kortene er utstedt av Danske Bank og SpareBank 1. Bildene er hentet fra Danske Bank (2023) og SpareBank 1 (2023).

Enkelte kort kommer uten BankAxept og har kun støtte for Visa eller Mastercard. Disse er vanligvis kredittkort, men det finnes kredittkort som også har støtte for BankAxept. Under ses eksempler på kredittkort uten støtte for BankAxept.

Bildene viser eksempler på kredittkort med støtte for hhv. Visa (til venstre) og Mastercard (til høyre), men som ikke støtter BankAxept. Kortene er utstedt av Bank Norwegian og Coop. Bildene er hentet fra Dinero (2023) og Gramnæs (2023).

For at terminalen skal kunne utføre kontrollmekanismene må den oppnå kontakt med eksterne aktører. Dette er tilrettelagt gjennom programvaren. Tietoevry er et eksempel på en aktør som tilbyr den typen programvaretjenester som fungerer som et bindeledd mellom terminalen og de eksterne aktørene. Eksempler på aktører terminalen skal oppnå kontakt med i verifiseringsprosessen, kan være kundens bank, sperreregistre med mer. Mellomleddet mellom terminalens programvare og de eksterne aktørene er prosessoren som finnes eksternt i et datasenter hos en leverandør, for eksempel Nets.

Banken eller en annen finansinstitusjon som har utstedt kortet er også involvert i transaksjonen. Det er hos banken at det kontrolleres at kortet som brukes til å gjennomføre transaksjonen har tilgjengelige midler. Hvilken bank eller finansinstitusjon som er involvert vil variere alt ettersom hvor betalingskortet er utstedt fra. Eksempler på banker i det norske markedet er SpareBank 1, DNB, Bulder Bank og Eika.

I tillegg til dette kreves det enkelte støttefunksjoner for at terminalen skal være i normal drift. Det kreves for eksempel både tilgang på strøm og et nettverk.

Forskjellige terminaltyper har ulike strømtilganger. En stasjonær terminal er fastmontert og vil vanligvis ha direkte strømtilgang via kabel. Trådløse terminaler er flyttbare og brukes gjerne steder hvor betalingene ikke skjer på et bestemt sted, slik som på restauranter, ferger og lignende. Disse terminalene går på batterier som vanligvis er oppladbare.

Måten fastmonterte og trådløse terminaler kobler seg på et nettverk er også forskjellig. En trådløs terminal krever tilgang på et mobilnettverk, som igjen er basert på satellittfunksjoner. En fastmontert terminal må også ha internettilgang, men vil vanligvis ha tilgangen gjennom et mer stabilt nettverk, for eksempel det trådløse nettverket (Wi-Fi) hvor den er montert.

Dette er det grunnleggende i hvordan en betalingsterminal fungerer, hvilke aktører som er involvert når en transaksjon gjennomføres gjennom en terminal og hvilke støttefunksjoner en terminal er avhengig av for å virke. Med det i bakhodet kan vi rette blikket mot hvilke sårbarheter en betalingsterminal har.

2.4 Sårbarheter ved betalingsterminaler

Professor Kristian Gjøsteen, som blant annet forsker på IT-sikkerhet og -sårbarhet ved NTNU i Trondheim, uttrykte i et intervju bekymring for at systemet for betalingsterminaler falt ut av seg selv 16. mai 2022 og la til at systemet nærmest kunne kollapse ved en større påkjenning (Solli, 2022). Ut fra det er det tydelig at det finnes en rekke trusler mot betalingsterminaler. De kan eksistere i form av både naturlige og menneskeskapte årsaker, og være både tilsiktede og utilsiktede. Dette delkapittelet utforsker nærmere hva som kan føre til bortfall av betalingsterminaler, men det må ikke forstås som et forsøk på å lage en utfyllende liste over hendelser, årsaker og avhengigheter. Derimot er det tenkt som en illustrasjon på hvor mangfoldige og mangslungne truslene mot betalingsterminaler er.

Betalingsterminaler er avhengige av flere andre typer infrastrukturer for å fungere. De trenger elektrisitet, IT-tjenester, telekommunikasjon og benytter seg også av satellittbaserte tjenester (Meld. St. 10 (2019-2020), s. 65). For å utbrodere litt fra forrige delkapittel er det verdt å kommentere forskjellene mellom betalingsterminaler i litt større detalj. Ulike betalingsterminaler har forskjellige behov for å fungere normalt. Enkelte baserer seg eksempelvis på Wi-Fi og/eller Bluetooth-teknologi, som gjør at de egner seg best i faste lokaler, mens andre benytter seg av mobilnettet. Den typen passer bedre for utsalg på farten. Sist nevnte jeg restauranter og ferger, men også ulike former for budtjenester, for eksempel matlevering, fungerer som eksempel på hvor denne typen betalingsterminaler er i bruk. Nyere betalingsterminaler vil ofte ha mulighet for tilkobling via begge metodene (Hautemanière,

2019). Uansett vil en betalingsterminal være avhengig av andre typer infrastrukturer for å opprettholde normal drift og bortfall av en av disse vil kunne medføre at betalingsterminalene slutter å fungere inntil feilen i det andre systemet er utbedret. Samtlige av de ovennevnte avhengighetene er, i likhet med befolkningens tilgang til betalingsmidler, en del av det som regnes med i samfunnets kritiske funksjoner i henhold til DSB, som redegjort for tidligere i dette kapittelet.

I NOU 2015: 13, *Digital sårbarhet – sikkert samfunn*, ble befolkningens tilgang til betalingsløsninger identifisert som ett av fem områder for digital sårbarhet i finanssektoren (s. 174). BankAxept var i 2015 det dominerende betalingsmiddelet i norsk varehandel, selv om internasjonale kredittkortfirmaer gradvis har økt sine markedsandeler. I 2023 utgjør BankAxept omkring 80 prosent av betalingstransaksjonene i Norge (BankAxept, 2023a). Årsaken er at alle betalingsterminaler i Norge godtar BankAxept. Derfor vil et bortfall av BankAxept-løsningen medføre de største konsekvensene for samfunnet og kan påvirke landets økonomiske stabilitet. På den andre siden vurderte utvalget som utarbeidet NOU 2015: 13 at det å ha en tydelig ledende markedsaktør i Norge, i form av BankAxept, kunne være svært fordelaktig. Med en veldig dominant aktør er det enklere å investere i et felles system, som igjen gjør det lettere å finne løsninger som øker både effektiviteten og sikkerheten (s. 175-176). Sjansen for bortfall av betalingsterminaler vil dermed minske, men konsekvensene hvis de faller bort vil også bli større. Mot slutten av 2021 introduserte BankAxept en forbedret reserveløsning for bortfall av betalingsterminaler (BankAxept, 2023c; BFI, 2022). Denne gjør det mulig for varehandelen å drifte betalingsterminalene uten noen økonomisk risiko i inntil seks timer, mens utsalgssteder som selger nødvendighetsvarer (dagligvarer, medisin og drivstoff) har den samme muligheten i inntil 168 timer, altså syv døgn. Dette, samt den planlagte forbedringen av reserveløsningen som skal fases inn fra 1. juni 2023 og som gjør at den også fungerer uten tilgang på et nettverk, kommer jeg nærmere inn på i kapittel 5.

Som nevnt i kapittel 1 i forbindelse med hendelsen 16. mai 2022, kan interne IT-feil skape store forstyrrelser i systemet. I dette tilfellet lå årsaken i en intern IT-feil hos leverandøren og er et eksempel på en av sårbarhetene betalingsterminaler har. Andre typer IT-feil vil kunne ha samme innvirkning. Som alle apparater som er avhengige av elektrisitet for å fungere (Skaar, 2018), benytter også betalingsterminaler seg av elektromagnetisme. Det gjør en betalingsterminal sårbar for flere mulige hendelser, deriblant hacking. I 2016 ble det for eksempel utviklet en databrikke som kunne installere skadevare direkte inn i terminalen ved å utnytte betalingsterminalens elektromagnetiske felt (Computerworld, 2016). Akkurat dette har antakelig blitt tettet i løpet av de syv årene som har gått siden det ble oppdaget, men det fungerer

som eksempel på at det er mulig å hacke seg inn i betalingsterminaler for å skade eller manipulere dem.

Utenforstående kan også manipulere gjenstander som inngår i det som kalles tingenes internett. Det vil si gjenstander som i stadig større grad sammenkobles gjennom internett i den hensikt å forenkle folks hverdag. Dessuten utvikles det gradvis nye betalingsterminaler tilpasset tingenes internett (Excelsecu, 2023), uten at denne typen betalingsterminaler vies noen spesiell oppmerksomhet i denne oppgaven. Foruten muligheten for at noen hacker seg inn i en betalingsterminal for eksempelvis økonomisk vinning eller sabotasje, kan det også utgjøre en trussel mot personvernet. Betalingsterminalen kan potensielt være med på å overvåke personer uten deres viten og vilje (NSM, 2015, s. 18). Samtidig later vi til å stå overfor en ny sikkerhetssituasjon i Europa som følge av krigen i Ukraina. Enkelte spekulerer sågar i at vi står overfor en ny kald krig drøyt 30 år etter Sovjetunionens fall (se f.eks. Kronheim, 2022; og Suvatne og Gilbrant, 2023). Hvorvidt det er tilfellet skal ikke jeg driste meg til å drøfte her, men det viser at den sikkerhetspolitiske situasjonen i Europa er mer spent enn på lenge. Derfor er det ikke utenkelig at vi kan oppleve mer statlig styrt spionasje, sabotasje og kanskje til og med former for hybrid krigføring. I det denne oppgaven skrives våren 2023 er det fortsatt ikke brakt på det rene hvem som i virkeligheten sto bak sabotasjen av gassrørledningene Nord Stream 1 og 2 i Østersjøen i september 2022. Spekulasjonene raser og det har blant annet blitt pekt på Russland, Ukraina, proukrainske aktivister, USA og Norge som mulige sabotører (se f.eks. Paust, 2023). Uansett bidrar dette til å illustrere et mer uoversiktlig sikkerhetsbilde, hvor både statlige og ikke-statlige aktører kan bestemme seg for å ramme diverse infrastruktur av forskjellige årsaker. I senere år har Stortinget (august 2020), Østre Toten kommune (januar 2021), BankID (juni 2022) og Arbeidstilsynet (juni 2022) blitt rammet av dataangrep av ulike proporsjoner (NTB, 2022d; Rise, 2021; Lode, 2022). Norske mål unntas med andre ord ikke denne utviklingen og Nasjonal sikkerhetsmyndighet (NSM) advarte i mai 2023 om at det norske sikkerhetsnivået for cybertrusler var for dårlig (Johnsen, 2023). I april 2023 ble femten russiske diplomater tilknyttet den russiske ambassaden i Oslo utvist fra Norge, fordi de var mistenkt for å være etterretningsagenter (Grimstad m.fl., 2023). Med andre ord mente norske myndigheter at de var spioner. Det er en kjensgjerning at mange land utplasserer spioner ved ambassadene sine. Ifølge professor Anthony Glees ved University of Buckingham finnes det spioner ved hver eneste ambassade i verden (BBC, 2018). Men historien viser at ambassadeansatte kan finne på mer enn å grave etter etterretning. De nordkoreanske ambassadene i København og Oslo drev storstilt smugling av alkohol og tobakk frem til det ble avdekket av de respektive landenes politimyndigheter i 1976. Noen år senere stengte Nord-Korea ambassadene de hadde i

København og Oslo. Den eneste representasjonene de fortsatt har i Skandinavia er deres ambassade i Stockholm (Hansen, 2020). Denne historien viser at man ikke har noen garantier for hva andre land kan finne på å utrette for egen vinnings skyld. Hvis et fremmed land ser seg tjent med å angripe den finansielle infrastrukturen i Norge, kan betalingsterminaler eller andre deler av betalingssystemet bli et mål.

Til tross for at finansnæringen i det store og hele ikke har vært rammet av en alvorlig tilsiktet hendelse hittil, betyr ikke at det vil være tilfellet i fremtiden. Professor Gjøsteen ved NTNU, som også deltok i arbeidet med NOU 2015: 13, hevder at et målrettet cyberangrep mot betalingsinfrastrukturen kan resultere i at en bank kollapser (Solli, 2022). Den nye sikkerhetssituasjonen i Europa kan medføre at antallet aktører med intensjoner om å påføre skade på sivilsamfunnet øker. En måte det er mulig å forestille seg å ramme et samfunns betalingsmidler på, er ved hjelp av såkalt elektromagnetisk puls (EMP).

Hendelser som skaper EMP, vil også kunne påvirke betalingsterminaler negativt. EMP kan oppstå på grunn av både naturlige og menneskeskapte kilder. Det finnes EMP-baserte våpen som kan skade elektrisk infrastruktur, betalingsterminaler inkludert. Bruk av atomvåpen vil også medføre kraftig nok EMP til å gjøre stor skade, foruten de øvrige ringvirkningene (Wilson, 2019). Selv om det i et slikt tilfelle er nærliggende å tro at andre ting enn bortfall av betalingsterminaler får førsteprioritet, er det verdt å være klar over at EMP-ens nedslagsfelt er av en slik karakter at et stort geografisk område vil bli rammet (Andersen og Liseter, 2022). EMP forekommer også naturlig, blant annet i lynnedslag. Disse er ikke kraftige nok til å utgjøre en reell fare mot infrastrukturen. Av større fare er kraftige solstormer. Ved et såkalt koronamasseutbrudd, hvor Sola slynger ut en sky av plasma ladet med et magnetfelt, kan det påvirke den elektriske infrastrukturen på Jorda. Den antakelig sterkeste solstormen i historisk tid fant sted i 1859 og er kjent som Carrington-hendelsen, oppkalt etter astronomen Richard Carrington som observerte koronamasseutbruddet. Det er anslått at dette koronamasseutbruddet hadde like stor kraft som ti milliarder hydrogenbomber som går av samtidig (Jensen, 2022). Den gangen var det lite annet enn telegrafsystemet som var høyteknologisk nok til å bli rammet. Det ble blant annet rapportert om at enkelte telegrafstasjoner kunne sende telegrammer uten at batteriene som ellers var nødvendige for å sende meldinger var tilkoblet. Andre steder førte overspenninger til branner (Klein, 2012). I våre dager er samfunnet i langt større grad basert på elektrisitet enn hva tilfellet var i 1859. Heldigvis har vi ikke blitt truffet av en like kraftig solstorm siden da, men det har likevel vært flere hendelser som understreker det generelle farepotensialet. Under Vietnam-krigen, i 1972 førte en solstorm til at rundt 4000 sjøminer detonerte. Dette var magnetminer. De ble utløst av forstyrrelsene i magnetfeltet som

koronamasseutbruddet forårsaket (Aarønæs, 2019). I mars 1989 ble Jorda truffet av to solstormer med kun noen dagers mellomrom. Resultatet var at den canadiske provinsen Quebec ble mørklagt som følge av at elektrisiteten forsvant (Odenwald, 2009). Mens jeg skrev denne oppgaven ble vi på nytt minnet om hvilke krefter som er i sving. 13. mars 2023 ble et koronamasseutbrudd observert på den andre siden av Sola. Det ble anslått til å være minst like kraftig som Carrington-hendelsen i 1859. Til tross for at plasmaskyen skjøt ut i motsatt retning av Jordas posisjon i forhold til Sola, ble det registrert radioforstyrrelser ved polene og nordlys ble sett så langt sør som i New York (Hatfield, 2023; Luntz, 2023; Carter, 2023). En solstorm har potensial til å skape voldsomme forstyrrelser på mange områder, også for betalingsterminaler. I verste fall vil betalingsterminalene kunne være ute av drift i månedsvis i kjølvannet av en kraftig solstorm (Yago, 2020, s. 105). Den ville også ha resultert i en rekke andre problemer, slik at bortfall av betalingsterminaler ikke ville vært det mest presserende å utbedre. På sikt ville det like fullt blitt et problem. Mens andre infrastrukturer, som strømproduksjon og internett, ville blitt prioritert som viktigere å tilbake i funksjon igjen enn betalingsterminaler, kan man bli stående uten tilstrekkelige betalingsmetoder som følge av manglende betalingsterminaler.

Det finnes med andre ord en rekke hendelser som direkte og indirekte kan skape forstyrrelser og også medføre komplett bortfall av betalingsterminaler. Ovenfor har jeg gått litt mer i dybden på enkelte trusler. Når det gjelder registrerte hendelser de siste knappe 20 årene, er disse sammenfattet i Tabell II nedenfor. Denne er basert på rapporterte hendelser som ble ansett som alvorlige nok til at de ble nevnt i årsrapportene til Beredskapsutvalget for finansiell infrastruktur (BFI) eller de årlige ROS-analysene til Finanstilsynet, samt eventuelle tilsyn og øvelser, i årene mellom 2004 og 2022. Generelt viser en gjennomgang av årsrapportene at det jevnlig er mindre forstyrrelser på systemet for betalingsterminaler grunnet lokale strømbrudd eller andre driftsproblemer, men disse har blitt løst uten særlige konsekvenser for den finansielle infrastrukturen. Det er først og fremst kunder og selgere på lokalt plan som har blitt rammet av dette (se f.eks. BFI, 2008, s. 2-3).

Tabell II. Oversikt over hendelser, tilsyn og øvelser knyttet til betalingsterminaler mellom 2004 og 2022 gjengitt i rapporter fra BFI og Finanstilsynet.

ÅRSTALL	HENDELSE
2006	En del problemer i betalingstjenestene, blant annet nettbank, minibank og kortsystemer, førte til problemer for forretninger og kunder. Problemene var imidlertid ikke så alvorlige at de resulterte i vesentlige skader på den finansielle infrastrukturen (BFI, 2007, s. 2-3).

2007	Lokale avbrudd i strømforsyningen eller andre driftsproblemer gjorde at det var en del problemer i systemene for betalingstjenester. De ble løst uten alvorlige skadevirkninger for den finansielle infrastrukturen (BFI, 2008, s. 2-3).
2009	De første registrerte svindelforsøkene med betalingsterminaler på brukersteder rapporteres inn til BFI. Tiltakene som ble iverksatt for å motvirke dette ble oppfattet som effektive (BFI, 2010, s. 5).
2011	Det ble meldt inn en hendelse som førte til at en rekke korttransaksjoner mislyktes. Dette medførte store problemer for kjøper og selger (BFI, 2012, s. 5). Dette ble kjent som «Påskehendelsen» ettersom den inntraff onsdagen før påske og kunder opplevde at bruk av betalingskort i betalingsterminaler og minibanker enten ble avbrutt eller gikk svært sakte. Omkring 1/3 av transaksjonene brukte over fire sekunder og ble derfor prosessert gjennom Stand-in processing (STIP – forklares nærmere i kapittel 5, men en kortfattet forklaring er å finne i oversikten over forkortelser innledningsvis i oppgaven). Feilen var forårsaket av en hardwarefeil og at reserveløsningen (forklares nærmere i kapittel 5) ikke var oppgradert med samme kapasitet som primærløsningen da sistnevnte ble oppgradert høsten 2010. En følgefeil førte til at flere kunder fikk kortene belastet dobbelt opp i form av reservasjoner på kortet. Saldoen deres fremstod derfor som lavere enn den i realiteten var. Siden bankene var stengt i påsken ble ikke den feilen rettet før første arbeidsdag etter påske (Finanstilsynet, 2012, s. 31-32).
2013	Finanstilsynet og Norges Bank samarbeider om å utføre et tematilsyn på beredskapsløsninger for innenlands betalingsformidling. Dette følger opp en rapport fra 2009, «Alternative betalingsmåter i en beredskapssituasjon» (BFI, 2014, s. 5-6).
2014	Stabiliteten til betalingstjenestene hadde en periode i mai og juni hvor det var flere driftshendelser med få dagers mellomrom. Dette rammet mange banker (BFI, 2015, s. 4).
2014	En følgefeil forårsaket av en mindre feil fører til at kundene i en større bank ble belastet dobbelt ved VISA-transaksjoner. Da dette skulle reverseres førte en tredje feil til at kundene ble belastet en tredje gang for den samme transaksjonen. Hendelsen varer fra 7. til 9. oktober og karakteriseres i BFIs årsrapport som «alvorlig» (Ibid., s. 5).
2017	Stort sett stabile betalingstjenester, men enkelte dager med alvorlige operasjonelle driftsforstyrrelser. Stabiliteten var i disse tidsrommene «ikke tilfredsstillende». Medførte lange avbrudd i betalingstjenestene og rammet mange kunder (BFI, 2018, s. 4).
2017	En BFI-øvelse ledet av Bits ble gjennomført 5. desember. Scenariet baserte seg på at tilliten til kontanter var svekket på grunn av falske sedler i omløp og betalingskortinfrastrukturen var samtidig rammet av hendelser. Både personer og bedrifter kunne ikke betale for varer i butikk eller på internett, verken med kontanter eller betalingskort i en periode på 14 dager. Reserveløsningen fungerte, men ble selv med maksimal utvidelse oppbrukt. Øvelsen viste et behov for å kartlegge fire konkrete svakheter ved systemet, deriblant en mulig utvidelse av reserveløsningen, som vi tidligere så ble implementert sent i 2021, og hvilket reservepotensial elektroniske betalingsmetoder som er uavhengige av betalingskortinfrastrukturen har, f.eks. mobilbetalinger (Ibid., s. 5).

2019	Etter øvelsen i 2017 gjenstod det i 2019 fortsatt å avklare bankenes beredskapsløsninger for betalingskort som ikke omfattes av STIP-regelverket. Dette gjelder hovedsakelig ungdomskort. Noen banker har avtaler om at de kan bestille iverksetting av STIP på ungdomskort hos Nets i tilfeller hvor bankens autorisasjonssystem ikke fungerer (BFI, 2020, s. 5).
2020	På våren og sommeren var det flere hendelser hos felles leverandører som medførte redusert tilgang til betalingstjenestene hos mange foretak (BFI, 2021, s. 5).
2021	Den nye reserveløsningen for kortbetalinger med utvidet kapasitet ble satt i produksjon i andre halvår. Denne tilbys utvalgte brukersteder hvor det selges dagligvarer/mat, medisiner og/eller drivstoff (BFI, 2022, s. 6).
2022	Formiddagen 16. mai 2022 oppstod det problemer med bruk av betalingskort. Både BankAxept og internasjonale kort var rammet. Offline-reserveløsning med signatur fungerte de stedene det var aktivert, men noen brukersteder hadde ikke tatt den i bruk. Feilen stammet fra en nettverksendring utført i Nets og en teknisk feil hos en av terminalleverandørene forsterket problemene (Finanstilsynet, 2023, s. 39). Feilen påvirket betalingsterminaler med fast tilkobling som utgjør omtrent halvparten av betalingsterminalene i landet. Folk strømmet til minibanker for å ta ut kontanter. Det førte til at flere minibanker gikk tomme for kontanter (BFI, 2023, s. 4-5).

Det er tydelig at norske myndigheter i lang tid har sett med bekymring på sårbarheten ved elektroniske betalingssystemer. I BFIs årsrapport for 2006 fremkommer det at det er ønskelig at den finansielle infrastrukturen prioriteres med tanke på strømforsyning og telekommunikasjon i en beredskapssituasjon. På bakgrunn av dette ble det samme år opprettet en arbeidsgruppe som skulle utrede alternative betalingsmåter i en beredskapssituasjon i løpet av kalenderåret 2007 (BFI, 2007, s. 4; BFI, 2008, s. 3-4). Progresjonen i arbeidsgruppen ble dokumentert i årsrapportene for både 2007 og 2009. I 2007 ble muligheten for å bruke blant annet sjekker og blanketter som beredskapsløsninger for betalingsterminaler vurdert, men ble funnet å være urealistisk. De fastslo at kontanter var et mer hensiktsmessig alternativ (BFI, 2008, s. 3). Denne konklusjonen ble stadfestet i årsrapporten for 2009 (BFI, 2010, s. 6-7).

Fokuset på alternative betalingsløsninger førte imidlertid ikke til at den elektroniske beredskapen for betalingssystemet nødvendigvis ble bedret. I et brev til Finansdepartementet understrekte Finanstilsynet og Norges Bank i 2016 at den elektroniske beredskapen ikke var god nok (Steffensen og Weme, 2016). Som allerede nevnt ble dette utbedret gjennom en forbedret reserveløsning i 2021.

Beredskap er med andre ord viktig for å forsikre at betalingsterminalene opprettholder sine funksjoner og bidrar til å ivareta den norske pengesikkerheten.

2.5 Oppsummering

I dette kapittelet har jeg satt betalingsterminalene inn i en større rolle. Jeg startet med en gjennomgang av betalingsmidlenes historie. Der viste jeg kort deres utviklingstrekk de siste 4500 årene. Deretter satte jeg betalingsterminalene inn i vår samtidige sammenheng som en del av det som er definert som samfunnets kritiske funksjoner. En forenklet forklaring av hvordan en betalingsterminal fungerer fulgte, før jeg avsluttet med å se på sårbarheter ved betalingsterminaler og en oversikt over registrerte hendelser mellom 2004 og 2022.

Dette kapittelet viste at beredskap er av stor betydning for den finansielle infrastrukturen generelt og betalingsterminaler spesielt. I neste kapittel skal jeg se nærmere på beredskap som teoretisk konsept.

3 Teori

Beredskap som teoretisk konsept blir i dette kapittelet knyttet opp mot kritisk infrastruktur før jeg presenterer beredskapsarbeidsprosessen. Denne prosessen blir deretter sett i lys av teorier om krisefaser. Jeg ser også på hvordan det generelle beredskapsarbeidet er organisert i den finansielle infrastrukturen og hvordan risiko- og sårbarhetsanalyser brukes i finanssektoren. Etter gjennomgangen av beredskap gjennomgår jeg resiliens som sikkerhetsperspektiv og avslutter kapittelet med en redegjørelse for Darwin Resilience Management Guidelines (DRMG), som er retningslinjer utviklet med utgangspunkt i teorier om resiliens. Men først ser jeg altså på beredskap i relasjon til kritisk infrastruktur.

3.1 Beredskap knyttet til kritisk infrastruktur

Beredskap er et begrep som tillegges ulike betydninger. Som Eriksen m.fl. (2021) poengterer, er det vanskelig å finne en allment akseptert definisjon av begrepet (s. 18). Derfor velger jeg å vise noen eksempler på begrepets definisjoner og samtidig vil jeg fastslå hvordan beredskap forstås i denne oppgaven.

Etter en gjennomgang av flere definisjoner og en diskusjon basert på ulikhetene mellom dem, kom Eriksen m.fl. (2021) frem til denne definisjonen: «Beredskap er forberedelse og utøvelse av konsekvenshåndtering ved uønskede situasjoner.» (s. 30). De spesifiserer at de med «uønskede situasjoner» inkluderer kritiske situasjoner (fare- og trusselsituasjoner), kriser,

ulykker og katastrofer. Uavhengig av situasjonens størrelsesorden eller alvorlighetsgrad, må den på en eller annen måte håndteres slik at man får begrenset skader og tap (Ibid.). Deres definisjon omtaler med andre ord beredskap som forberedelsene man gjør i forkant av at en uønsket situasjon inntreffer og hvordan man håndterer dens konsekvenser etter at den har manifestert seg.

Lundes (2019) definisjon av beredskap er «tiltak for å forebygge, begrense eller håndtere uønskede hendelser og kriser» (s. 38 & 43). Den er hentet fra NOU 2000: 24, *Et sårbart samfunn* (s. 20). I likhet med den foregående definisjonen forstår Lunde beredskap som noe som fungerer både sannsynlighets- og konsekvensreduserende.

Definisjonen som brukes i Meld. St. 5 (2020-2021), *Samfunnssikkerhet i en usikker verden,* gjør et skille mellom beredskap og forebygging. Beredskap forstås som «planlagte og forberedte tiltak som gjør oss i stand til å håndtere uønskede hendelser slik at konsekvensene blir minst mulig» (s. 11). I denne definisjonen er det altså bare konsekvenshåndteringen beredskapen tar for seg. De sannsynlighetsreduserende tiltakene, som er sentrale i de to foregående definisjonene, blir i denne omtalt som forebygging (Ibid.). Denne definisjonen er nærmest identisk med den som benyttes i Meld. St. 10 (2016-2017), *Risiko i et trygt samfunn*. Også den stortingsmeldingen skiller mellom forebygging og beredskap (s. 22).

Som den korte diskusjonen om definisjoner på beredskap antyder, er det ikke gitt at beredskap handler om både sannsynlighets- og konsekvensreduserende tiltak. Det er også vanlig å skille mellom forebyggende- og beredskapsanalyser, selv om det er verdt å understreke at de komplementerer hverandre og må ses i sammenheng både med hverandre og den forutgående risiko- og sårbarhetsanalysen (ROS-analysen) (Njå m.fl., 2020, s. 331). ROS-analyser diskuteres senere i dette kapittelet. Selv om det kan være interessant å diskutere forskjeller mellom ulike beredskapsdefinisjoner og hvorvidt beredskap omfatter både sannsynlighets- og konsekvensreduserende tiltak eller kun det sistnevnte, er det ikke hensiktsmessig for denne oppgaven. Jeg tar derfor utgangspunkt i at beredskap viser til tiltak som skal fungere både sannsynlighets- og konsekvensreduserende, slik eksempelvis Lundes definisjon gjør. Som vist omfatter hans definisjon både uønskede hendelser og kriser. Det fordrer en kort forklaring på hva som ligger i de to begrepene.

En uønsket hendelse kan forstås på lik linje med en uønsket situasjon, som ble forklart ovenfor. Det innebærer kritiske situasjoner, kriser, ulykker og katastrofer (Eriksen m.fl., 2021, s. 30). Lunde skriver at uønskede hendelser er «[u]lykker, trusler, farer eller andre hendelser med åpenbart negative konsekvenser» (Lunde, 2019, s. 29). Selv om Lunde skiller mellom uønskede hendelser og kriser i beredskapsdefinisjonen hans, samler han dem i det han omtaler

som beredskapssituasjoner. Det vil si situasjoner som krever full eller delvis mobilisering av en beredskapsorganisasjon (Ibid., s. 48). Dermed skiller han ikke noe mer mellom uønskede hendelser og kriser enn det Eriksen m.fl. gjør. Like fullt er det nødvendig å definere krisebegrepet, ettersom Beredskapsutvalget for finansiell infrastruktur (BFI) selv har definert det for finanssektoren. Kort fortalt er krise en samlebetegnelse på hendelser, tilstander og situasjoner som har kritisk betydning for noen (Ibid., s. 46). Opprinnelig kommer begrepet fra gresk (*krisis*), som betyr noe i retning av avgjørende vendepunkt og/eller plutselig endring (Engen m.fl., 2021, s. 300). Andre stikkord som kjennetegner en krise er at de har potensial til å true viktige verdier, svekke evnen til å utføre samfunnsfunksjoner, tidspress og usikkerhet. Hvilket ståsted man har vil også påvirke hvorvidt noe oppfattes som en krise eller ei. Det som er en krise for noen, behøver ikke å være en krise for andre. Et vanlig eksempel er trafikkulykker. Det vil ofte være en krise for de som er involvert i ulykken, men for nødetatene på stedet vil det stort sett være en rutineoperasjon (Ibid., s. 301). Det er dette som ligger i det ovennevnte om at situasjonen har kritisk betydning for noen. Hva en krise i finanssektoren innebærer ble det enighet om i BFI i 2015. Definisjonen utvalget ble enige om lyder:

> En krise er en hendelse som kan resultere i store forstyrrelser i den finansielle infrastrukturen. Med store forstyrrelser menes bortfall av en tjeneste som fører til at (større deler av) befolkningen ikke har tilgang til nødvendige betalingsmidler, økonomisk aktivitet og handel stopper opp og/eller finansiell stabilitet trues (BFI, 2016, s. 5).

Definisjonen lever opp til den skisserte samlebetegnelsen ovenfor. Bortfall av en eller flere av disse tjenestene vil kunne ha kritisk betydning, avhengig av hvilke tjenester det er snakk om, hvilket omfang bortfallet har, samt varigheten. Først og fremst for samfunnet som helhet, men også berørte virksomheter. I henhold til denne definisjonen vil det at befolkningen, eller i det minste store deler av den, mister tilgangen til nødvendige betalingsmidler, være å anse som en krise. Når vi vet at den store majoriteten av transaksjoner i Norge gjennomføres ved hjelp av en betalingsterminal, som vist i kapittel 1, vil det si at bortfall av dem i hele eller store deler av landet har potensial til å resultere i en krise. Dette vil avhenge av hvilke og hvor effektive beredskapstiltak som iverksettes.

3.1.1 Beredskapsarbeidsprosessen

For å identifisere beredskapstiltak og utføre annet beredskapsarbeid, er det vanlig å følge en beredskapsarbeidsprosess. Den består av seks aktiviteter: kartlegge, vurdere, forberede,

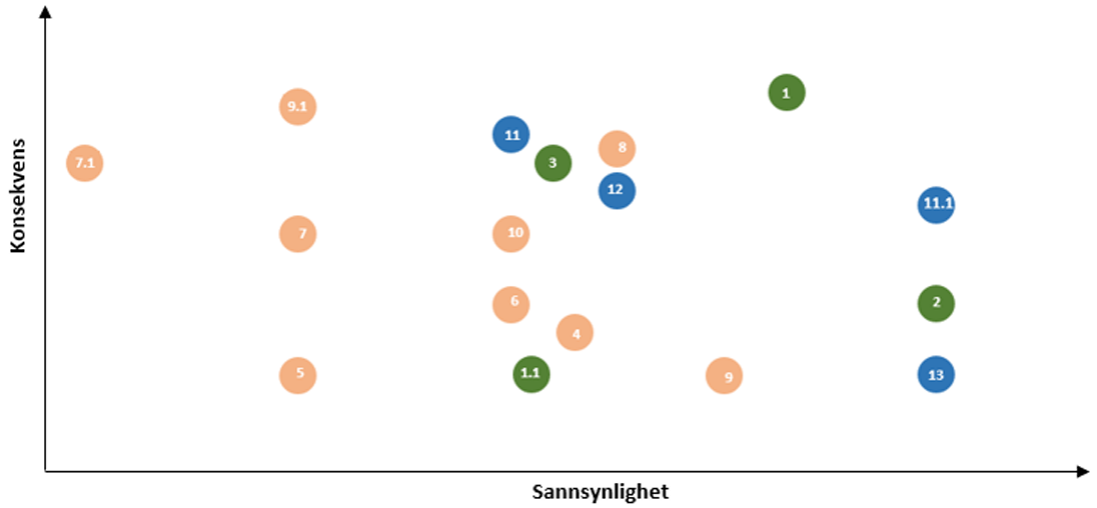
håndtere, gjenopprette og lære. Disse gjennomføres jevnlig, sett bort fra å håndtere og gjenopprette. De utføres kun i forbindelse med hendelseshåndtering og dens umiddelbare etterspill (Eriksen m.fl., 2021, s. 43). Den følgende diskusjonen om de spesifikke aktivitetene er ment å gi et overblikk over hva de går ut på og må ikke forstås utfyllende.

3.1.1.1 Kartlegge

Den første aktiviteten i beredskapsarbeidsprosessen er kartlegging. Det innebærer av man finner ut av hvilke uønskede situasjoner og hendelser som potensielt kan oppstå og hva konsekvensene av dem kan bli. For å danne et risikobilde, det vil si en oversikt over hva som kan ramme oss, er det flere fremgangsmåter man kan benytte seg av. Dette inkluderer eksempelvis HAZID-/HAZOP-analyser og sikringsrisikoanalyser. Den kanskje mest brukte er den tidligere nevnte ROS-analysen (Ibid., s. 43-44). For å lage en ROS-analyse tas det utgangspunkt i en eller flere uønskede hendelser. Hva som forstås som en uønsket hendelse vil variere ut fra konteksten de oppstår i. En flom vil i mange tilfeller forstås som en uønsket hendelse med stort skadepotensial. Under Storofsen i 1789 skal 68 mennesker ha omkommet og mer enn 3000 hus blitt ødelagt da flere elver i Norge, deriblant Glomma, gikk over sine bredder, for bare å nevne noen av skadevirkningene (NOU 1996: 16, s. 43). Men det faraoiske Egypt var i stor grad basert på at Nilen flommet over og etterlot seg store mengder slam som førte til at jordbruket blomstret, selv om mange landsbyer i en periode ble liggende som «øyer omgitt av brunt hav» (Tvedt, 2012, s. 23). Tvert imot kunne manglende Nil-flom resultere i matmangel og hungersnød (Moon, 2017). Poenget mitt er at hvilke uønskede hendelser som bør vurderes og analyseres, vil avhenge av konteksten man befinner seg i. Man vurderer risikoen ved hendelser som har et skadepotensial for de verdiene man har som målsetning å beskytte.

Hensikten med kartleggingen er altså å danne seg et bilde over hvilke uønskede hendelser som kan ramme det man skal beskytte. Et ledd i prosessen er også å skaffe seg en forståelse for de styrker, svakheter og særegenheter som er av betydning – det være seg i form av omgivelser, interessenter, organisasjon, gjensidige avhengigheter eller lignende. Andre faktorer, som rammebetingelser og usikkerhet, er også med på å tegne et risikobilde for det man jobber med (Eriksen m.fl., 2021, s. 44-45). Videre vurderes både hva som kan føre til at hendelsen oppstår og sannsynligheten for at så skal skje, samt hvilke konsekvenser den kan medføre. Konsekvensene vurderes ofte ut fra et bestemt sett med verdier, for eksempel liv og helse, økonomi eller miljø. Konsekvensen og sannsynligheten for hver enkelt hendelse plasseres på en forhåndsbestemt skala som uttrykker konsekvensomfanget og

sannsynlighetsgraden av dem. Dette kan fremstilles grafisk i form av en risikomatrise, hvor hver enkelt hendelse er plassert i henhold til konsekvens og sannsynlighet, slik at det komplette risikobildet kan illustreres på en lettfattelig måte (Njå m.fl., 2020, s. 295-300). Se Figur VI for et eksempel. Den viser risikobildet Bodø kommune presenterte i form av en risikomatrise med diverse uønskede hendelser plassert i henhold til en vurdering av konsekvens og sannsynlighet i 2018 (Bodø kommune, 2018, s. 3).



NATURHENDELSER

1. Smitteutbrudd
1.1. E.coli utbrudd
2. Sterk vind og ekstreme nedbørsmengder
3. Kvikkeleireskred

STORE ULYKKER

4. Områdebrann
5. Flyhavari Bodø lufthavn
6. Uønsket hendelse til sjøs
7. Utslipp av farlige stoffer
7.1 Atomulykke
8. Langvarig strømbortfall
9. Bortfall av IKT-infrastruktur
9.1 Bortfall av elektronisk kommunikasjon (ekom)
10. Svikt i vannforsyning

TILSIKTEDE HENDELSER

11. Terrorangrep
11.1 Hacking av kommunale IKT-systemer
12. PLIVO i utdanningsinstitusjon
13. Masseankomst av flyktninger/asylsøkere

Figur VI. Risikobilde Bodø 2018.

3.1.1.2 Vurdere

Etter at hendelsene er kartlagt, gjøres det en vurdering av beredskapen. Formålet er å etablere et grunnlag for valg av beredskapsløsninger. Vurderingen foregår i tre trinn: identifisere, analysere og evaluere. Med utgangspunkt i kartleggingen lages det som kalles beredskapsområdet. Dette er de identifiserte uønskede hendelsene det er bestemt å ha en beredskap for. Analysen utføres ofte i form av en beredskapsanalyse og går ut på å samle inn informasjon om og bli kjent med alternative beredskapsløsninger. Til slutt evalueres

beredskapsløsningene og man utarbeider anbefalinger til beslutningstakerne (Eriksen m.fl., 2021, s. 45).

3.1.1.3 Forberede

Når beredskapsløsningene er vedtatt av de rette instansene, starter arbeidet med å forberede dem. Ved å ta utgangspunkt i den allerede etablerte beredskapen justerer man beredskapstiltakene slik at de oppfyller beredskapskravene som har blitt satt. Når det ønskede beredskapsnivået er møtt, vedlikeholder man det ved hjelp av gjennomganger og eventuelle oppdateringer av beredskapsplanene, samt via trening og øvelser (Ibid., s. 45-46).

3.1.1.4 Håndtere

Dersom en uønsket hendelse oppstår skal den håndteres på bakgrunn av de etablerte beredskapstiltakene som er tilpasset situasjonen. Uansett hvor godt forberedt beredskapen er vil det alltid være behov for å tilpasse beredskapen til den konkrete hendelsen, siden ingen hendelser er identiske. Dessuten kan det oppstå hendelser man ikke har tatt høyde for og hendelser man har forberedt seg på kan utvikle seg på en uortodoks eller uventet måte. Derfor er det viktig at beredskapen er fleksibel og robust. Etter hvert som situasjonen utfolder seg, må måten man håndterer den på tilpasses slik at innsatsen har den ønskede effekten (Ibid., s. 46).

3.1.1.5 Gjenopprette

I etterkant av en uønsket hendelse kan det være mange ting som må tas hånd om. Det kan eksempelvis gjelde gjenoppbygging av fasiliteter og infrastruktur, driftskontinuitet, avklaring av ansvars- og strafferettslige forhold med mer. Gjenopprettingsarbeidet bør være godt strukturert og få tilstrekkelig finansiering, slik at det ikke blir mangelfullt (Ibid., s. 46-47).

3.1.1.6 Lære

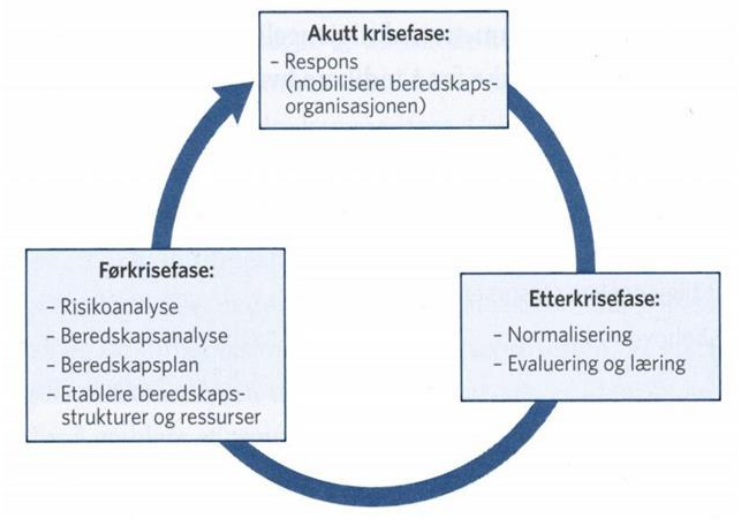
Basert på det som skjer i de forskjellige forutgående prosessene, finnes det et grunnlag for læring. Dette skjer som oftest i form av opplæring, trening og øvelser, men kan også være et resultat av andre ting. Fordi det er et begrenset antall uønskede hendelser som rammer en selv,

vil det også være hensiktsmessig å lære av andre. Det kan man gjøre ved å lese rapporter eller andre relevante dokumenter og å snakke med personer som besitter erfaring fra konkrete hendelser. Denne erfaringen, uavhengig av hvor den stammer fra, må deretter generaliseres, slik at den kan bli brukt i nye situasjoner. For at læringen faktisk skal inkorporeres, er det en fordel å ha systematiske rutiner som sørger for at erfaringen blir inkludert i fremtidige aktiviteter (Ibid., s. 47).

3.1.2 Beredskapsarbeid og krisefaser

I henhold til den ovennevnte beredskapsdefinisjonen skal beredskapsarbeidet, og den prosessen det følger, være både sannsynlighets- og konsekvensreduserende. Det sistnevnte viser til at beredskap er ment å forbedre krisehåndteringen. Det er vanlig å dele opp kriser i tre faser: førkrisefasen, den akutte krisefasen og etterkrisefasen. Disse kan ses i sammenheng med hverandre, slik at arbeidet som gjøres i de ulike fasene påvirker hverandre og man får det som kalles det utvidede krisebegrepet. I det forstås krisefasene som en sirkulær prosess. Den akutte krisefasen ses i forbindelse med det som hendte før krisen oppstod (førkrisefasen) og med det som skjer etter at den akutte krisen er over (etterkrisefasen). På samme måte vil det man lærer i etterkrisefasen kunne påvirke arbeidet som gjøres i den kommende førkrisefasen (Engen m.fl., 2021, s. 304-305).

Den utvidede kriseforståelsen kan ses i sammenheng med beredskapsarbeidet. Ulike trinn i beredskapsarbeidet kan gagne forskjellige krisefaser. Hvis man slår disse to sammen, får man figuren som er gjengitt i Figur VII (hentet fra Ibid., s. 328).



Figur VII. Det utvidede krisebegrepet med tilhørende faser i beredskapsarbeidet.

Figuren viser at førkrisefasen innebærer en eller flere former for risikoanalyser, beredskapsanalyse, utvikling av en beredskapsplan og etablering av de nødvendige beredskapsstrukturene med tilhørende ressurser. Dette er ikke en mal for hvordan det skal utføres, men viser heller hvordan det kan gjøres. For eksempel er det ikke uvanlig å gjennomføre en mer omfattende risikoanalyse som inkluderer mulige risikoreduserende tiltak og derfor ikke lage en beredskapsanalyse.

Videre illustrerer figuren at det i den akutte krisefasen kun er responsen, altså den reelle krisehåndteringen, som gjelder. I denne fasen handler det om å håndtere og få kontroll over situasjonen, slik at den får færrest mulige negative konsekvenser for de verdiene som står i fare, uavhengig av om det det er liv og helse, økonomi, omdømme, miljø eller noe annet. Eller en kombinasjon av dem, for den saks skyld.

Etter at krisen er over og hendelsen er under kontroll, starter arbeidet med å normalisere situasjonen. Hvis det for eksempel har vært en togulykke i en tunnel, vil normaliseringen innebære å rydde området, utbedre eventuelle skader på jernbanesporet og/eller tunnelen og alt annet arbeid som gjør tunnelen og sporet i brukbar stand igjen, slik at den blir klar for normal drift igjen. Det er også gode muligheter for å lære av hendelsen og ta med seg den nyvunne lærdommen inn i den nye førkrisefasen. Dermed peker etterkrisefasen på en ny førkrisefase og prosessen starter om igjen, men forhåpentligvis med et bedre utgangspunkt enn hva tilfellet var sist.

3.1.3 Beredskap i den finansielle infrastrukturen

For at den økonomiske sektoren i Norge skal ha tilfredsstillende beredskap og god krisehåndteringsevne, er risikostyringen regulert av et regelverk som forvaltes av Finansdepartementet, Finanstilsynet og Norges Bank. Tilsynet med sektoren utføres av Finanstilsynet og Norges Bank. De har ansvar for ulike deler av den. Ansvaret for kunderettede betalingstjenester, herunder blant annet betalingsterminaler, ligger hos Finanstilsynet (Regjeringen, 2020). Dette er nedfelt i Betalingssystemlovens (1999) kapittel 3 om systemer for betalingstjenester. Det er i denne sammenhengen verdt å nevne at Norges Bank også spiller en rolle i beredskapsarbeidet ved at den står for kontantforsyningen i landet (Norges Bank, 2019). Kontantenes rolle fremheves som svært viktig av Norges Bank ved svikt i de elektroniske betalingsløsningene (Norges Bank, 2022b, s. 26).

Selv om tilsynsansvaret er delt mellom Finanstilsynet og Norges Bank, ble Beredskapsutvalget for finansiell infrastruktur (BFI) etablert i 2000 for å tilrettelegge for mest mulig samordning i beredskapsarbeidet i den norske finanssektoren. Foruten Finansdepartementet, Finanstilsynet og Norges Bank, er det i 2023 tolv andre aktører i finansnæringen som er tilknyttet BFI som fullverdige styremedlemmer, varamedlemmer eller observatører. Enkelte av dem tilbyr elektroniske betalingstjenesteløsninger, som betalingsterminaler, eller er på en annen måte involvert i arbeidet med dem. I tillegg har BFI flere observatører fra andre bransjer. Dette inkluderer tele- og kraftsektoren, verdipapir- og fondsmeglersektoren og Nasjonal sikkerhetsmyndighet. Finanstilsynet er ansvarlig leder for BFI og det avholdes tre faste møter i året under normale omstendigheter. Der orienteres det blant annet om alvorlige hendelser som har skjedd i den forutgående perioden. Det utgis årlige rapporter om arbeidet i utvalget (Finanstilsynet, 2017). En fullstendig oversikt over de femten organisasjonene med representasjon i BFI er gjengitt i Tabell III.

Tabell III. Medlemmer i Beredskapsutvalget for finansiell infrastruktur.

ORGANISASJON	VIRKSOMHETSOMRÅDE
Finanstilsynet	Et selvstendig myndighetsorgan som fører kontroll og tilsyn med finanssektoren på bakgrunn av lover og vedtak fra Stortinget, regjeringen og Finansdepartementet. Har lederansvaret for BFI.
Norges Bank	Den norske sentralbanken. Har som oppgave å sørge for finansiell stabilitet og forvalter Statens pensjonsfond utland og valutareservene.
Bits AS	Bank- og finansnæringens infrastrukturselskap. Hovedoppgaven er å bevare og forsterke den norske betalingsformidlingen og betalingsinfrastrukturen.
BankID BankAxept (BidBax)	BankID er en ID- og signeringsløsning som ble introdusert i Norge i 2004 og blir i 2023 brukt av det offentlige, samtlige av landets banker og et økende antall virksomheter i andre bransjer. BankAxept er det nasjonale betalingssystemet i Norge. Det er den mest brukte betalingsløsningen for betalingskort, både på fysiske brukersteder og i netthandelen.
Nets Norge	Den norske seksjonen av et europeisk betalingsteknologiselskap. Tilbyr tjenester som dekker alle delene av verdikjeden for betalinger, deriblant produksjon av betalingskort, fysiske betalingsterminaler, autorisasjon, prosessering og avregning for betalingsterminaler med mer.
Mastercard Payment Services Norge	Den norske avdelingen av et multinasjonalt selskap som tilbyr tjenester innen betalingstransaksjoner, særlig for debet- og kredittkort.
Tietoevry Norge	Den norske delen av et finsk selskap som tilbyr IT- og produktutviklingstjenester. Opererer i flere bransjesektorer og har en egen avdeling for bank- og

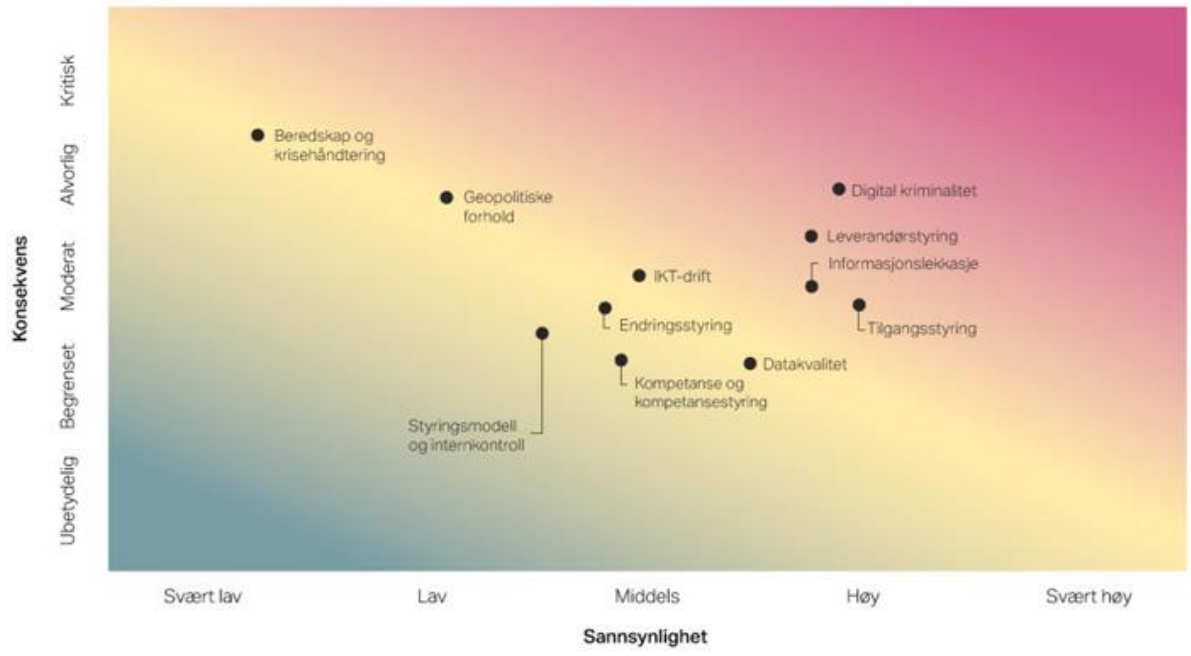
	finanstjenester. Tilbyr blant annet betalingsprogramvare, korttjenester og prosesseringssystemer.
Euronext Securities Oslo/Verdipapirsentralen ASA (VPS)	Selskapet leverer infrastruktur og tjenester tilknyttet oppgjør og registrering av rettigheter for verdipapirer. Dette inkluderer aksjer, obligasjoner, egenkapitalbevis, sertifikater og fond.
DNB	Norges største finanskonsern. Tilbyr finansielle tjenester, deriblant utstedelse av betalingskort.
Nordea Bank AB. filial Norge	Nordens største finanskonsern med hovedsete i Finland. Den norske avdelingen tilbyr finansielle tjenester, deriblant utstedelse av betalingskort.
SpareBank 1 Gruppen	En allianse bestående av tolv norske banker som opererer under samme merkevare. Tilbyr finansielle tjenester, deriblant utstedelse av betalingskort.
Eika Gruppen	En sammenslutning av en rekke norske lokalbanker. Tilbyr finansielle tjenester, deriblant utstedelse av betalingskort.
Danske Bank	Danmarks største bank- og finanskonsern med virksomhet i atten land, inkludert Norge. Banken er den tredje største på det norske markedet og tilbyr finansielle tjenester, deriblant utstedelse av betalingskort. I juni 2023 annonserte Danske Bank at de planlegger å trekke seg ut av det norske privatmarkedet for banktjenester (Bøe m.fl., 2023). Det kan bety at banken etter hvert forlater BFI.
Finansdepartementet	Et departement som har ansvaret for å planlegge og iverksette den norske finanspolitikken.
Nordic Financial CERT (NFCERT)	En ideell organisasjon eid av en rekke aktører i den finansielle infrastrukturen i Norden med hovedsete i Oslo. Oppgaven deres er å forsterke den nordiske finansindustriens evne til å motstå cyberangrep og andre tilsiktede hendelser i IKT-sfæren.

Norges Bank ga BFI sitt mandat ved opprettelsen i 2000 og hadde ansvaret for utvalget frem til Finanstilsynet overtok det i juni 2010. Ifølge mandatet skal BFI: (1) være ansvarlige for å finne og koordinere tiltak som skal forebygge og løse krisesituasjoner, samt andre situasjoner som kan medføre store forstyrrelser i den finansielle infrastrukturen; (2) varsle og informere berørte aktører og myndigheter om hva slags problemer som har oppstått, hvilke konsekvenser de kan få og hvilke tiltak som iverksettes for å løse problemene i en krisesituasjon; (3) lede koordineringsarbeidet med beredskapssaker i finanssektoren og skal, basert på Sivilt beredskapssystem (SBS), samordne både utarbeidelse og iverksettelse av varslingsplaner og beredskapstiltak i tilfelle sikkerhetspolitiske kriser og krig; (4) tilpasse representasjonen i utvalget for å løse den aktuelle krisesituasjonen og synkronisere utarbeidelsen av beredskapsplaner og implementering av omleggingstiltak; og (5) ikke erstatte den enkelte institusjons eget ansvar for beredskapen i egen virksomhet (Finanstilsynet, 2010). Mandatet gitt

til BFI aktiveres dersom det er store forstyrrelser i den finansielle infrastrukturen som resulterer i bortfall av tjenester som gjør at store deler av befolkningen mister tilgangen til nødvendige betalingsmidler, handel stanses og/eller det oppstår trusler mot den økonomiske stabiliteten (BFI, 2022, s. 2).

3.1.4 ROS-analyser i finanssektoren

BFI utarbeider selv ingen risikoanalyser. Det gjør derimot Finanstilsynet, som har ansvaret for BFI. Finanstilsynet utgir årlig offentlig tilgjengelige ROS-analyser. De er basert på funn Finanstilsynet har gjort gjennom tilsyn hos ulike finansforetak, samtaler med foretakene om risiko, informasjon fra utenlandske kontaktpersoner innen finans og kontroll, analyser utført av IKT-tilsynet, analyser av inntrufne hendelser, innmeldte hendelser med mer. Målsetningen er at den årlige ROS-analysen skal beskrive de viktigste risikoene, men er ikke ment å være aktuell for ett bestemt foretak. De er heller tenkt å være til støtte for finansforetak når de jobber med sine egne risikoanalyser og tiltak (Finanstilsynet, u.å.). Samlet sett baserer Finanstilsynets ROS-analyser seg altså på samfunnsbildet og vurderer også hvordan trusselbildet mot finanssektoren endrer seg fra år til år. Figur VIII viser Finanstilsynets risikofremstilling slik den fremstod i ROS-analysen som ble publisert våren 2023 og fungerer som et eksempel på hvordan en overordnet ROS-analyse kan presenteres innen finanssektoren (hentet fra Finanstilsynet, 2023, s. 48).



Figur VIII. Finanstilsynets vurderinger av sårbarheter og risiko for 2022.

Uansett om det er i finanssektoren eller andre steder er tanken at beredskap skal bidra til å redusere sannsynligheten for uønskede hendelser og konsekvensene av dem hvis de likevel inntreffer, men kan beredskapen ha begrensninger? Gary Klein hevder det. Han argumenterer for at risikotilnærmingen hvor man identifiserer de største risikoene og finner måter å eliminere dem på stort sett fungerer godt, men at det i komplekse situasjoner ikke er mulig å styre risikoen. Hvis det er en risiko man enten ikke forstår eller ikke vet om, vil det heller ikke være mulig å påvirke den. I stedet mener Klein at man bør håndtere risiko i komplekse situasjoner ved hjelp av resiliens fremfor å identifisere og forhindre risikoer (Klein, 2009, s. 246-247).

3.2 Bruk av resiliens i beredskap for kritisk infrastruktur

Som begrep brukes resiliens innen flere fagområder. Opprinnelig stammer det fra det latinske ordet *resilire* og kom til norsk fra det engelske *resilience*. Ifølge Det Norske Akademis ordbok (NAOB) betyr *resilire* å springe eller fare tilbake. Innen psykologien beskriver resiliens den kapasiteten man har for å håndtere stress og påkjenninger (NAOB, 2023). Stor norsk ordbok (2023) definerer resiliens på en lignende måte. Der trekkes motstandsdyktighet frem som en av de forklaringene på hva resiliens innebærer. Motstandsdyktighet, eller robusthet, blir innenfor risikofaget forstått som et systems evne til å tåle stress og påkjenninger (Aven, 2022b), og bygger opp under NAOBs definisjon. Robusthet er dermed antonymet til sårbarhet, som går ut på at stress og påkjenninger kan medføre uønskede konsekvenser for de verdiene vi tar utgangspunkt i, for eksempel liv og helse (Aven, 2023). En lignende forståelse for sårbarhet kommer til uttrykk hos Njå m.fl. (2020):

> Sårbarhet er manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin tilstand eller funksjon etter hendelsen. Manglende evne relateres til vår usikkerhet om fremtiden (s. 52).

De kobler også fraværet av sårbarhet opp mot robusthet som de igjen knytter sammen med resiliens (Ibid.). Resiliens har vokst frem som et sentralt begrep i beskrivelser av robusthet og kan forstås som en utdypning av det (Engen m.fl., 2021, s. 172). Enkelte bruker begrepene om hverandre (Aven, 2022a, s. 81), mens andre tar til orde for å holde dem atskilt. De mener at robusthet i risikofaglig sammenheng handler om evnen til å motstå kjente trusler. Resiliens går derimot ut på å forsterke systemet slik at det i tillegg til de kjente truslene også vil være i stand

til å motstå ukjente og/eller svært usannsynlige trusler (Renn, 2008, s. 179). En rapport fra Forsvarets forskningsinstitutt (FFI) advarer mot å likestille motstandsdyktighet og robusthet med resiliens, fordi de ikke er dekkende for hva resiliens-begrepet innebærer (Stavland og Bruvoll, 2019, s. 37).

I forlengelsen av det er det verdt å redegjøre kort for distinksjonen enkelte gjør mellom passiv og aktiv resiliens. Passiv resiliens er et systems evne til å absorbere forstyrrelser, komme seg raskt i etterkant av dem og returnere til sin normaltilstand. Legg merke til likhetene mellom passiv resiliens og robusthet. Aktiv resiliens handler derimot om at systemet gradvis blir sterkere ved at det lærer fra erfaring og derigjennom blir bedre rustet til å håndtere fremtidige forstyrrelser. I denne forståelsesrammen sidestilles robusthet med passiv resiliens, mens aktiv resiliens sammenlignes med det Taleb kaller antisårbarhet. Det er et systems evne til å bli sterkere som følge av vellykket å ha håndtert moderate forstyrrelser (Martin, 2019, s. 76-77). Implisitt legger Martin til grunn at resiliens ikke er det samme som robusthet, men at resiliens innehar robusthetens karaktertrekk. Den samme forståelsen er utgangspunktet for resiliens-begrepet i denne oppgaven, selv om Martins forståelse av resiliens later til å være begrenset til systemets evne til å motstå forstyrrelser og ikke dets evne til også å gripe muligheter. I den følgende diskusjonen hvor jeg definerer resiliens-begrepet nærmere ser vi at også det et viktig aspekt innen resiliens.

Som nevnt brukes resiliens innen en rekke disipliner. Det medfører at det også finnes mange ulike definisjoner. En litteraturstudie utført i 2015 identifiserte over 300 forskjellige definisjoner (Woltjer, 2015, s. 26). Ulike definisjoner vektlegger forskjellige aspekter og dette mangfoldet blir av enkelte vurdert som problematisk. Disse hevder at resiliens-begrepet risikerer å bli meningsløst, fordi det innehar så mange ulike betydninger (Lundberg og Johansson, 2015, s. 22-23). Det kan skape forvirring og slik sett virke mot sin hensikt, men kan også være til hjelp ved at man kan bruke en tilpasset definisjon. Siden denne oppgaven ikke handler om resiliens-begrepet som sådan nøyer jeg meg med å bemerke at dette er en del av diskusjonen rundt resiliens. I oppgaven forholder jeg meg til Erik Hollnagels definisjon. Det er verdt å bemerke at hvordan han definerer resiliens har forandret seg med årene. Dette forklarer han med at resiliens som sikkerhetsperspektiv stammer fra rundt årtusenskiftet og at diskusjoner og nye perspektiver har medført utvikling i hva som tillegges vekt (Hollnagel, 2018, s. 14). Fra 2006 til 2018 hadde han tre definisjoner som gradvis endret seg.

I 2006 ble følgende definisjon foreslått:

> Essensen av resiliens er derfor den iboende evnen en organisasjon (et system) har for å ivareta eller gjenvinne en dynamisk stabil tilstand, som tillater den å fortsette funksjoner etter et større uhell og/eller i nærværet av kontinuerlig stress (Hollnagel sitert i Ibid., min oversettelse).

I de påfølgende årene førte diskusjoner rundt robusthet, resiliens og sårbarhet til at det ble tydelig at resiliens ikke bare handler om å unngå feil. Derfor endret han definisjonen sin i 2011, slik at den i stedet lød:

> Den iboende evnen et system har til å justere sitt funksjonsnivå før, under og etter endringer og forstyrrelser, slik at det kan opprettholde nødvendige funksjoner under både ventede og uventede forhold (Hollnagel sitert i Ibid., min oversettelse).

Som vi ser ble det gjort endringer både ved at det refereres til «ventede og uventede forhold» i stedet for «større uhell og/eller i nærværet av kontinuerlig stress» og «evnen (…) til å justere sitt funksjonsnivå» i stedet for «å ivareta eller gjenvinne en dynamisk stabil tilstand». I forlengelsen av denne utviklingen ble det gjort ytterligere forandringer i 2018 for å utvide omfanget av resilient ytelse. Hensikten er å vise at resiliens ikke bare gjelder å komme seg i kjølvannet av trusler og stressfaktorer, men i større grad om evnen til å yte etter behov under varierte forhold, samt å svare på en passende måte overfor både forstyrrelser og muligheter. Dermed flyttes fokuset i resiliens mot resilient ytelse:

> Resiliens er et uttrykk for hvordan folk, alene eller sammen, håndterer hverdagssituasjoner – store og små – ved å tilpasse ytelsen deres etter forholdene. En organisasjons ytelse er resilient hvis den kan fungere som nødvendig under både ventede og uventede forhold (endringer/forstyrrelser/muligheter) (Hollnagel sitert i Ibid., s. 14-15, min oversettelse).

Hollnagel fremhever betydningen av at muligheter er inkludert i den siste definisjonen. Det er viktig for skiftet fra beskyttende sikkerhet (Safety-I) til produktiv sikkerhet (Safety-II) og for at resiliens ikke kun skal assosieres med sikkerhet, ettersom resiliens primært handler om ytelse (Ibid., s. 15). Derfor er resiliens ikke i konkurranse med det dominerende sikkerhetsparadigmet som baserer seg på det Hollnagel kaller Safety-I, men er ment å utfylle det og bidra til å forbedre sikkerhetsnivået (se f.eks. Eriksen m.fl., 2021, s. 180).

Til tross for at det finnes mange definisjoner av hva resiliens er, tar jeg som nevnt utgangspunkt i Hollnagels siste definisjon. Dermed legges forståelsen om at resiliens innehar både proaktive og reaktive kvaliteter til grunn her. Med proaktiv og reaktiv resiliens vises det

til tidsaspektet. Som navnene tilsier omhandler proaktiv resiliens det man gjør før en eventuell hendelse, mens reaktiv resiliens er evnen til å gjenopprette skadde funksjoner etter at en hendelse har inntruffet (Stavland og Bruvoll, 2019, s. 12).

Noe det er langt bredere enighet om enn definisjonen er hva som kjennetegner et resilient system. Hollnagel m.fl. (2011) trekker frem fire kjennetegn på det resiliente systemet, nemlig evnen til å (1) respondere; (2) overvåke; (3) forvente; og (4) lære.

3.2.1 Respondere

Å respondere handler om å vite hva man skal gjøre eller evne å imøtegå forskjellige former for endringer, forstyrrelser og muligheter ved å iverksette forberedte responsmønstre eller ved å finne nye måter å gjennomføre tiltak på, som ved å justere systemet normale funksjon. Dette er evnen til å håndtere det aktuelle (Ibid., s. xxxvii; Hollnagel, 2018, s. 26).

For å overleve må så godt som ethvert system være i stand til å respondere overfor hendelser som oppstår. Det gjelder ikke enhver hendelse, men mange av dem vil være av en slik karakter at en form for respons er nødvendig. Hendelsene kan være både av positiv eller negativ art og være både kjente og ukjente. Det de har til felles er at konsekvensene ved ikke å respondere er mindre tiltalende enn konsekvensene ved å respondere (Hollnagel, 2018, s. 28). Spørsmålet blir dermed når og hvordan man bør respondere. Forholdene for det som trigger responsen kan ha bakgrunn i en forandring i situasjonen eller en plutselig utvikling som forstyrrer den pågående aktiviteten. I en krisesituasjon er det et akutt behov for informasjon, men det er ikke gitt at den verken er tilgjengelig i tilstrekkelig grad eller holder høy nok kvalitet til å være brukbar. Mens jakten på gjerningsmennene pågikk etter bombeangrepet mot Boston-maratonen i april 2013 førte for eksempel rykter som ble spredt i sosiale medier til at flere redaksjonelle medier gikk ut med informasjon om og bilder av mistenkte terrorister som var uskyldige (Lee, 2013). Dette er et eksempel på dårlig informasjon som kan komme politi og etterforskere i hende mens de forsøker å håndtere en krise. Krisen må håndteres selv i fraværet av god og nok informasjon. Håndteringen krever da evnen til å bruke den informasjonen man faktisk har og gjøre det beste ut av den ved å se det usynlige, altså klare å tillegge situasjonen mening (*sensemaking*). Dette gjelder særlig i komplekse situasjoner hvor utfallet er uvisst. Aktørene som er involvert i krisehåndteringen kan ha forskjellige prioriteringer, målsetninger, meninger, strategier og politiske agendaer knyttet til hvordan de mener situasjonen bør håndteres (Steen m.fl., 2023, s. 1-2). Når man vurderer om situasjonen krever at det responderes på en eller annen måte er det med andre ord mange forhold som spiller inn når den vurderingen

gjøres. På samme måte som man vurderer hvorvidt forholdene krever en form for respons, må man også vurdere når responsen skal opphøre. Den må ikke avsluttes for tidlig eller for sent. Stopper den for tidlig lykkes man ikke med å oppnå det ønskede utfallet. Hvis den slutter for sent fører den fortsatte responsen til at man taper ressurser man ikke egentlig behøver å miste. Et ledd i det å respondere er derfor å overvåke forholdene eller situasjonen hvor responsen finner sted, slik at man kan avgjøre om man har oppnådd den ønskede effekten (Hollnagel, 2018, s. 29).

Dessuten må responsen være betimelig og effektiv, slik at man faktisk oppnår det ønskede utfallet i tide. For at et system skal kunne respondere må det først oppdage at noe har skjedd, gjenkjenne hendelsen og til slutt vite når og hvordan responsen skal skje. I tillegg må det være tilstrekkelig kapasitet til å gjennomføre den og man må evne å skille mellom det som haster og det som er viktig i den akutte krisefasen (Hollnagel m.fl., 2011, s. 283-284). Selve responsen kan være planlagt på forhånd eller noe som utvikles etter hvert som situasjonen utfolder seg. Det er en fordel å ha tenkt gjennom mulige hendelser og forberedt tiltak for å håndtere dem, slik hensikten med beredskapsplanlegging er, men det er en grense for hvor mye man kan forberede seg på. Hendelser og situasjoner som skjer på jevnlig basis vil ofte være de det er mest effektivt å ha planlagte tiltak for. Derimot er det urealistisk å være forberedt på hendelser som inntreffer uregelmessig eller sjelden. I slike tilfeller må tiltakene utarbeides fortløpende under hendelsesforløpet (Hollnagel, 2018, s. 29-30). Det er i denne typen situasjoner spesielt og komplekse situasjoner generelt at Gary Klein tar til orde for at ordinær risikostyring, gjennom identifisering av risikoer med påfølgende planlagte tiltak for å håndtere dem ikke fungerer. Den typen risikostyring fungerer med godt kjente risikoer som oppfører seg som ventet. Disse risikoene befinner seg ute i åpent lende og er fullt synlige. Ifølge Klein er de synlige i skinnet fra gatelysene og omtaler dem derfor som risikoer som oppholder seg under *streetlights*. Risikoene som derimot lusker i skyggene og som følgelig ikke er like synlige, og kanskje til og med er usynlige, blir av Klein forstått som å befinne seg i *shadows* (Klein, 2009, s. 10). Slike risikoer mener han ikke kan avverges eller konsekvensene reduseres i tilstrekkelig grad ved hjelp av tradisjonell risikostyring. I stedet peker Klein på resiliens som en bedre løsning, fordi resiliens søker å forbedre en organisasjons evne til omstilling for å håndtere uventede forstyrrelser. Han er av den oppfatning at resiliens kan forstås som risikostyring gjennom oppdagelse (Ibid., s. 246-247), som samsvarer med det som er gjengitt av Hollnagel ovenfor. I tillegg mener Klein at responsen overfor uforutsigbare situasjoner kan bli skadelidende dersom man utelukkende baserer seg på risikostyring og at en organisasjon i

verste fall kan gi seg selv en falsk trygghetsfølelse, som i realiteten kan gjøre vondt verre (Ibid., s. 249).

Hendelser som betegnes som sorte svaner er en variant av den typen hendelser som Klein omtaler som skyggebelagte. En sort svane er en hendelse som ifølge Taleb (2010) har tre kjennetegn: (1) den er ikke forventet siden ingenting i fortiden overbevisende kan peke mot dens mulighet for å inntreffe; (2) den har ekstrem innvirkning; og (3) man finner forklaringer på hvorfor den oppstod i etterkant slik at den i etterpåklokskapens lys fremstår som mulig både å forklare og forutse (s. xxii). På bakgrunn av disse kjennetegnene kan en sort svane defineres som «en overraskende ekstremhendelse relativt til ens kunnskap» (Aven og Thekdi, 2022, s. 51). Lee Kuan Yew kom med et eksempel på en sort svane under et intervju i 2009. Han var statsminister i Singapore i 31 år (1959-1990) og fortsatte å inneha en regjeringsrolle i ytterligere 21 år frem til han fratrådte i 2011 (PMO, 2023). Singapores landsfar, som han ble kjent som, gis ofte æren for at landet utviklet seg til å bli et globalt handels- og finanssenter (Shen og Armstrong, 2015). I intervjuet mente han at det viktigste han hadde lært de siste 20 årene var at «det umulige kan skje» og omtalte Sovjetunionens raske kollaps som «utenkelig» i 1989, to år før unionens sammenbrudd (Charlie Rose, 2009, 49:36). En av historiens mest erfarne statsmenn mente at blant hans viktigste lærdommer var at det som var allment kjent som umulig og/eller utenkelig like fullt kan oppstå. Med andre ord: ikke undervurder sorte svaner. Eksempelet hans oppfyller dessuten samtlige av Talebs tre kriterier på en sort svane. Terje Aven trekker frem perfekte stormer som en variant av den sorte svanen. De innebærer at flere kjente trusler inntreffer simultant og forsterker hverandre til den grad at det resulterer i en overraskende ekstremhendelse (Aven, 2022a, s. 53).

Taleb bruker ikke begrepet resiliens som et svar på hvordan man bør håndtere sorte svaner, men han bruker robusthet – et begrep som av noen brukes som et synonym til resiliens. Om det er tilfellet for Taleb skal ikke jeg spekulere i, men han hevder i hvert fall at det blir lettere å håndtere sorte svaner når de dukker opp dersom man øker robustheten overfor feil fremfor å forbedre forutsigelsene som er tenkt å oppdage de sorte svanene før de manifesterer seg (Taleb, 2010, s. xxiv). Jeg oppfatter det slik at han legger den samme tankegangen til grunn for håndteringen av uventede og overraskende hendelser som Hollnagel og Klein. Ett eksempel Taleb bruker for å illustrere hvordan det er mulig å forberede seg på en kjent trussel på feil måte, er den franske Maginot-linjen. Det var et forsvarsverk som franskmennene bygget etter 1. verdenskrig for å motstå en ny tysk invasjon. Da Tyskland invaderte Frankrike i 1940 unngikk de Maginot-linjen ved å invadere via et belgisk skogsområde som var allment antatt å være ufremkommelig for store hærstyrker. Tyskerne gikk rett og slett rundt de franske

forsvarsstillingene og Maginot-linjen var dermed verdiløs (Ibid., s. xxvi). Franskmennene hadde lært av hendelsene under 1. verdenskrig og tok grep for å unngå at fransk territorium igjen skulle bli åsted for harde og langvarige kamper. Løsningen deres var å bygge et kraftig forsvarsverk langs den tyske grensen, men da tyskerne angrep fra en annen kant, og dermed ikke oppførte seg som franskmennene ventet, hadde det planlagte tiltaket (Maginot-linjen) i realiteten bare gjort vondt verre. Etter at tyskerne hadde gått rundt forsvarsverket falt de det i ryggen, erobret det og tok mer enn en halv million soldater som krigsfanger (History.com Editors, 2009). Eksempelets paralleller med argumentene til Klein gjengitt ovenfor er slående.

For at man skal evne å respondere må man som nevnt ha tilstrekkelig kapasitet. Det vil si at man har tilgang til bestemte ressurser for å håndtere situasjonen. Eksempler kan være bemanning, verktøy og materialer. Hva som behøves kan også endre seg i løpet av hendelseshåndteringen. Derfor er det også viktig å styre responsen etter hvert som den skrider frem. Som oftest er responsen sammensatt, krever flere faser og går over tid. I mange tilfeller må man også opprettholde den normale driften ved siden av, om enn med et redusert funksjonsnivå (Hollnagel, 2018, s. 30-31). Hvis en hendelse vurderes som alvorlig nok kan responsen likevel være å endre fra en normal operativ status til en beredskapsstatus eller å ta spesifikke skritt for å håndtere den aktuelle situasjonen. For å agere må man altså enten ha forberedte tiltak med tilstrekkelige ressurser eller ha stor nok fleksibilitet, slik at man klarer å hente frem nok ressurser ved behov (Hollnagel m.fl., 2011, s. 284). Hvilken fremgangsmåte som er mest hensiktsmessig vil som nevnt avhenge av hvilken type situasjon som oppstår.

For å respondere trengs det kjennskap om hva som kan skje. Et system må evne å følge med på det som kan påvirke det både internt og eksternt. Det må evne å overvåke.

3.2.2 Overvåke

Å overvåke det som er eller kan bli en trussel går ut på å vite hva man skal se etter. Overvåkingen må dekke både det som skjer i selve systemet og i dets miljø. Dette er evnen til å håndtere det kritiske (Ibid., s. xxxvii).

Intet system kan være resilient med mindre det fleksibelt evner å overvåke både det som skjer internt (dets egen prestasjon/ytelse) og eksternt (utenfor systemet). Det siste kan også forklares som miljøendringer som kan påvirke systemet. Fleksibiliteten i overvåkingen fordrer jevnlige vurderinger og tilpasninger av dens grunnlag (Ibid., s. 284-285; Hollnagel, 2018, s. 31). Overvåking bedrer oddsen for at et system vil beherske både muligheter og trusler som kan oppstå i nær fremtid. Hvis man responderer i det en hendelse inntreffer kan det hende at det er

for lite og for sent. Effektiv styring krever at man klarer å respondere selv overfor små forandringer og å oppdage og gjenkjenne tendenser som kan være for små til å representere en reell endring, men som likevel kan medføre alvorlige konsekvenser. Ikke minst dersom situasjonen senere utvikler seg til en større hendelse. For at overvåkingen skal være effektiv må den være proaktiv. Det vil si at den må kunne gjenkjenne kommende hendelser og benytte seg av de viktigste kjennetegnene (Hollnagel, 2018, s. 31). Systemer som ikke utfører noen former for overvåking vil til enhver tid bli tatt på senga, fordi alle hendelser vil komme som overraskelser (Ibid., s. 33).

I motsetning til de tre øvrige kjennetegnene på et resilient system – respondere, forvente og lære – må overvåking foregå kontinuerlig, om enn i varierende grad. Under spesielle forhold og forutsetninger kan for eksempel overvåkingen måtte intensiveres. Det er også viktig å vite hva man skal overvåke og hvorfor. Dersom man ikke skjønner det som overvåkes vil overvåkingen ha liten eller ingen verdi. I så fall vil ressursene man bruker på å gjennomføre overvåkingen være mer eller mindre bortkastet (Ibid., s. 34).

Hensikten med overvåking er enten å utløse en respons eller å få systemet over i en ny tilstand ved behov (Ibid.). Mulige negative ringvirkninger av overvåking er at det åpner for at responsen kommer for tidlig, altså før noen respons er nødvendig, og at den valgte responsen er feil. På den andre siden kan det å vente til at man er helt sikker føre til at responsen er for sen, med de konsekvenser det bringer med seg (Ibid., s. 35). Klein påpeker at å vente til man er sikker før man hopper til konklusjoner – i dette tilfellet agerer – blant annet medfører passivitet (Klein, 2009, s. 151). Det kan fungere i oversiktlige situasjoner hvor tidligere erfaringer hjelper til med å forstå informasjonsflyten. Da vet man sånn cirka hvor mye informasjon man behøver før man responderer, men i komplekse og uoversiktlige situasjoner er det ikke gitt at man vet når man har tilstrekkelig med informasjon (Ibid., s. 154). Derfor bør man forsøke å forutse hvordan tvetydige situasjoner kan utvikle seg, som av Lipshitz og Strauss (1997) omtales som antakelsesbasert vurdering (s. 153). Det vil dessuten bidra til å overvåke situasjonen, siden oppmerksomheten i større grad vil være rettet mot områdene hvor det er mest sannsynlig at avvikene manifesterer seg og de kan lettere oppdages hvis de oppstår (Klein, 2009, s. 158-159). Overvåking av komplekse og tvetydige situasjoner må med andre ord ikke forstås som noe passiviserende i påvente av stadig ny og oppdatert informasjon. I slike tilfeller må overvåkingen komme i tillegg til proaktive skritt, som evnen til å forutse hvordan en situasjon kan utvikle seg og ta grep på bakgrunn av det (Ibid., s. 163).

Å overvåke det som kan skje i nær fremtid og nåtid er en sentral del av et resilient system. Likeledes gjelder det over et lengre tidsperspektiv. Da er det snakk om hva man kan forvente.

3.2.3 Forvente

Å forutse hvilke utviklinger, trusler og muligheter som kan oppstå i et lengre tidsperspektiv, er å vite hva man kan forvente. Dette er evnen til å håndtere det potensielle (Hollnagel m.fl., 2011, s. xxxvii). Mens overvåkingen tar for seg det samtidige og den nære fremtiden, handler det å forvente om å se inn i den fjernere fremtiden for å lete etter og avdekke mulige fremtidige hendelser, tilstander eller andre endringer som kan påvirke systemets ytelsesevne i både positiv og negativ forstand (Ibid., s. 286). Hensikten for de to kjennetegnene på et resilient system er det samme: å orientere seg og forstå hva som foregår på innsiden og utsiden av systemet (Hollnagel, 2018, s. 42). Der hvor overvåking handler om det som kan skje innenfor rammene av de pågående aktivitetene, går forventning ut på å se utover det. Det kan enten gjøres i tid eller ved å se på noe uten direkte tilknytning til eller påvirkning på systemet. Hollnagel oppsummerer forskjellen ved å bemerke at å overvåke er å se på noe, mens å forvente er å tenke på eller forestille seg noe (Ibid., s. 43).

Det er vanligvis to måter organisasjoner ser inn i fremtiden på og som på overflaten ligner på det å forvente: planlegging og risikoanalyser.

Planlegging styrer hvordan en organisasjon og et system oppfører seg på. Man tenker gjennom og organiserer detaljene ved en aktivitet før de finner sted. Med andre ord tar planlegging for seg noe som konkret skal skje. Dermed skiller planlegging seg fra forventning, siden forventning handler om noe hypotetisk, noe som kan skje. De er også forskjellige i den forstand at planlegging tar utgangspunkt i systemets nåværende tilstand og er slik sett en videreføring av det som skjer i samtiden. Forventning har derimot ikke det samme utgangspunktet. Poenget med forventning er å se for seg alternative scenarioer og tenke seg til hvordan man kan håndtere en helt forandret situasjon (Ibid.). Dessuten ligger det i planleggingens natur at de planene som legges skal føre frem til et konkret og ønsket utfall. Planleggingen har med andre ord et tydelig mål. Selv om det er fordelaktig å sette seg et mål før enhver aktivitet, kan det i komplekse og tvetydige situasjoner virke mot sin hensikt (Klein, 2009, s. 207-208). Hvis målsetningen viser seg å være ufullstendig og er i konstant endring blir man stående overfor det som er kjent som et slemt problem (*wicked problem*). Det innebærer at problemet er vanskelig å beskrive, har flere gjensidige avhengige årsaker og ikke har et riktig

svar. Det eneste man vet med sikkerhet i møte med slemme problemer er at det vil komme overraskelser (Martin, 2019, s. 42). Fordi løsningene på et slemt problem ikke har noen fasit, er det heller ikke mulig å teste løsningene objektivt. De forstås i stedet som (mindre) gode eller (mindre) dårlige. Derfor finnes det heller ingen objektiv måte å måle graden av suksess for den valgte løsningen. Dette er et prima eksempel på en problemtype som befinner seg i skyggene. Et slemt problem vil gjøre det vanskelig, om ikke umulig, å definere en målsetning innledningsvis i planleggingen, men det kan bli tydeligere underveis i prosessen (Klein, 2009, s. 212-213). For å imøtegå slemme problemer, trekker Klein også her frem styring gjennom oppdagelse, hvor man reviderer og erstatter målsetninger etter hvert som man lærer seg mer om problemet (Ibid., s. 223-224). Ved å ha tydelige definerte mål i starten av en prosess, slik man har i planlegging, mister man noe av evnen til å tilpasse seg og man må være i stand til tilpasning i situasjoner som bærer preg av kompleksitet og tvetydighet (Ibid., s. 228). Dette handler også om evnen til å se for seg alternative scenarioer og finne ut av hvordan man kan håndtere en situasjon som ser helt annerledes ut enn den gjør i dag.

Som tidligere nevnt er hensikten med risikoanalyser å identifisere forhold eller hendelser som kan medføre negative konsekvenser for et system. Det som er verdt å legge til her er at risikoanalyser, og for så vidt beredskapsarbeid generelt, fungerer godt i tilfeller hvor systemets funksjoner er godt kjente, miljøet er stabilt over tid osv., altså det Klein refererer til som *streetlights*. Organisasjoner og systemer befinner seg i stadig mindre grad i forhold som samsvarer med slike. Derimot blir forholdene mer uhåndterlige og ligner i stadig større grad på forhold som ifølge Klein befinner seg i skyggene. Under slike forhold blir tradisjonelle risikoanalyser utilstrekkelige og kan i verste fall ha negativ innvirkning. I motsetning til forventning vil en risikoanalyse være begrenset av hvordan systemets funksjoner er beskrevet. Dessuten fokuserer risikoanalyser på det som kan gå galt, men de har ingen metoder for å vurdere fremtidige muligheter, som er vel så viktig som å avdekke fremtidige trusler (Hollnagel, 2018, s. 43-44). Med andre ord er forventning et bredere konsept enn det som er iboende i planlegging og risikoanalyser. Forventning starter med en aksept for at man behøver å være forberedt. Fremtiden er usikker og derfor må man vurdere hvilke forberedelser som kan være nødvendige (Ibid., s. 45-46). Det er eksempelvis en fordel å ivareta personlige og profesjonelle forhold i og med at det er for sent å utvikle dem når krisen eller den uønskede hendelsen allerede er et faktum. Kortsiktige omstruktureringer og andre kostnadsbesparende tiltak kan bryte opp uformelle nettverk og følgelig bidra til å redusere organisatorisk resiliens (Martin, 2019, s. 92).

Målsetningen for forventning er at det skal skape prioriteringsområder eller andre mulige fokusområder. Produktet av forventning representerer ideene om fremtidig utvikling og

hvordan de fremtidige forholdene kan påvirke organisasjonens eller systemets levevilkår og ytelse (Hollnagel, 2018, s. 46).

I likhet med å overvåke, foregår forventning i forkant av responsfasen med et mål om å forbedre denne. En annen fase som også tar sikte på å forbedre responsen, men som foregår i etterkant av den er det å lære.

3.2.4 Lære

Å lære av erfaring, og helst hvordan man skal trekke riktig lærdom ut fra den rette erfaringen, er å vite hva som har skjedd. Dette er evnen til å håndtere det faktiske (Hollnagel m.fl., 2011, s. xxxvii). Læring kan forstås som måter en organisasjon eller et system endrer eller anskaffer seg nye kunnskaper, kompetanser og ferdigheter. Det er en aktiv utviklingsprosess fremfor en passiv samling av fakta og kunnskap. Potensialet til å lære er avgjørende for et resilient system, også fordi potensialet til både å respondere og overvåke avhenger av læring. De eneste unntakene er i tilfeller hvor miljøet systemet opererer i er helt stabilt og forutsigbart (Hollnagel, 2018, s. 36).

Det finnes mange typer læring. En type er såkalt fremvoksende læring som er et biprodukt av at man håndterer og løser umiddelbare problemer etter hvert som de oppstår (Steen og Rønningsbakk, 2021). Å lære av andre innebærer en overføring av kunnskap mellom personer (Moskaliuk m.fl., 2016). Det gjøres også skiller mellom læringsformer, for eksempel mellom strukturell og kulturell læring, hvor den strukturelle refererer til de institusjonaliserte strukturelle ordningene som er på plass for å samle og bearbeide informasjon og den kulturelle viser til de kulturelle aspektene som påvirker den organisatoriske læringskapasiteten (Popper og Lipshitz, 1998). Eksempler på slike er felles verdier og normer. Dette er et lite utvalg av måter å lære på. Hensikten med læring, uavhengig av hvordan den foregår, er å skape og overføre kunnskaper, kompetanser og ferdigheter i det henseende å forsterke evnen til å håndtere fremtidige utfordringer (Steen m.fl., 2023, s. 3).

Hvor effektiv læringen er kommer an på hvilke hendelser og erfaringer som tas med i betraktningen, samt hvordan hendelsene blir analysert og forstått. I den sammenhengen er det viktig å skille mellom det som er enkelt å lære og det som er meningsfullt å lære. Det er langt viktigere å vite hvorfor noe skjedde i stedet for hvor ofte det hendte (Hollnagel, 2018, s. 36-37).

I sikkerhetsstyring har man tradisjonelt prioritert å lære fra hendelser med negative konsekvenser, både fordi de tiltrekker seg oppmerksomhet og fordi de gir grunn til bekymring.

Den tankegangen blir ofte forlenget ved at man antar at jo alvorligere en hendelse er, jo viktigere er det å lære av den og jo mer er det mulig å lære av den. Større ulykker og katastrofer er sjeldne. Det betyr at det er få hendelser å trekke lærdom fra. Derfor øker læringsgrunnlaget dersom man utvider horisonten til ikke bare å inkludere mindre uhell og nestenulykker, men også hendelser som ikke faller inn under ulykkekategorien i det hele tatt. Ettersom andelen hendelser som ender godt er mange ganger større enn antallet hendelser som går galt, mener Hollnagel at det er bedre å lære av hendelser som er representative i form av deres frekvens fremfor å basere læringen på hendelser som skaper bekymring på grunn av konsekvensenes alvorlighetsgrad. Hvis læringen tar utgangspunkt i det som skjer ofte, altså vanlig arbeid og aktiviteter, må den også foregå kontinuerlig i stedet for å være en reaksjon på en alvorlig enkelthendelse (Ibid., s. 37). For at læringen skal være effektiv må det foreligge tilstrekkelige læringsmuligheter, hendelsene må ha en viss grad av likhet og det må være mulig å bekrefte at noe har blitt lært. Læring innebærer en endring i oppførsel som gjør enkelte utfall mer sannsynlige og andre mindre sannsynlige. Derfor er det viktig å lære av alle representative hendelser fremfor kun de hendelsene der noe gikk galt (Hollnagel m.fl., 2011, s. 287-288). Dette fremgår også av definisjonen på resiliens jeg gjenga tidligere, hvor Hollnagel selv fremhever at muligheter er inkludert i definisjonen på lik linje med endringer og forstyrrelser (Hollnagel, 2018, s. 15). Dette er et viktig aspekt ved resiliens. Å trekke ut lærdom fra kriser og andre uønskede hendelser er vel og bra, men for å få en bredere forståelse av konteksten man arbeider i understreker resiliens viktigheten av også å lære av det som fungerte godt. Hvis en uønsket hendelse oppstår vil det å lære hva som fungerte, ikke fungerte og hva i beredskapsplanene som kunne vært forandret sett i lys av innsatsen i den akutte krisefasen, forbedre en organisasjons evne til å opprettholde sin krisehåndtering (Steen m.fl., 2023, s. 4). Resiliens kan bygges opp ved aktivt å lære av erfaring, slik at man gradvis blir sterkere over tid. Det er hjørnesteinen i det Martin kaller aktiv resiliens (Martin, 2019, s. 89-90) og som langt på vei samsvarer med ideen om at resiliens er noe et system gjør og ikke noe det har (Hollnagel m.fl., 2011, s. 275).

Læring er dessuten tid- og ressurskrevende. Det betyr at organisasjonen må prioritere og tilrettelegge for at den skal kunne finne sted. Det trengs både kompetente ansatte og en kompetent ledelse. Noen må samle inn informasjon, analysere den, trekke konklusjoner på bakgrunn av analysen og formulere hvordan det man har lært best kan tas i bruk i praksis. Erfaringene må deretter brukes som grunnlag for å gjennomføre passende endringer i organisasjonen eller systemet. Hvilke endringer som blir innført vil påvirke hvor lang tid det tar før de i realiteten er implementerte. Noen endringer vil ha tilnærmet umiddelbar effekt, for eksempel utskifting av utstyr, mens andre kan bruke mye lenger tid før de manifesterer seg. Det

kan eksempelvis gjelde hvis endringen tar tid eller fordi man må vente på at en lignende situasjon oppstår på nytt (Hollnagel, 2018, s. 39-40).

En fallgruve som kan føre til at man ikke lærer noe som helst kan være at hovedfokuset er rettet mot kortsiktig produktivitet og effektivitet. Det oppmuntrer til det Hollnagel kaller en «reparer-og-glem»-taktikk. Velger folk å reparere og glemme når de står overfor et problem? Reparerer, rapporterer og glemmer de problemet? Eller velger de reparere, rapportere og forsøke å lære av det? Det er den sistnevnte løsningen som er den beste og er også den eneste som samsvarer med et forebyggende sikkerhetsperspektiv (Ibid., s. 40).

Læring foregår i etterkant av hendelser, uansett hvilke hendelser som velges ut i det øyemed, og er som nevnt det eneste kjennetegnet på et resilient system som skjer på det tidspunktet. Responsfasen foregår i det en situasjon eller hendelse utspiller seg, mens overvåkings- og forventningsfasene utføres i forkant av responsen. Derfor er det verdt å ta en kjapp titt på hvordan samspillet mellom de fire kjennetegnene fungerer.

3.2.5 Samspillet mellom de fire kjennetegnene

Som Figur IX under viser, fører alle veier til responsfasen. De tre andre kjennetegnene er ment å underbygge og forbedre hendelseshåndteringen som foregår i den fasen. Læringsfasen skjer som sagt i etterkant og skal bedre systemets ytelse og responsfasen. Av figuren ser vi at læringen peker direkte på responsen. Det samme gjør overvåkingen. I overvåkingsfasen forsøker man å få oversikt over det som kan påvirke systemet sett i en kort tidshorisont enten det skjer på innsiden eller utenfor og uansett om det vil medføre negative eller positive ringvirkninger. Hvis man forsøker å skaffe seg oversikt over det som kan skje i et lengre tidsperspektiv er vi i forventningsfasen. Ifølge figuren peker den rett på overvåkingsfasen. Det som skjer når vi forventer og forutser hva som kan påvirke systemet på lang sikt har direkte innvirkning på det vi søker å få oversikt over under overvåkingen. Forventningen peker følgelig indirekte til responsfasen, men altså via overvåkingen.

Figur IX speiler samspillet mellom de fire faktorene som utgjør hjørnesteinene innen resiliens (tegningen er basert på figuren i Hollnagel m.fl., 2011, s. xxxvii).

Figur IX. De fire hjørnesteinene innen resiliens.

Blant de nyere tilskuddene til hvordan man kan forbedre resiliens innen alle de fire kjennetegnene er DARWIN Resilience Management Guidelines (DRMG), som er dreiepunktet for denne oppgaven.

3.3 DARWIN Resilience Management Guidelines (DRMG)

DRMG er resultatet av et EU-støttet forskningsprosjekt som varte mellom 2015 og 2018. Hensikten var å forbedre responsen overfor både ventede og uventede kriser som rammer kritiske samfunnsstrukturer i form av naturlige og menneskeskapte hendelser, samt å tilby de som drifter de ulike infrastrukturene med oppdaterte og effektive retningslinjer for raskere, mer effektiv og svært tilpasningsdyktige responsmekanismer til kriser. Prosjektet ble koordinert av SINTEF (Selskapet for industriell og teknisk forskning ved Norges tekniske høgskole), som er tilknyttet Norges teknisk-naturvitenskapelige universitetet (NTNU). De øvrige deltakerne i prosjektet kom fra Tyskland, Irland, Italia, Israel og Sverige (DARWIN, u.å.).

Retningslinjene som ble utarbeidet gjennom forskningsprosjektet består av veiledende prinsipper som skal bistå en bestemt organisasjon i opprettelsen, vurderingen eller forbedringen av sine egne retningslinjer og kan forstås som et hjelpemiddel for å vurdere en organisasjons evne til kontinuerlig forbedring (Steen m.fl., 2023, s. 2). Prinsippene er ment å hjelpe organisasjonen med å utvikle et kritisk blikk på krisehåndteringsaktivitetene hos dem selv, som håndteringen av ressurser, prosedyrer, trening og lignende på bakgrunn av konsepter innen resiliens. En organisasjon i denne sammenhengen forstås som offentlige og private selskaper, myndigheter eller offentlige etater på lokalt, nasjonalt og/eller internasjonalt nivå. Hovedmålgruppen er likevel beslutningstakere og ledere på ulike nivåer i organisasjonen. De som arbeider i den skarpe enden benytter seg av de retningslinjene, prosedyrene og praksisene

som utformes ved hjelp av DRMG. Dessuten er retningslinjene ment å supplere, ikke erstatte, allerede eksisterende retningslinjer, prosedyrer og praksiser. Antakelsen som ligger til grunn for den vurderingen er at den nødvendige kunnskapen og kompetansen for å etablere organisasjonsspesifikke retningslinjer ligger hos hver enkelt organisasjon. Følgelig er ikke retningslinjene en oppskrift man følger for å oppnå ønsket resultat, men de må tolkes inn i den spesifikke konteksten hvor de skal brukes og må tilpasses de spesifikke målsetningene og karakteristikkene til organisasjonen som benytter seg av dem (DARWIN, 2018, s. 11). Eksempler på områder hvor det har blitt gjort bruk av DRMG inkluderer luftfart og helsetjeneste (Cedrini m.fl., 2018), katastrofemedisin (Hermelin m.fl., 2020) og beredskapsoperasjoner i Nordsjøen (Steen m.fl., 2023). Tabell IV gir en oversikt over temaene og de tilhørende emnene i DRMG og er oversatt med utgangspunkt i DARWIN (2018), s. 5.

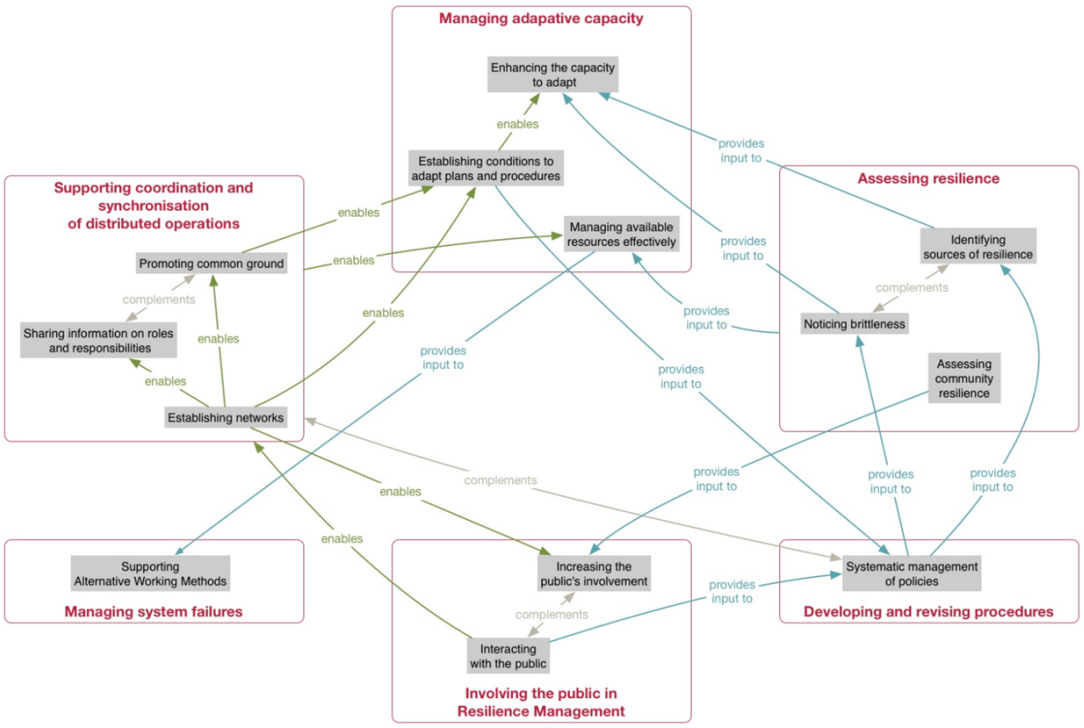
Tabell IV. DRMG-temaer og -emner.

DRMG-temaer	DRMG-emner
Støtte koordinering og synkronisering av fordelte oppgaver	• Fremme felles forståelse for tverrorganisatorisk samarbeid i krisehåndtering. • Etablere nettverk for å fremme interorganisatorisk samarbeid i krisehåndtering. • Dele informasjon om roller og ansvarsområder blant organisasjonene involvert i krisehåndteringen.
Styring av adaptiv kapasitet	• Forsterke kapasiteten for å tilpasse seg overfor både ventede og uventende hendelser. • Etablere forhold for planer og prosedyrer som tilpasser seg under kriser og andre hendelser som utfordrer normale planer og prosedyrer. • Styre de tilgjengelige ressursene effektivt for å håndtere endrede krav.
Vurdering av resiliens	• Vurdere samfunnets resiliens for å forstå og utvikle dets kapasitet til krisehåndtering. • Identifisere kildene til resiliens: å lære av det som fungerer. • Å legge merke til skjørhet.
Utvikle og revidere prosedyrer og sjekklister	• Systematisk styring av politikk som involverer beslutningstakere og operativt personell i forbindelse med håndteringen av nødsituasjoner og forstyrrelser.
Involvere offentligheten i resiliensstyringen	• Kommunikasjonsstrategier for å samhandle med offentligheten. • Øke hvor involvert offentligheten er i resiliensstyringen.
Håndtere systemfeil	• Støtte utviklingen og vedlikeholdet av alternative arbeidsmetoder.

3.3.1 Kapabilitetskort

Totalt inneholder DRMG tretten resiliensstyringskapabiliteter fordelt på seks hovedtemaer. En oversikt over dem finnes i Tabell IV ovenfor. Hver enkelt kapabilitet representeres av et kapabilitetskort (engelsk: *Capability Card*, forkortet som CC). Retningslinjene bygger på

kapabilitetskortene. Disse er organisert og satt inn i en sammenheng sett overfor hverandre, ettersom resiliensstyringskapabilitet ikke er uavhengig av hverandre. Derfor samhandler kortene med hverandre på ulikt vis. Enkelte kapabilitetskort muliggjør andre (*enables*). Det vil si at de må utføres i en bestemt rekkefølge. Det vil for eksempel ikke være mulig å fremme felles forståelse før det har blitt etablert et nettverk. I andre tilfeller mater kortene informasjon til hverandre (*provides input to*), slik at informasjonen som er samlet inn gjennom arbeidet med ett kapabilitetskort kan brukes i arbeidet med et annet. Å involvere offentligheten i resiliensstyringen kan for eksempel føre til endringer i synet på den systematiske styringen av politikk. Kortene kan også komplementere hverandre (*complements*). Da beriker to kapabilitetskort hverandre, som ved at kortene for å oppdage skjørhet og identifisere resilienskilder er til gjensidig nytte (Branlat, 2018, s. 21). Figur X viser et kart med en oversikt over hvordan forholdene og samhandlingene mellom de ulike kapabilitetskortene er (DARWIN, 2018, s. 12).



Figur X. DRMG-kart.

Kapabilitetskortene foreslår inngrep som kan iverksettes for å oppnå de kapabilitetene som foreskrives av krisehåndteringspraksis og vitenskapelig litteratur. Hvert kort består av et sett med informasjonsdeler som støtter opp om forståelsen og implementeringen av de foreslåtte

inngrepene. Følgende innholdselementer er oppgitt for kortene: (1) bakgrunnsinformasjon; (2) beskrivelse av inngrepene; og (3) informasjonskategorisering (DARWIN, 2018, s. 11-12).

Bakgrunnsinformasjonen beskriver målsetningene og begrunnelsen som ligger til grunn for den resiliensstyringskapabiliteten som er benyttet, i tillegg til tilknyttede fordeler, utfordringer og aktører i krisehåndteringen (Ibid., s. 11-12).

Beskrivelse av inngrepene, organisert av krisehåndteringsfasene, inkluderer ofte «utløsende spørsmål» hvis mål er å fange opp essensielle problemer brukerne bør tenke gjennom eller forsøke å adressere. Spørsmålene er også ment å hjelpe brukerne til å ta i bruk et resiliensorientert perspektiv, som kan være litt annerledes enn tradisjonelle syn på risiko og sikkerhet. Inngrepene viser til strategier, metoder, verktøy og praksiser som er hentet fra litteratur eller erfaring, og som legges kortfattet frem. Dette vil typisk være hovedelementer ved implementeringen, kapabilitetskortenes relevans og referanser til eksterne kilder for tilleggsinformasjon. Når det er mulig bruker kapabilitetskortene malende eksempler og hint for å gi ytterligere veiledning, anslå teknologimodenhet på en TRL-skala (*Technology Readiness Level*, se Innovasjon Norge, 2021 for et eksempel på en slik skala) og diskusjon rundt implementeringskostnader (Ibid., s. 12).

Informasjonskategorisering knytter kapabilitetskortene opp mot andre temaer, kategorier, resiliensevner, krisehåndteringsfunksjoner og type aktører. Vanligvis er kortene tilknyttet flere elementer i hver kategori, som fungerer mer som en slags merking enn en hard klassifisering. Et viktig formål med informasjonskategoriseringen er å være en navigeringsmekanisme og foreslå relatert innhold for å tilrettelegge for implementeringen av kapabilitetskortene i sammenheng med de generelle retningslinjene. Av samme grunn blir forholdene til andre kapabilitetskort oppgitt når det er relevant (Ibid.).

Som nevnt i kapittel 1 fokuserer denne oppgaven på to hovedtemaer fordelt på tre tilhørende kapabilitetskort. De er:

1) Støtte koordinering og synkronisering av fordelte oppgaver
    a. Fremme felles forståelse for tverrorganisatorisk samarbeid i krisehåndtering
    b. Dele informasjon om roller og ansvarsområder blant organisasjonene involvert i krisehåndteringen
2) Styring av adaptiv kapasitet
    c. Forsterke kapasiteten for å tilpasse seg overfor både ventede og uventede hendelser

3.3.2 Fremme felles forståelse for tverrorganisatorisk samarbeid i krisehåndtering

Kapabilitetskortet for å fremme felles forståelse for tverrorganisatorisk samarbeid i krisehåndtering baserer seg på at kortet for nettverksetablering for å fremme interorganisatorisk samarbeid allerede er iverksatt (se Figur X for forholdet mellom de to kortene). Utgangspunktet mitt var at Beredskapsutvalget for finansiell infrastruktur (BFI) er å regne som den nødvendige forløperen for å fremme felles forståelse og at kriteriet for å vurdere den felles forståelsen på tvers av organisasjonene involvert i krisehåndteringen følgelig er oppfylt. Hvorvidt det faktisk stemmer er gjenstand for diskusjon i kapittel 6.1, men det var grunnlaget for valget av dette kapabilitetskortet. Det ble gjort til tross for at det, etter hva jeg vet, ikke er gjort noen studier for å kartlegge i hvilken grad driften av BFI samsvarer med retningslinjene i DARWIN.

Kortet for å fremme felles forståelse for tverrorganisatorisk samarbeid i krisehåndtering vektlegger periodiske tverrorganisatoriske formidlingsøvelser som en måte å øke de involverte organisasjonenes felles bevissthet om de andres motiver, perspektiver, terminologier og arbeidspraksiser. Hensikten er at dette kan tilrettelegge for et forbedret samarbeid når kriser inntreffer, ettersom partene da er mer bevisste på hvilken oppførsel de kan forvente fra ansatte hos de andre involverte aktørene (Ibid., s. 13). Målsetningen er dermed at den felles innsatsen for å håndtere krisen skal bli bedre enn den ellers ville vært (Ibid., s. 18).

I bunn og grunn er det de samme anbefalingene som legges frem for både før- og etterkrisefasen. I den akutte krisefasen vil fasens varighet være avgjørende for hvorvidt de involverte bør ta seg tid til å fremme felles forståelse. Jo lenger tid krisen varer, jo viktigere blir det å fremme felles forståelse på tvers av organisasjoner, men det må ikke gå på bekostning av de aktivitetene som utføres for å håndtere krisen (Ibid., s. 16).

Det mest fordelaktige er å fremme gjensidig forståelse i førkrisefasen. Da er ikke de ulike organisasjonenes ledere farget av tolkningene av hendelsene som oppstod under forrige krise og er mindre bekymrede med tanke på å dele informasjon som kan bli brukt for å fordele skyld for tidligere hendelser. På den andre siden kan det være vanskelig å rettferdiggjøre ressursbruk på å fremme felles forståelse uten at det har skjedd noe bekymringsverdig (Ibid., s. 14). Den største fordelen med å fremme felles forståelse i etterkrisefasen, foruten at det sannsynligvis er lettere å rettferdiggjøre ressursbruken på det, er at det man har lært i løpet av krisen kan fungere som en veileder for både å identifisere sprik i den felles forståelsen og de koordineringspraksisene som fungerte godt. Samtidig er det viktig å understreke at det er en fare for at arbeidet i etterkrisefasen blir for spesifikt rettet inn mot den nylig avsluttede krisen,

slik at læringspunktene i mindre grad blir allmenngyldige og brukbare i den neste krisen (Ibid., s. 16-17).

For å fremme felles forståelse er det anbefalt at man først identifiserer mulige sprik mellom ens egen organisasjon og de organisasjonene man samarbeider med. Deretter bør en eller flere av følgende tiltak gjennomføres (Ibid., s. 14-15):

1. Organisere workshops for informasjonsdeling: Hensikten er at en organisasjons ansatte skal få anledning til å få innsikt i oppdraget, kulturen og hvordan andre organisasjoner som deltar i krisehåndteringen opererer. Dette kan gjøres ved å invitere ansatte i andre organisasjoner til å:
    a. overvære presentasjoner om det organisatoriske oppdraget, ressursene, avhengighetene og forventingene til andre organisasjoner og arbeidsmetodene og praksisene hos ens egen organisasjon.
    b. presentere det samme for de ansatte i ens egen organisasjon.
2. Organisere at egne ansatte periodisk besøker andre organisasjoner, slik at de får muligheten til å lære om ressursene og prosedyrene hos relevante organisasjoner. På samme måte la andre organisasjoners ansatte besøke egen organisasjon.
3. Organisere felles kriseforberedelsesøvelser for å avdekke mulige kilder for brudd i felles aktiviteter, for eksempel bruk av terminologi som kan være uklar eller tvetydig for andre organisasjoner eller konflikter i ressursbruk.

Foruten å bidra til identifisering av mulige fallgruver, kan de også øke kunnskapen organisasjonene har om hverandres kapasiteter og ressurser, slik at de kan avlaste hverandre i tilfeller hvor en organisasjon mangler de nødvendige ressursene for å håndtere krisen (Ibid., s. 15).

3.3.3 Dele informasjon om roller og ansvarsområder blant organisasjonene involvert i krisehåndteringen

I likhet med kapabilitetskortet for å fremme felles forståelse, legger kortet for å dele informasjon om roller og ansvarsområder til grunn at det allerede finnes et nettverk som fremmer interorganisatorisk samarbeid. Som nevnt fyller BFI offisielt den rollen og muliggjør dermed også dette kapabilitetskortet.

På generelt grunnlag fremhever kortet at det er essensielt at partene har god nok kjennskap om tre bestemte aspekter (Ibid., s. 34):

1. Hvem som må kontaktes under en krise.
2. Hva som er de relevante rollene for håndteringen av både generiske og spesifikke former for kriser.
3. Hvilke ansvarsområder som er de viktigste for disse rollene, slik at man får en klar og tydelig forventning om hvordan man skal samhandle med dem.

Hensikten med dette kortet er med andre ord å fremheve at aktørene som deltar i styringen av resiliens må vite hvilke roller og ansvarsområder ulike parter involvert i krisehåndteringen faktisk har. Altså bør de involverte organisasjonene besitte tilstrekkelig kunnskap om hvilke roller og ansvarsområder deres egen organisasjon har, samtidig som de også er kjent med rollene og ansvarsområdene til organisasjonene de samarbeider med under en krise har. På den måten blir det lettere å oppdage eventuelle hull i krisehåndteringen og tilrettelegge for bedre samarbeid før, under og etter kriser (Ibid., s. 13). Målsetningen er at dette skal resultere i en mer effektiv demping av krisens effekter og en raskere normalisering av situasjonen (Ibid., s. 39).

Kortet inneholder følgelig retningslinjer for hvordan tilretteleggingen av informasjonsdelingen bør foregå før, under og etter kriser. Slik forskningsspørsmålet knyttet til dette kortet er formulert skal jeg se spesifikt på aktiviteten under og etter bortfallet av betalingsterminaler 16. mai 2022. I den følgende gjennomgangen er det som kommer frem av anbefalinger og forslag for både førkrisefasen og den akutte krisefasen å anse som bakgrunnsinformasjon. Det er etterkrisefasen som er av størst interesse for denne oppgaven og det som skjedde i selve krisehåndteringen må i denne sammenhengen forstås i lys av at hvordan innsatsen ble brukt for å utbedre informasjonsdelingen. Derfor behandler jeg alle tre krisefasene for kortet her og noe av det gjør jeg bruk av i drøftingen i kapittel 6.2, men det er kun etterkrisefasen som får en fullverdig vurdering.

Før en krise oppstår tar kortet til orde for at det bør finnes prosedyrer som spesifiserer hvem som skal ta initiativ når det er behov for å koordinere innsatsen mellom flere organisasjoner. Dette innebærer at det er flere handlinger som bør være utført forut for en krise:

1. Identifisere organisasjoner med delte ansvarsområder under krisehåndteringen.
2. Organisere periodiske koordineringsmøter mellom organisasjonene som tar for seg:

    a. Hvilke roller som kan kontaktes innen hver organisasjon for å koordinere håndteringen av både generiske og spesifikke kriser.
    b. Hvilke ansvarsområder disse rolleinnehaverne har.
    c. Hvordan rolleinnehaverne kan bli kontaktet.
    d. Hvilke kommunikasjonsmidler som bør brukes.
    e. Hva som er den mest oppdaterte terminologien for å indikere rollene og å beskrive ansvarsområdene deres.
3. Sørge for at minst en representant fra hver organisasjon deltar på koordineringsmøtene og at hver organisasjon har en kontaktperson som håndterer den koordineringen.
4. Sørge for at kontaktpersonene arrangerer interne oppdateringsaktiviteter i egen organisasjon etter hvert koordineringsmøte.
5. Ordne det slik at store endringer som påvirker prosedyrene for nødsituasjoner i hver organisasjon blir vurdert for hvilke ringvirkninger det kan ha for samhandlingen med andre organisasjoner og formidle dette til relevante mottakere.
6. Hvis det er mulig bør hver organisasjon lage en hurtigreferanseguide av prosedyrene som er simplifisert og tilpasset til de spesifikke behovene til den aktuelle organisasjonen. Dette anbefales kun i kontekster hvor forholdene er relativt stabile over tid og ikke er i rask endring. (Ibid., s. 34-35).

Dersom prosessen i førkrisefasen lykkes, bør de ansatte i hver organisasjon være klare for å reagere effektivt og antallet misforståelser og feiltolkninger om roller og ansvarsområder til egen og andres organisasjoner bli redusert. Underveis i krisen anbefales det å gjøre følgende:

1. Utføre krisehåndteringen mens man tar informasjonen og/eller opplæringen man har fått gjennom de interne oppdateringsaktivitetene om roller og ansvarsområder hos andre organisasjoner involvert i krisehåndteringen.
2. Bruke hurtigreferanseguiden for lett å finne frem til relevante roller og ansvarsområder for de involverte organisasjonene hvis den er tilgjengelig. (Ibid., s. 36).

I kjølvannet av en krise er det en gyllen mulighet for å gjennomgå alle rutiner og prosedyrer som ble delt mellom de involverte partene. Etter en krise er følgende handlinger nødvendige (Ibid., s. 37):

1. Å organisere ekstraordinære koordineringsaktiviteter utover de som er planlagte til vanlig, for å vurdere de felles prosedyrene og oppdatere de viktigste rolle- og ansvarsområdene for hver organisasjon etter behov.
2. Vurdere hvorvidt nye organisasjoner bør inkluderes i de delte prosedyrene og de periodiske koordineringsmekanismene. Eventuelt om enkelte organisasjoner som har mistet relevansen sin i prosedyrene bør fjernes.

Dette vil kunne bidra til å gjøre samtlige involverte bedre rustet for den nye førkrisefasen, som følger etter at den foregående krisens etterkrisefase er over.

3.3.4 Forsterke kapasiteten for å tilpasse seg overfor både ventede og uventede hendelser

Som DRMG-kartet i Figur X viser krever kapabilitetskortet for å forsterke kapasiteten for å tilpasse seg flere forløpere, deriblant å fremme felles forståelse. Det får også viktige innspill fra andre kort, for eksempel å oppdage skjørhet – et kort som ikke er valgt ut til denne oppgaven. I motsetning til de to foregående kortene har jeg få forutsetninger for å vite om kriteriene som muliggjør å forsterke kapasiteten for å tilpasse overfor både ventede og uventede hendelser er på plass. Det er nemlig et ledd mellom å fremme felles forståelse og å forsterke kapasiteten for tilpasning: etablering av forhold for planer og prosedyrer som tilpasser seg under kriser og andre hendelser som utfordrer normale planer og prosedyrer. Det kortet utforskes ikke her, men jeg legger til grunn at det til en viss grad er oppnådd. Ikke minst på bakgrunn av at det i regi av BFI avholdes minimum en felles beredskapsøvelse i året, slik at det er grunn til å anta at elementer som autoritet og kapabilitet, som er sentrale for mellomleddet (Ibid., s. 56), langt på vei er avklart på et generelt grunnlag.

Utgangspunktet for kapabilitetskortet som går ut på å forsterke kapasiteten for å tilpasse seg overfor både ventede og uventede hendelser er at nødsituasjoner kan oppstå plutselig og uten varsel. Derfor må organisasjoner være forberedte og evne å tilpasse sine funksjoner slik at de responderer på nødsituasjoner så raskt som mulig. Enkelte nødsituasjoner kan være ventede, mens andre kan være uventede. Roller, trening, strategier og prosedyrer må være innrettet for å oppnå den ønskede kapasiteten ved å ta i bruk en «all-hazard»-tilnærming, som tar inn over seg nødsituasjonens fellesnevner på forskjellige områder, for deretter å lage en generisk responsplan som kan tilpasses spesifikke hendelser (Ibid., s. 46). Målsetningen er at denne tilnærmingen skal både tilrettelegge for og muliggjøre at aktørene vil klare å håndtere mer

komplekse hendelser, som kan springe ut fra flere enn én type trusler eller muligheter og være et resultat av blanding av ventede og uventede omstendigheter (Ibid., s. 51).

Ifølge kortet er det anbefalt at responsplanene er basert på to hovedtrekk: den daglige driften og en «all-hazard»-tilnærming (Ibid., s. 47):

1. Selv om en krisesituasjon skiller seg fra den vanlige driften, stammer kapasiteten for å tilpasse seg fra den samme generelle kapasiteten som brukes når alt fungerer som normalt i det daglige. Dessuten vil de ansattes kjennskap til prosedyrer og retningslinjer gjøre det lettere å iverksette og drifte dem i nødsituasjoner.
2. Det er viktig at organisasjoner kartlegger og forstår mulige nødsituasjoner, samtidig som de klarer å kjenne igjen felles komponenter ved ulike trusler. På bakgrunn av det kan de lage generiske responsplaner for mange typer uventede hendelser, mens hver trussel har en bestemt utvidelse for å imøtekomme dens behov.

Som vist tidligere i kapittelet, vil de forskjellige beredskapsfasene passe inn i ulike krisefaser. Det samme gjelder her.

I førkrisefasen må organisasjonene først kartlegge mulige scenarioer som kan påvirke dem negativt på bakgrunn av eksperters erfaring og relevant faglitteratur. Etter kartleggingen må de identifisere beredskapens felleskomponenter, deriblant sjekklister for handling, som blant annet må inneholde kontaktinformasjon for interne og eksterne aktører som må involveres i gitte situasjoner. Videre kreves det en grundig analyse av hver hendelse for å skape en så nøyaktig forståelse som mulig om hvor unik hver situasjon er, for deretter å legge til tilpassede komponenter utover den første responsplanen. DRMG anbefaler at planene de tilpassede komponentene bygges opp rundt de daglige aktivitetene. Slik bruker man kjente ressurser og øker de ansattes kjennskap med retningslinjene (Ibid., s. 47-48).

For den akutte krisefasen er det selve håndteringen som er i fokus. Ved å la aktørene opptre på en måte de er kjent med, altså slik at de er så nære å skjøtte sitt daglige virke som mulig, øker man kapasiteten og selvtilliten deres. Innledningsvis i den akutte krisefasen, mens man fortsatt handler i henhold til den grunnleggende beredskapsplanen, må man diagnostisere den spesifikke situasjonen og justere planen deretter (Ibid., s. 49).

I etterkrisefasen må man gjennomføre en evalueringsprosess og revidere planverkene og prosedyrene i henhold til prosessens resultater. For en «all-hazard»-tilnærming er det dessuten viktig å evaluere strukturen til beredskapsplanene for å oppdage felleskomponenter for diverse nødsituasjoner og hva som er unikt ved hver trussel. Det er med andre ord en

revidering av det arbeidet som ble gjort i førkrisefasen basert på eventuell ny kunnskap. Til slutt kan koblingene mellom den daglige driften og krisehåndteringen påvirke både hvordan den daglige driften fungerer, så vel som fremtidige kriser (Ibid., s. 50).

3.4 Oppsummering

Krisehåndtering har vært det overhengende temaet for dette kapittelet. Jeg har redegjort for teorier om beredskap og sett på dette i lys av kritisk infrastruktur. Beredskapsarbeidsprosessen ble kort introdusert og sett i sammenheng med de tre krisefasene. Hvordan beredskap fungerer mer spesifikt i den finansielle infrastrukturen og hvordan ROS-analyser utarbeides der ble også viet oppmerksomhet. Deretter ble søkelyset rettet mot resiliens og jeg var blant annet innom de fire kjennetegnene på et resilient system. Til slutt presenterte jeg DRMG generelt og de tre kapabilitetskortene som er aktuelle for denne oppgaven spesielt. Men før jeg kan legge frem de empiriske funnene som skal drøftes ut fra dette teoretiske rammeverket, skal jeg vise hvilket metodisk utgangspunkt oppgaven har.

4 Metode

Som tidligere nevnt er målsetningen med denne oppgaven å undersøke hvorvidt bruk av konsepter innen resiliens kan bidra til å forbedre finanssektorens beredskap for betalingsterminaler. For å gjennomføre dette falt valget på DRMG og retningslinjenes kapabilitetskort. Jeg minner om problemstillingen som lyder:

«Hvordan kan anvendelse av konsepter og metoder innen resiliens forbedre finanssektorens beredskapsevne for betalingsterminaler?»

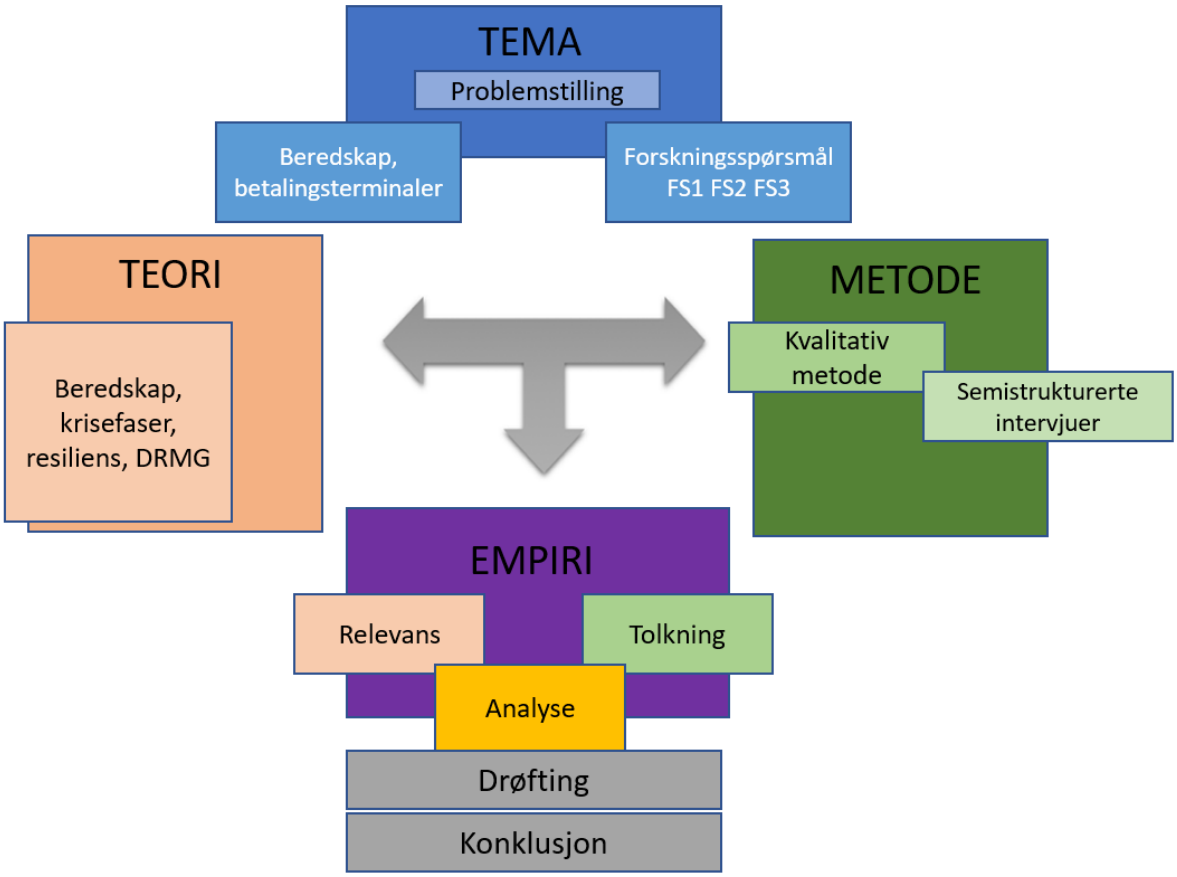
Det følgende kapittelet søker å belyse hvordan jeg har jobbet for å besvare problemstillingen og viser hvilken metodikk som ligger til grunn for oppgaven. Hensikten er å demonstrere oppgavens reliabilitet og validitet, slik at dens vitenskapelige kvalitet kan vurderes.

Det første jeg gjør i dette kapittelet er å presentere oppgavens forskningsdesign. Det etterfølges av en beskrivelse av kvalitativ forskning. Neste delkapittel handler om hvordan datainnsamlingen foregikk og inkluderer et underkapittel om semistrukturerte intervjuer. En redegjørelse for validitet og reliabilitet, og hvorfor jeg mener oppgaven oppfyller kravene de

stiller, følger deretter. Avslutningsvis nevner jeg fordeler og ulemper med metodevalget for oppgaven. Men i tråd med vanlig kutyme starter også dette kapittelet med begynnelsen. Tillat meg å legge frem oppgavens forskningsdesign.

4.1 Forskningsdesign

Oppgaven er lagt opp som en kvalitativ studie hvor det empiriske materialet er hentet inn fra informanter gjennom semistrukturerte intervjuer. Fordi forskningsspørsmålene i stor grad tar for seg elementer som samarbeid, informasjonsdeling og lignende, ønsket jeg å tilegne meg informasjon fra flere kilder. Tanken ved å bruke flere kilder var det ville hjelpe meg med å kunne tegne et så helhetlig bilde som mulig. Jeg benyttet meg av noe supplerende materiale som forelå i dokumentformat, men dette utgjør en svært liten andel av empirien. Det er snakk om et sidetall på mindre enn ti sider. Følgelig er oppgaven er å forstå som en kvalitativ studie som gjør bruk av induktiv logikk. Hva det innebærer kommer jeg tilbake til nedenfor.



Figur XI. Forskningsdesign.

En oversikt over oppgavens forskningsdesign er gjengitt i Figur XI ovenfor. Den viser hvordan oppgavens tema bidro til å utlede en problemstilling med tilhørende forskningsspørsmål. På bakgrunn av temaet og problemstillingen ble det teoretiske perspektivet og den metodologiske fremgangsmåten definert for å finne et svar på problemstillingen. Det empiriske materialet ble hentet inn på bakgrunn av teorien og metoden. Slik sørget jeg for at det forholdt seg relevant til det oppgaven tok mål av seg å finne ut av. Empirien skal henge sammen og derfor måtte materialet, som stammet fra ulike kilder, fortolkes inn i en større sammenheng. Jeg måtte forsøke å sette bitene sammen for å få et mer helhetlig bilde av beredskapen. Deretter ble materialet analysert, slik at det kunne drøftes opp mot teorien som danner grunnlaget for oppgaven og derigjennom finne et svar på problemstillingen og trekke en konklusjon.

Figur XI gjentar påstanden min om at oppgaven er basert på kvalitativ metode. For å demonstrere at det faktisk er tilfellet er det på sin plass å se nærmere på hva kvalitativ forskning går ut på.

4.2 Kvalitativ forskning

Ettersom jeg hentet inn data gjennom intervjuer og dokumenter for deretter å sette det inn i en fortolkende kontekst, er oppgaven av kvalitativ art (Blaikie og Priest, 2019, s. 200-204). En kvalitativ studie tar som oftest sikte på å oppnå dybdekunnskap og helhetlig forståelse av bestemte kontekster eller i forbindelse med utvikling av begreper, kategorier og typologier (Grønmo, 2023). Denne oppgaven søker, så langt det er mulig og innenfor de rammene jeg har satt, en helhetlig forståelse av hvordan beredskapsevnen for betalingsterminaler er i Norge med et formål om å undersøke hvorvidt den kan forbedres ved hjelp av resiliens. Dermed oppfyller oppgaven kravet om å være en kvalitativ studie.

Kvalitative data er vanskelige å gjenskape. Selv om noen bruker de samme informantene som meg vil konteksten uansett være annerledes. For det første vil dataene som hentes inn være av nyere dato og endringer kan ha funnet sted på feltet siden jeg snakket med informantene av ulike årsaker. I neste kapittel nevnes det for eksempel at en informant rapporterte om en betydelig endring i sikkerhetstilnærmingen i finanssektoren i løpet av det siste drøye året. Forandringer kan skje og tidspunktet for når informasjonen er innsamlet vil derfor være av stor betydning. For det andre innebærer kvalitativ forskning en viss grad av sosialt samkvem. De sosiale situasjonene kan aldri gjenskapes. Det er mulig å tenke seg til en rekke faktorer som kan påvirke situasjonene, deriblant dagsform, sultfølelse, personlige hensyn og forhold, arbeidsbelastning med mer. Små endringer i noen av dem eller andre faktorer kan påvirke

intervjuets gang. Dette fungerer som eksempler på hvorfor det er vanskelig, om ikke umulig, å gjenskape vitenskapelige resultater basert på kvalitative data. Men det er heller ikke målsetningen for kvalitativ forskning. Derimot er målet å skape en helhetlig og belysende beskrivelse av en situasjon som er sammenhengende og fundert på detaljerte studier av den bestemte situasjonen (Blaikie og Priest, 2019, s. 212).

Jeg følger opp tråden om gjenskapning av kvalitative data i kapittel 4.4.2 og den korte drøftingen om induktiv logikk i kapittel 4.4.1.3 kan anses som en forlengelse av diskusjonen om kvalitativ forskning, men før jeg kommer dit er det på sin plass å redegjøre for hvordan jeg gikk frem for å samle inn oppgavens empiriske materiale.

4.3 Datainnsamling

Som nevnt ovenfor bygger denne oppgaven i all hovedsak på datainnsamling gjort ved hjelp av semistrukturerte intervjuer. De ble gjennomført i løpet av våren 2023. Totalt bygger oppgaven på intervjuer med fem informanter fordelt på fem ulike organisasjoner i den finansielle infrastrukturen. I tillegg hadde jeg også en uformell samtale med en representant fra Finanstilsynet som bidro med noen pekere om hvilke virksomheter som var mest aktuelle å kontakte i forbindelse med en oppgave om betalingsterminaler. De rådene ble fulgt og jeg fikk intervjuet representanter for tre av de fire organisasjonene jeg ble anbefalt. Grunnleggende matematikk tilsier at jeg intervjuet personer fra to organisasjoner utenom anbefalingen. Samtlige av organisasjonene som deltok hadde representasjon i Beredskapsutvalget for finansiell infrastruktur (BFI) per 2023, men ikke alle informantene var personlig representert i utvalget. Like fullt hadde de en viss grad av innsikt i hva som foregikk der gjennom kollegaer i samme organisasjon i tillegg til bekjente i andre organisasjoner. En relevant organisasjon uten medlemskap i BFI, men som spesifikt ble navngitt som en jeg burde snakke med av Finanstilsynet, avslo å bidra til oppgaven. De oppga manglende kapasitet som årsak. Av personvernhensyn vil ingen av informantene navngis eller identifiseres. Hvilken organisasjon de kom fra vil heller ikke eksplisitt bli nevnt, men referanser til bestemte organisasjoners løsninger og ansvarsområder forekommer. Dette må ikke forstås som noe annet enn at løsningen eller ansvarsområdet er særlig relevant for det feltet og betyr ikke nødvendigvis at jeg har vært i kontakt med akkurat den virksomheten.

Underveis fikk jeg innsyn i noe sensitiv informasjon. Noe av den informasjonen vil ikke bli gjengitt i oppgaven etter avtale mellom meg og de(n) det gjelder. I enkelte tilfeller har informanten og jeg blitt enige om hvordan jeg kan omformulere informasjonen i mer generelle

vendinger, slik at den kan brukes og publiseres fritt i oppgaven. Dette gjelder for eksempel tilgang til detaljert statistisk informasjon om driftsstabiliteten til norske betalingsterminaler. Den informasjonen bruker jeg for å gi et generelt bilde om betalingsterminalenes driftsstabilitet, men de eksakte detaljene er ikke gjengitt i oppgaven. Det er verdt å understreke at den sensitive informasjonen jeg ble tiltrodd ikke var av en slik karakter at utelatelsen av den vil påvirke oppgavens funn eller den påfølgende analysen av dem.

Det er dataene som ble samlet inn gjennom intervjuer som danner hovedgrunnlaget for oppgaven. Enkelte data, som foreligger i tekstformat, har blitt brukt som supplerende empiri. Det vil si at dokumentene brukes for å bekrefte eller avkrefte informasjon som har kommet frem i intervjuer eller som på annen måte utfyller empirien. Dette gjelder informasjon fra relevante nettsider og rapporter. Fordi det kun er snakk om et fåtall skriftlige kilder som totalt utgjør mindre enn ti sider, vil jeg ikke gjøre noen vurdering av dokumentanalyse som metode.

4.3.1 Semistrukturerte intervjuer

Oppgaven bygger som nevnt på dataene som ble samlet inn gjennom intervjuene. For å danne meg et så helhetlig bilde som mulig intervjuet jeg representanter for ulike ledd i verdikjeden som kreves for å gjennomføre transaksjoner ved hjelp av en betalingsterminal. Alle organisasjonene var medlemmer av BFI per 2023 og norske myndigheter anser dem følgelig som viktige aktører i den finansielle infrastrukturen. Essensielle støttefunksjoner, som telekommunikasjon og strømforsyning, ble ikke inkludert i utvalget jeg gjorde i forbindelse med datainnsamlingen. Bakgrunnen for det er at selv om alle fastmonterte betalingsterminaler ikke vil fungere uten for eksempel elektrisitet er det ikke gitt at kraftselskapene bidrar spesifikt inn mot beredskapen for betalingsterminaler. Som jeg kommer inn på i konklusjonskapittelet kan det være en idé for videre studier i fremtiden. Jeg valgte heller ikke å innhente informasjon fra utsalgssteder selv om de kan tilrettelegge for beredskapsløsninger ved strømbrudd i form av tilgang til strømaggregater i butikkene. Dessuten avslo som nevnt en komplementær aktør å delta med begrunnelse om at de ikke hadde kapasitet. Det kunne beriket oppgaven, men ble dessverre ikke en realitet.

Det var ikke bare representativitet for betalingsterminalenes verdikjede jeg søkte. Jeg ønsket også kvalitativ informasjon som ville hjelpe meg med å besvare forskningsspørsmålene og problemstillingen. Informantene hadde lang erfaring fra finanssektoren. Flere hadde arbeidet i ulike deler av den finansielle infrastrukturen og hadde følgelig innsikt utover sin nåværende arbeidsplass. Dette samsvarer med ideen bak et dybdeintervju. Der intervjuer man

nøkkelinformanter, altså personer med særlig stor innsikt og kunnskap om det bestemte feltet (Andersen, 2006, s. 279). Dette er en versjon av et kvalitativt intervju hvor hensikten er å skape mening og forståelse rundt temaet (Kvale og Brinkmann, 2015, s. 20), samtidig som man søker nyanserte beskrivelser av informantenes livsverden (Ibid., s. 47).

Intervjuene ble gjennomført som semistrukturerte intervjuer. Det betyr at jeg utarbeidet en intervjuguide (se Vedlegg A) med spørsmål knyttet opp mot hvert av de tre forskningsspørsmålene. Den ble brukt som en mal for intervjuet, men hvilke spørsmål som ble stilt og rekkefølgen på dem avhengte av hvordan intervjuet forløp. Fordi de forskjellige aktørene besatt ulike roller i infrastrukturen, var heller ikke samtlige spørsmål relevante for alle aktørene. Det kom an på deres konkrete rolle i arbeidet med beredskapen for betalingsterminaler.

Tabell V. Oversikt over informanter

INFORMANTER	INTERVJUDETALJER
Informant 1 Avdelingsleder teknisk infrastruktur	Gjennomført digitalt på Teams. Varighet ca. 50 minutter. Utdypning av spørsmål besvart per e-post.
Informant 2 Kortselskap	Gjennomført digitalt på Teams. Varighet ca. 60 minutter. Oversendte tilleggsinformasjon per e-post.
Informant 3 Teknologi- og programvareselskap	Gjennomført digitalt på Teams. Varighet ca. 30 minutter. Utdypning av spørsmål besvart per e-post.
Informant 4 Daglig leder	Gjennomført digitalt på Teams. Varighet ca. 25 minutter. Spørsmål besvart per e-post i forkant av intervjuet. Intervjuet brukt for å få utdypet noen svar.
Informant 5 Leverandør av terminaler med mer	Gjennomført ved fysisk oppmøte i virksomhetens lokaler i Osloregionen. Varighet ca. 60 minutter.

Tabell V viser en oversikt over informantene som deltok i forbindelse med studien og detaljer fra intervjuene. Informantene er nummerert og sortert i henhold til intervjudato, hvor Informant 1 var den første som ble intervjuet, mens Informant 5 var den siste. Som nevnt navngis ikke organisasjonen de ulike informantene representerer og i de tilfellene hvor en generisk beskrivelse av virksomheten ikke er mulig står informanten oppført med stillingstittel i stedet.

Intervjudetaljene gir en oversikt over hvor intervjuet ble gjennomført og dets varighet (oppført i omtrentlig tid og kan derfor avvike med rundt fem minutter i hver retning), samt eventuelle tilleggsopplysninger som var relevante for det bestemte intervjuet.

For å skape best mulig relasjon til hver enkelt informant i forkant av intervjuet ønsket jeg at informanten selv bestemte rammene for hvordan de skulle intervjues. Det inkluderte hvor intervjuet fant sted, når det ble gjennomført og intervjuets lengde. Optimalt sett hadde alle intervjuene hatt den samme varigheten, men med mange informanter som har ulike timeplaner og arbeidspress, mente jeg det beste var å la dem avgjøre det fremfor å presse dem til et bestemt antall minutter. Samtlige informanter tillot og oppfordret at jeg kom med eventuelle oppfølgingsspørsmål i etterkant, for eksempel hvis det var noe jeg ikke rakk å få spurt om. Dette ble gjort via e-post og svarene ble slettet etter at dette prosjektet var avsluttet.

I og med at dette prosjektet ikke ble meldt inn til Norsk senter for forskningsdata (NSD), kunne jeg ikke lagre personopplysninger om noen av informantene. Derfor identifiseres de heller ikke i oppgaven. Ei heller i forordet, selv om jeg gjerne skulle gjort det. Av samme grunn tok jeg heller ingen opptak under intervjuene, men noterte svarene fortløpende. Det største ankepunktet ved dette valget, som jeg kommer nærmere inn på senere, er at jeg kan ha gått glipp av relevant og viktig informasjon. På den andre siden kan det ha bidratt til at informantene snakket friere enn hva tilfellet kunne vært dersom de visste at samtalen ble tatt opp, selv om de i så fall ville signert et skjema som forsikret dem om at opptakene ville blitt slettet etter transkriberingen.

Metodisk kan det å basere en studie på intervjuer være problematisk. Det er mye som kan påvirke hvordan en informant svarer på spørsmålene, for eksempel dagsform. Enda viktigere vil heuristikker kunne være. Særlig tilgjengelighetsheuristikken som går ut på at informasjon som er lett tilgjengelig i hjernen kan påvirke ens umiddelbare oppfatning av noe (Kahneman, 2012, s. 144). Hvis en informant nylig har vært eksponert for en spesiell hendelse kan dette ubevisst påvirke hvordan vedkommende besvarer enkelte spørsmål. Videre kan måten spørsmålene var formulert på og hvordan de ble stilt (toneleie, tidspunkt i samtalen og lignende) påvirke hvordan de ble besvart. I det hele tatt er det et utall av forutinntattheter, skjevheter, heuristikker og potensielle språklige misforståelser som kan farge intervjuet på den ene eller andre måten. Dette er umulig å etterprøve. Ikke minst fordi det ikke finnes opptak av intervjuene, men selv ikke opptak ville klart å fange opp alt som foregikk i intervjusituasjonen. For eksempel ville ikke et lydopptak klart å få med seg kroppsspråk, ansiktsuttrykk eller lignende. Dessuten ville det vært umulig å få med i transkripsjonen selv om man hadde kameraer som fanget opp alle inntrykk i sanntid og i henhold til lovgivningen måtte intervjuet

blitt slettet etter at transkriberingen var gjort. I tillegg kan det skje ting som påvirker intervjuet som ikke fanges opp av kameraene. I løpet av det intervjuet som ble gjennomført ved fysisk tilstedeværelse opplevde vi at en fugl kolliderte med vinduet to ganger på kort tid før den fløy sin vei. Den distraksjonen påvirket umiddelbart intervjuet og det kunne vært vanskelig å oppfatte hvorfor om man ikke fikk med seg fuglens nærmøte med vinduet. Altså er det en umulighet å få med seg alle aspekter i et intervju uansett hvor godt det er dokumentert. Samtidig kan det faktum at det ikke ble gjort opptak ha minimert sjansen for at informantenes svar ble påvirket av kunnskapen om at det de fortalte ble tatt opp, men det blir ren spekulasjon og er således lite fruktbart. Ellers var det som nevnt viktig at informantene skulle få et godt inntrykk av meg, slik at de snakket så fritt som mulig. Det var også bakgrunnen for at jeg lot hver enkelt informant velge den intervjusituasjonen de opplevde som mest passende og komfortabel.

I forlengelsen av dette med heuristikker kan det også nevnes at informantene har en rolle i en organisasjon. En utfordring er at informantene følgelig er på innsiden av et system og kan være farget av det. Det kan føre til at de bevisst eller ubevisst ønsker å fremstille sin egen organisasjon i best mulig lys, for eksempel ved å hoppe bukk over informasjon av mer negativ art. Foruten å være klar over at informantene kan sminke sannheten, er det viktig å ta en aktiv og bevisst rolle i intervjuet for å redusere sjansen for at nettopp det skal skje. Dette medfører økt analytisk kontroll og i fortsettelsen av det også forbedret validitet og reliabilitet (Andersen, 2006, s. 279).

4.4 Validitet og reliabilitet

Validitet og reliabilitet, også kjent som gyldighet og pålitelighet, gir en indikasjon på en studies vitenskapelige forankring.

4.4.1 Validitet

Validitet, eller gyldighet, handler om i hvilken grad funnene i en studie fører til gyldige slutninger om studieobjektet (Dahlum, 2021). Det er tre fremgangsmåter man kan ta i bruk for å sørge for at studien innehar høy validitet: å skape validitet, indre validitet og ytre validitet (Yin, 2018, s. 42-43).

4.4.1.1 Skape validitet

Å skape validitet går ut på å finne riktige målebegreper for det man studerer (Ibid., s. 42). Yin (2018) presenterer tre måter man skape validitet på: å bruke flere kilder, skape en beviskjede og la informanter gjennomgå et utkast av studien før den ferdigstilles (Ibid., s. 44).

I denne oppgaven bruker jeg flere kilder i form av informanter fra forskjellige relevante virksomheter. En redegjørelse for informantene ble foretatt ovenfor og oversikten er sammenstilt i Tabell V. Det er likevel verdt å nevne at jeg har tatt grep for at denne oppgavens resultater skal kunne anses som gyldige. Informantene kom fra et bredt spekter av organisasjoner som på en eller annen måte er involvert i arbeidet med betalingsterminaler. Alle representerte som tidligere nevnt en organisasjon med representasjon i BFI. Det må forstås som et tegn på aktørenes relevans for det generelle beredskapsarbeidet for den finansielle infrastrukturen i Norge. En bekreftelse på at dette gjaldt for minst tre av organisasjonene kom i form av en direkte anbefaling om å kontakte dem fra Finanstilsynet. Dermed baserer oppgaven seg på informasjon som stammer fra personer med direkte kunnskap om hvordan beredskapsarbeidet for betalingsterminaler fungerer i Norge. Det som derimot er et åpent spørsmål er hvorvidt flere aktører burde vært intervjuet, slik at oppgaven ville vært basert på et enda bredere utvalg av informanter. For eksempel kunne det vært aktuelt å inkludere representanter for andre sektorer som betalingsterminalene er avhengige av for å fungere, som energisektoren. Det kunne skapt større forståelse for hvordan det overordnede beredskapsarbeidet foregår, men kunne samtidig ha vannet ut funnene ved at representanter for andre sektorer ikke kan antas å ha annet enn begrenset forståelse og kunnskap om de vurderingene som ligger til grunn for beredskapen i finanssektoren. Det ble et avveiningsspørsmål og jeg valgte ikke å benytte andre informanter enn personer fra nettopp den finansielle infrastrukturen.

En beviskjede skal gjøre det mulig å gjennomgå hvert trinn i prosessen som har ført frem til funnene. Dette innebærer blant annet å referere til andre aspekter ved studien underveis i oppgaven, slik at enhver som leser den lett skal kunne følge beviskjeden (Ibid., s. 134-136). Jeg har etter beste evne forsøkt å gjøre det, slik at enhver kan følge beviskjeden. Hvorvidt jeg har lykkes med det er opp til leseren.

Den siste fremgangsmåten som, ifølge Yin (2018), vil forsterke den totale validiteten i en studie, er å la informantene som har bidratt til oppgaven se gjennom et utkast av den før den ferdigstilles. Dermed kan informantene komme med tilbakemeldinger og rette opp eventuelle misforståelser, feiltolkninger eller på andre måter kommentere hvordan de oppfatter studiens

kvalitet i den hensikt å forbedre den (Ibid., s. 240-241). Alle informanter fikk tilbud om å se et forkortet utkast av oppgaven som inkluderte kapittel 2.3 og hele kapittel 5. Utkastet ble sendt ut til dem om kvelden mandag 29. mai 2023 med svarfrist onsdag 7. juni 2023. En informant kom med tilbakemelding som førte til korreksjoner. Det som likevel kan svekke validiteten i denne sammenhengen er oppgaven skulle leveres innen en gitt tidsfrist (15. juni 2023) og det er derfor ikke gitt at informantene hadde tid til å lese gjennom og eventuelt komme med tilbakemeldinger på hva de forstår som svakheter ved empirigjengivelsen eller andre former for kommentarer.

4.4.1.2 Indre validitet

Indre validitet viser til at funnene er riktige og gyldige for det studerte utvalget (Pripp, 2018). Det vil si at studien faktisk målte det den tok sikte på å gjøre. Indre validitet har størst betydning for forklarende effektstudier og årsaksstudier blant de kvalitative studieformene (Yin, 2018, s. 42), og er slik sett ikke like viktig for denne oppgaven. Den er mest aktuell i tilfeller hvor man forsøker å koble hvordan og hvorfor en hendelse førte til en annen hendelse. Hovedhensikten med indre validitet er at den skal sørge for å påvise kausale sammenhenger eller utforske om det kan være andre bakenforliggende årsaker som forklarer bestemte hendelser enn de årsakene man tror det er i tilfeller hvor sammenhengen ikke kan påvises direkte (Ibid., s. 45).

Fordi denne oppgaven verken kan sies å være enten en effekt- eller årsaksstudie, vil det å påvise indre validitet ikke være relevant. Deskriptive og utforskende studier forholder seg ikke til indre validitet (Ibid., s. 42) og denne oppgaven er nettopp utforskende. Den skal utforske beredskapstilstanden for betalingsterminaler og vurdere om det er mulig å forbedre arbeidet ved hjelp av resiliens.

4.4.1.3 Ytre validitet

I kapittel 4.2 antydet jeg at jeg ville fortsette diskusjonen om kvalitativ forskning og generaliseringen av denne her. Årsaken er at hvorvidt og hvordan en studies funn kan generaliseres er selve hensikten med ytre validitet (Ibid., s. 45) og passer dermed inn i den følgende drøftingen.

Ved hjelp av induktiv logikk er det mulig å etablere begrensede generaliseringer av karakteristikker og regelmessigheter (Blaikie og Priest, 2019, s. 92-93). Hvorvidt bruk av

konsepter fra resiliens kan forbedre beredskapen for betalingsterminaler vil være en form for begrenset generalisering hvor generaliseringen av funnene enten bygger opp under ideen om at resiliens kan forbedre beredskapen eller at de ikke gjør det. De beskrivelsene som gjøres med bruk av induktiv logikk skal ikke forstås som allmenngyldige. Det vil si at bare fordi denne oppgaven konkluderer på en bestemt måte, vil ikke det bety at de samme konseptene nødvendigvis vil ha samme innvirkning for beredskapen andre steder. Resultatene som stammer fra en induktiv studie er med andre ord ikke direkte overførbare til andre scenarioer og/eller kontekster (Ibid., s. 94). Samtidig er det sånn at mange kvalitative studiers målsetning ikke er å generalisere, men heller å tilføre en bred og kontekstualisert forståelse gjennom studier av spesifikke objekter, hendelser eller andre elementer relevante for det feltet man undersøker (Polit & Beck, 2010, s. 1451). Slik sett er det som kommer frem i en kvalitativ studie indirekte overførbart. Hvis kvaliteten på beskrivelsene som gjøres i studien er gode nok, vil det være mulig å overføre dens funn og forståelse til andre kontekster (Ibid., s. 1453). Dermed kan en kvalitativ studie basert på induktiv logikk likevel ha en generaliserende verdi, men det forutsetter at beskrivelsene av det aktuelle fenomenet er av tilstrekkelig kvalitet. En oppgave om beredskapen for betalingsterminaler kan derfor være overførbar til øvrig beredskap i den finansielle infrastrukturen eller i helt andre sektorer. For eksempel vil aktørene som samarbeider om beredskapen for betalingsterminalene kunne ha et samarbeid også på andre fronter, både internt i finanssektoren og eksternt til andre sektorer som telekommunikasjon. I så fall vil denne oppgaven kunne bidra til å forbedre beredskapen utover enn kun for betalingsterminaler. Den ytre validiteten er derfor ivaretatt så langt det lar seg gjøre i en kvalitativ studie gjennom bruk av induksjon.

Foruten validitet er også reliabilitet et viktig premiss for å demonstrere en studies vitenskapelige forankring.

4.4.2 Reliabilitet

Reliabilitet, også kjent som pålitelighet, er å vise at måten studien er gjennomført på kan gjentas med de samme resultatene (Yin, 2018, s. 42), slik at sjansen for feil og skjevhet minimeres (Ibid., s. 46). I kapittel 4.2 var jeg inne på at deler av diskusjonen ville bli videreført her, som i det ovenstående underkapittelet, og noe av dette må derfor ses i sammenheng med delkapittelet om kvalitativ forskning.

I kapittel 4.3 var jeg inne på hvorvidt det er mulig å gjenta de eksakt samme intervjuene som jeg gjennomførte i forbindelse med oppgaven og gikk langt i å antyde at det er mer eller

mindre umulig. Det jeg kan legge til er at jeg stort sett oppnådde kontakt med organisasjonene ved å gå runden via deres sentralbord, enten per telefon eller e-post, for deretter å bli satt i kontakt med relevante avdelinger og deretter den avdelingen anså som rette vedkommende. Den samme fremgangsmåten ble ikke fulgt i hvert tilfelle. I ett fikk jeg et konkret tips om en kontaktperson fra en informant og i et annet kom jeg frem til riktig person takket være hjelp fra bekjente som kjente personer med tilknytning til virksomheten. Dermed kom jeg frem til informanten via omveier i det aktuelle selskapet. Resultatene var stort sett de samme. Jeg ble satt i videre kontakt med de som hadde best grunnlag for å besvare spørsmål knyttet til betalingsterminaler og beredskap. Siden informantene ikke navngis i oppgaven finnes det ingen garantier for at noen som søker å gjenta eksperimentet vil komme i kontakt med de samme personene, men det er like fullt sannsynlig. Riktignok under forutsetning av at de samme personene fortsatt besitter de samme stillingene når studien blir forsøkt gjentatt. Et annet moment det er verdt å fremheve er at funnene i denne oppgaven er basert på studier gjort våren 2023. Mye kan endre seg på kort tid og det er heller ikke her noen garantier for at dette kan gjentas med de samme resultatene i 2024 eller senere. Dette er for øvrig et vanlig problem med reliabilitet for denne typen studier (Ibid.), men siden jeg har oppgitt fremgangsmåten for hvordan jeg kom frem til de resultatene jeg gjorde, ville det, etter mitt skjønn, vært mulig å gjenta studien med de samme resultatene i en ideell verden hvor alle forutsetninger var identiske under hele prosessen.

På bakgrunn av diskusjonen ovenfor mener jeg at oppgavens validitet og reliabilitet er gjort rede for og at den oppfyller de forventede vitenskapelige standardene.

4.5 Fordeler og ulemper ved metodevalg

Med utgangspunkt i diskusjonen i dette kapittelet mener jeg det er enkelte fordeler og ulemper med de metodiske valgene som er tatt. Noen av dem har allerede blitt diskutert og kan bli gjentatt i forkortet utgave i dette delkapittelet der det passer inn i sammenhengen.

4.5.1 Bruk av intervjuer

Som nevnt i kapittel 4.3.1 om semistrukturerte intervjuer finnes det flere snubletråder som kan svekke oppgavens kvalitet. Dette gjelder særlig en oppgave som denne hvor datagrunnlaget nesten utelukkende er basert på intervjuer.

Slik jeg antydet tidligere i kapittelet er det en rekke faktorer som kan påvirke et intervju. Respondentene kan svare annerledes avhengig av hvem som intervjuer dem. Intervjuerens kjønn, alder, etnisitet, attraktivitet, sosiale klasse, utdanningsnivå og oppfattet livserfaring er eksempler på faktorer som kan influere hvilke svar informantene gir (Waterfield, 2018). Personlig oppfattet jeg ikke at dette hadde noen innvirkning på intervjuene overhodet, men jeg er samtidig inhabil i så måte. At jeg heller ikke hadde noen erfaring fra eller spesielle kunnskaper om finanssektoren utover det helt generelle gjør meg dessuten kanskje mindre egnet til å oppdage hvorvidt svarene farges av meg og mine karakteristikker som intervjuer.

Et annet moment som også ble nevnt nevnte tidligere er at kroppsspråk, ansiktsuttrykk, toneleie, fremtoning og lignende kan påvirke en intervjusituasjon. For eksempel kan toneleiet et spørsmål stilles med bidra til å skape en forventning hos informanten om hva som er det «rette» svaret og svaret deretter (Ibid.). Fire av intervjuene ble gjort digitalt og kroppsspråk er mindre aktuelt i digitale intervjuer ettersom det er begrenset hvor mye av kroppen man ser. Det kan være både positivt og negativt. Positivt i den forstand at man unngår kroppsspråk som informanten kan reagere negativt på. Negativt fordi en del av det sosiale aspektet forsvinner og det blir vanskeligere å skape en relasjon. Andre aspekter kan også gå tapt uten å se informantens kroppsspråk. For eksempel er det mulig å se for seg at man lettere kan oppfatte at informanten tilbakeholder eller på annen måte kommer med misvisende informasjon ved fysisk tilstedeværelse. Derfor kan man argumentere for at jeg burde gjennomført alle intervjuene på samme måte, slik at jeg også fikk all informasjonen på samme måte. Mitt valg var å kjøre intervjuene på den måten informantene selv ønsket for å skape et best mulig forhold til dem. Å skape en god relasjon er også en viktig del av intervjuet. Jo bedre kontakt det er mellom intervjuer og informant, jo større er sjansen for at man får innsyn i sensitiv informasjon (Ibid.). Jeg kan legge til at jeg følte jeg kom meget godt overens med alle informantene og at alle var svært behjelpelige med å dele det de visste om de temaene de ble spurt ut om. Det er stort sett positivt, men kan også gjøre meg mindre kritisk enn jeg kanskje burde være. Akkurat det er noe jeg er obs på og som jeg i drøftingen i kapittel 7 streber etter å unngå.

Det finnes som tidligere nevnt heller ingen opptak eller transkripsjoner av intervjuene. Siden dette er et enmannsprosjekt er det fra et arbeidsmengdestandpunkt en fordel at det ikke ble gjort opptak. Hadde det blitt gjort ville det krevd mye ekstraarbeid og jeg valgte også å sette meg inn i temaer jeg hadde begrenset kunnskap om fra før av da jeg valgte å skrive denne oppgaven. Jeg har ingen tidligere relevant erfaring fra finanssektoren eller med betalingsterminaler utover at jeg har brukt dem i forbindelse med varekjøp. Resiliens hadde jeg noe kunnskap om fra før av, men den var i det store og hele på et overflatisk nivå. På den andre

siden er det fare for at informasjon går tapt, slik jeg diskuterte tidligere. Hvorvidt det er positivt eller negativt vil avhenge av hva man vektlegger som viktigst, men det er liten tvil om at det ville vært mindre rom for misforståelser fra min side i tolkningen av materialet dersom det forelå opptak og transkripsjoner av intervjuene. En av tankene bak å gi informantene et tilbud om å gå gjennom oppgaven før innlevering er nettopp for å bøte litt på risikoen for at jeg har misforstått, feiltolket, notert galt eller på andre måter behandlet empirien feil.

4.5.2 Kildegrunnlag

Semistrukturerte intervjuer er langt på vei den eneste kilden for datainnsamling i denne oppgaven. En fordel er at utvalget av informanter og deres kompetanse er av høy kvalitet. Alle hadde på intervjutidspunktet lang fartstid på fagfeltet og hadde god oversikt over det som foregår både internt i egen virksomhet og også i den finansielle infrastrukturen på mer generell basis. I tillegg var det et bredt utvalg av informanter sett i forhold til antallet virksomheter i BFI og hvor mange involverte det er i forbindelse med beredskapen for betalingsterminaler. Jeg har dekket de fleste prosessene som skjer i forbindelse med bruk av en betalingsterminal. Det kanskje viktigste unntaket er jeg ikke intervjuet noen representanter for en bank, men de er heller ikke involvert i beredskapsarbeidet på samme måte. En bankrepresentant jeg var i kontakt med innledningsvis i prosessen var også litt avmålt og skeptisk til hva de egentlig kunne bidra med rundt betalingsterminaler. Like fullt ville det ikke skadet å få inn perspektivet for en av bankene representert i BFI. Jeg skulle gjerne også hatt inn en aktør som komplementerer infrastrukturen for betalingsterminaler for å finne ut av i hvilken grad de er orienterte om det som foregår på betalingsterminalfronten. Tanken min er at de kan oppleve økt belastning på sine nettverk ved bortfall av betalingsterminaler og det hadde vært en berikelse for oppgaven dersom jeg kunne fått et inntrykk av deres eventuelle samarbeid med andre aktører i den finansielle infrastrukturen i den forbindelse, samt hvor forberedte de er hvis et langvarig bortfall skulle oppstå. De takket som nevnt nei til å bidra.

Når det gjelder selve valget av kildegrunnlag er det en mulig ulempe at jeg i så stor grad lener meg på materiale innhentet gjennom intervjuer. For å få et mer variert kildegrunnlag skulle jeg gjerne hatt flere skriftlige kilder, men det er begrenset hvor mange relevante og offentlig tilgjengelige skriftlige kilder som faktisk finnes. Et alternativ som muligens ville ført til at jeg kunne fått mer sensitiv informasjon fra informantene ville vært om jeg organiserte det slik at oppgaven ble unntatt fra offentligheten i en periode etter innlevering og publisering, men det var aldri ønskelig fra min side. For min egen del er det bedre at oppgaven er offentlig

tilgjengelig fra dag én – oppgaven kan hjelpe meg i jobbsøkerprosessen jeg står overfor etter at den er levert inn. Samtidig forsøkte jeg å avgrense oppgaven nettopp med tanke på å unngå at kildegrunnlaget skulle være basert i særlig grad på informasjon som kan være å forstå som bedriftshemmeligheter. Dette er med andre ord en ulempe jeg er villig til å leve med, men som jeg har forsøkt å imøtegå gjennom oppgavens avgrensning.

4.6 Oppsummering

I dette kapittelet har jeg presentert oppgavens forskningsdesign, redegjort for hva kvalitativ forskning innebærer og hvordan datainnsamlingen foregikk. Jeg forklarte også hvordan intervjuene ble foretatt og noe om hvordan semistrukturerte intervjuer passer inn som en fremgangsmåte innen kvalitativ metode. Videre forklarte jeg hva validitet og reliabilitet går ut på og hvorfor jeg mener denne oppgaven lever opp til de nødvendige standardene for en vitenskapelig studie, før jeg til slutt så på fordeler og ulemper ved oppgavens metodikk med et særlig blikk rettet mot de positive og negative sidene ved å bruke intervjuer som selve det empiriske kildegrunnlaget for oppgaven. Hvilken informasjon jeg fikk ut av intervjuene kommer frem i neste kapittel. Det omhandler empirien som oppgaven bygger på.

5 Presentasjon av empiri

Som nevnt i forrige kapittel er det empiriske grunnlaget for oppgaven i all hovedsak basert på materialet som kom frem gjennom intervjuene som ble foretatt i løpet av våren 2023. Den informasjonen presenteres i dette kapittelet. Det skjer systematisk, hvilket betyr at den presenteres for hvert enkelt forskningsspørsmål. Selve drøftingen av empirien sett i lys av teorien skjer i kapittel 6. Her vil dataene presenteres uten noen form for drøfting. Jeg minner om at forskningsspørsmålene var som følger:

1. Hvordan legger aktørene i finanssektoren til rette for å fremme felles forståelse på tvers av organisasjonene i forbindelse med beredskapen for betalingsterminaler?
2. Hvordan fungerte det interorganisatoriske samarbeidet mellom aktørene i finanssektoren under bortfallet av betalingsterminalene 16. mai 2022 og hvilken lærdom trakk de ut av det?
3. Hvordan innretter finanssektorens aktører beredskapen for betalingsterminaler?

Hvert enkelt forskningsspørsmål vil også bli gjentatt i begynnelsen av sine respektive delkapitler slik at hvert enkelt spørsmål skal være ferskt i minnet.

5.1 Fremme felles tverrorganisatorisk forståelse

Det første forskningsspørsmålet var: «Hvordan legger aktørene i finanssektoren til rette for å fremme felles forståelse på tvers av organisasjonene i forbindelse med beredskapen for betalingsterminaler?». I løpet av prosjektet fant jeg ut at dette skjer på flere fronter. Funnene i dette delkapittelet legges derfor systematisk frem i underkapitler basert på hvor og i hvilke sammenhenger kontakten mellom aktørene finner sted. Jeg starter med det organet som i størst grad er tilkjennegjort hittil i oppgaven: Beredskapsutvalget for finansiell infrastruktur.

5.1.1 Beredskapsutvalget for finansiell infrastruktur

I kapittel 3 beskrev jeg Beredskapsutvalget for finansiell infrastrukturs (BFI) rolle i den finansielle infrastrukturen. De har minst tre møter og en beredskapsøvelse i året. Ved behov arrangeres det ekstraordinære møter. I løpet av 2020 ble det avholdt tretten ekstraordinære møter i tillegg til de tre faste for å oppsummere status på beredskap og tiltak under koronapandemien (BFI, 2021, s. 4). Aktivitetene deres offentliggjøres dessuten årlig i form av årsrapporter som legges ut på deres nettsider. Per 2023 består BFI femten virksomheter, enten i form av faste medlemmer, varamedlemmer eller observatører. I tillegg er det observatører fra tele- og kraftsektoren, Nasjonal sikkerhetsmyndighet (NSM) og verdipapir- og fondsmeglersektoren. De femten medlemmene, som er offentliggjort på BFIs nettsider og gjengitt i Tabell III i kapittel 3.1.3, kommer alle fra finanssektoren. Hensikten med møtene og aktivitetene i regi av BFI er å samordne beredskapen i den finansielle infrastrukturen og bidra til at de ulike organisasjonene og virksomhetene får bedre forståelse av hverandres arbeidsoppgaver, ansvarsområder med mer. Dette er det mest formelle forumet hvor denne typen arbeid finner sted. Noe av dette arbeidet er gjengitt i Tabell II i kapittel 2.4. Der presenterte jeg et utvalg registrerte hendelser og øvelser fra 2004 til 2022. Dette er av såpass stor betydning for hvordan det skapes felles forståelse mellom de ulike involverte organisasjonene at det viktigste gjentas og utbroderes her.

Den viktigste øvelsen i forbindelse med betalingsterminaler de seneste årene fant sted i desember 2017 og ble avholdt i regi av Bits, som er bank- og finansnæringens

infrastrukturselskap. Øvelsen tok utgangspunkt i at sentrale deler av betalingskortinfrastrukturen var rammet av hendelser som førte til at det ikke var mulig å betale med kort i løpet av en toukersperiode (fjorten dager), men reserveløsningen fungerte. Den forklares nærmere i kapittel 5.3.3. Dette scenarioet skjedde samtidig med at tilliten til kontanter var på et lavpunkt som følge av stor spredning av falske kontanter (BFI, 2018, s. 5). Som nevnt i kapittel 2.4 førte øvelsen blant annet til en utvidelse av reserveløsningen for butikkjeder som selger dagligvarer, drivstoff og/eller medisiner. Utvidelsen ble gjennomført i 2021. Av større relevans i denne sammenhengen er at en slik øvelse krever samhandling på tvers av organisasjoner. Alle faste medlemmer i BFI har møteplikt og det må foreligge gode grunner for et eventuelt forfall. De fleste faste representantene har dessuten personlige vararepresentanter som overtar deres plass ved forfall. For organisasjonene som har representasjon i BFI vil derfor deltakelse på øvelsen vært obligatorisk. Følgelig ble øvelsen holdt som en tverrorganisatorisk øvelse, men den involverte ikke alle medlemsorganisasjonene som sådan. Det vil si at hver enkelt organisasjon ikke deltok med full organisatorisk tyngde, men heller den eller de representanten(e) de hadde til stede under øvelsen.

Av informantene som bidro til denne oppgaven var det kun informant 4 som selv har møteplikt i BFI. To av de andre informantene hadde andrehåndskjennskap til det som foregår på møtene fordi de blir informert og oppdatert av kollegaer som sitter i utvalget. En av informantene har liten oversikt over hva som foregår i beredskapsutvalget, mens den siste informanten implisitt forklarte at vedkommende ikke er kjent med detaljene i det arbeidet som gjøres i BFI.

Foruten BFI finnes det også andre formaliserte kontaktflater hvor virksomhetene er i kontakt med hverandre. Ett eksempel er et driftsforum for verdikjeden til betalingskort.

5.1.2 Driftsforum for betalingskort-verdikjede

Driftsforumet heter egentlig Driftsforum for XYZ verdikjede, hvor XYZ er navnet på selskapet. For å være sikker på å overholde personvernlovgivningen gjengis ikke navnet på organisasjonen som er ansvarlig for forumet. Bakgrunnen for etableringen av forumet var den såkalte «Påskehendelsen» i 2011, som er gjengitt i Tabell II i kapittel 2.4. Kort fortalt førte en hardwarefeil kombinert med at reserveløsningen ikke hadde samme kapasitet som primærløsningen til at bruk av betalingsterminaler og minibanker enten ble avbrutt eller gikk svært sakte (Finanstilsynet, 2012, s. 31). Informant 2 fortalte at driftsforumet ble opprettet som følge av at den påfølgende hendelsesevalueringen viste at konsekvensene av «Påskehendelsen»

kunne vært redusert dersom aktørene hadde hatt bedre kommunikasjon og samhandling. Derfor anmodet Kredittilsynet i 2011 om at dette forumet ble etablert og det har vært i funksjon siden.

Foruten betalingskortselskapet er flere banker og andre relevante aktører i den finansielle infrastrukturen med. Enkelte virksomheter har også representasjon i BFI, men det er også aktører som ikke er representert der som har medlemskap i dette driftsforumet. Alle medlemmene er på en eller annen måte involvert i verdikjeden for betalingskort, som er gjengitt i en forenklet utgave i kapittel 2.3.

Driftsforumet avholder tre til fire møter i året. Der drøftes hendelser, nedetider og annet som har skjedd eller som planlegges å skje. Det føres ingen referater fra møtene. På møtene avklares det for eksempel om noen skal utføre større vedlikeholdsarbeid i tiden som kommer, slik at de andre partene er orienterte og forberedte på at den bestemte virksomheten gjennomfører vedlikehold på gitte tidspunkt.

Enkelte av aktørene som deltar i driftsforumet kjenner hverandre også fra andre arenaer hvor kortselskapet ikke er representert. Sentrale leverandører til bankene har også bilaterale avtaler om samhandling ved driftshendelser seg imellom. Dette kommer jeg tilbake til i kapittel 5.3.1. Informant 3 bekreftet at dialogen mellom aktørene skjer både i formelle og uformelle sammenkomster og at det ofte er de samme personene som går igjen, slik at de får gode muligheter til å bli godt kjent med hverandre, både på person- og organisasjonsnivå.

5.1.3 Bits som møteplass

En av aktørene som går igjen blant informantene som sentral for tilretteleggingen og gjennomføringen av dialog mellom aktørene i den finansielle infrastrukturen er Bits. Bits er som tidligere nevnt bank- og finansnæringens infrastrukturselskap og er følgelig en viktig aktør i finanssektoren. Det er de som står for mesteparten av tilretteleggingen av den finansielle infrastrukturen i Norge.

Det er viktig å huske på at finansnæringen også er preget av konkurranse mellom enkelte aktører. I tilfeller hvor et selskap ønsker innsyn hos en konkurrent kan de ikke få det direkte. Ingen er pålagt å dele konkurrentinformasjon. Derimot kan man få indirekte innsyn i systemene ved å sende inn forespørsler og/eller klager til Bits, som deretter kan gjennomføre et tilsyn. Bits inntar i slike tilfeller en rolle som både koordinator og tilsynsorgan. Det er også mulig for Bits å utføre uanmeldte kontroller i likhet med eksempelvis Finanstilsynet.

Bits er hovedaktøren når det kommer til det meste av tilretteleggingen av den finansielle infrastrukturen i Norge. Det er de som regulerer sektoren og dermed også alt som omhandler

betalingsterminaler. For betalingsterminaler er kjeden slik at Bits (1) utvikler spesifikasjoner som de deretter distribuerer til relevante aktører; (2) som tester og verifiserer dem; (3) før de kommer i allmenn bruk. Den nasjonale reguleringen utvikles på grunnlag av regionale og globale standarder. Regionalt er det EU-regelverk som skal følges, mens det globalt er PCI-standarden, også kjent som PCI DSS (Payment Card Industry Data Security Standard), som definerer kravene til Visa og Mastercard. I henhold til PCI skal det dessuten gjennomføres minst en årlig kontroll av rutiner, arbeidsprosesser, teknikk med mer, en såkalt Quality Security Assessment (QSA). I organisasjonen til informant 5 utføres denne minst en gang i året, men noen ganger oftere og gjøres av en ekstern tredjepart som leies inn for anledningen.

Bits fungerer også som en arena hvor aktører møtes for å diskutere aktuelle saker, for eksempel reserveløsningen som er gjenstand for nærmere oppmerksomhet i kapittel 5.3.3.

5.1.4 Et konkurransepreget marked

Finansmarkedet er konkurransepreget og flere av aktørene er i direkte konkurranse med hverandre om markedsandeler. For eksempel leverer BankAxept, Visa og Mastercard betalingskort, mens Nets, Verifone, Zettle, Bambora og SumUp leverer betalingsterminaler. Påvirkes beredskapen av at det er skarp konkurranse i markedet?

Som nevnt ovenfor er det mulig for aktører å forespørre Bits om de kan foreta et tilsyn, hvilket de også gjør hvis det er skjellig grunn til det. Følgelig finnes det en nøytral aktør som har anledning til å kontrollere aspekter som er av interesse for konkurrenter uten at eventuelle bedriftshemmeligheter som skal gi firmaet et konkurransefortrinn settes i fare.

I og med at flere beredskapsoppgaver er delegert til kommersielle aktører kan beredskapsløsningene også bære preg av å være kommersielle. For det første kan det føre til at arbeidet tar tid siden det blir et spørsmål om hvem som skal stå for regningen. For det andre er det et åpent spørsmål hvorvidt beredskapsløsningene er de beste for samfunnet eller om virksomhetene nøyer seg med å iverksette de tiltakene de er pålagt av gjeldende regelverk. Med flere aktører som konkurrerer i et kommersielt marked er det vanskelig å få full oversikt over de som opererer i finansmarkedet. Fordi det er snakk om kommersielle aktører, vil det også kunne påvirke beredskapssammensetningen. De møtes likevel i både formelle og uformelle settinger hvor de går gjennom oppsett og hva de skal gjøre i forskjellige situasjoner. Ofte har de gjensidig interesse av å hjelpe hverandre. Det kan gagne dem selv på sikt. Hvis de hjelper noen i dag, kan de på samme måte motta hjelp ved neste korsvei. De har dessuten felles interesse i at offentlighetens tillit til finanssektoren opprettholdes. I tillegg vil et samarbeid kunne øke

sannsynligheten for at de kan være med på å styre utviklingen av nye bransjekrav og også påvirke når de innføres. Informant 3 bemerket at denne typen samarbeid mellom konkurrenter vil fortsette å fungere all den tid deres kommersielle interesser består, altså at det fortsetter å være enten økonomisk gunstig (økte inntekter og/eller reduserte kostnader) eller at risikoen kan reduseres.

Alle leverandørene som på en eller annen måte er involvert i arbeidet med betalingsterminaler inngår avtaler med kundene sine om servicenivå. Disse kalles Service Level Agreements (SLA) og de stiller tydelige krav til drift, feilretting, oppfølging og rapportering. Dermed er det også et juridisk aspekt i tillegg til det økonomiske. Avtalene legger føringer og/eller begrensninger både for hvilken informasjon som kan deles og hvordan det kan gjøres.

Selv om alle aktører har rapporteringsplikt til relevante myndighets- og tilsynsorganer, som Finanstilsynet, kan kommunikasjonen med organene oppfattes som mer formell og begrenset, særlig når den skjer skriftlig. Informant 3 stilte seg derfor tvilende til at informasjonsflyten fra de kommersielle aktørene til myndighets- og tilsynsorganene flyter så godt som den burde, blant annet fordi beredskap som oftest forstås mest som en utgiftspost. Eventuelle beredskapstiltak og konsekvenser av hendelser må til syvende og sist betales av noen. Kanskje kan det påvirke hvilken informasjon som kommer myndighets- og tilsynsorganene i hende.

Informant 4 hadde ikke inntrykk av at samarbeidet knyttet opp mot cyberforsvar var skadelidende på grunn av markedskonkurransen. Vedkommende pekte på at markedet er underlagt strenge reguleringer og at virksomhetene derfor må etterfølge stadig flere krav.

5.1.5 Andre møtepunkter

Det foregår også dialog utenfor de ovennevnte møtestedene. Det finnes flere interne fora, blant annet i regi av bankene, hvor det skjer tverrorganisatorisk utveksling. Akkurat hva som finner sted i disse har jeg ikke fått kjennskap til ettersom jeg ikke var i kontakt med noen banker. I hvilken grad betalingsterminaler er et diskusjonstema er dermed et åpent spørsmål.

Noe som ikke er et åpent spørsmål er at den samme informanten som deltar i driftsforumet nevnt tidligere i kapittelet bemerket at STIP, prosessen som slår inn hvis terminalen mislykkes i å oppnå kontakt med banken innen et gitt tidsrom, er en løsning mange involvert i den finansielle infrastrukturen misforstår eller ikke forstår fullt ut. Selv om det ofte er mange gjengangere i møtene, vil det ofte være noen nykommere også. Det er ikke alltid tilstrekkelig med tid til å gjennomgå STIP godt nok til at alle nødvendigvis danner seg et tydelig

og riktig bilde av hvordan prosessen fungerer. Informant 1 var også veldig tydelig på at det er helt essensielt å forstå hva STIP går ut på for å få en forståelse av beredskapen for betalingsterminaler. STIP blir redegjort for i kapittel 5.3.2.

Informant 4, som primært jobber opp mot tilsiktede hendelser, fortalte at de er i kontakt med andre organisasjoner både ofte og jevnlig. De er i daglig kontakt med andre aktører på et lavterskelnivå og mottar eller besøker andre organisasjoner på offisielle besøk omkring en gang i måneden. Informanten nevnte spesifikt at samarbeidet med andre organisasjoner fungerer bedre og går raskere hvis de kjenner den aktuelle organisasjonen fra før av. De tar grep for å forbedre samarbeidet med organisasjoner de ønsker å samarbeide med. En fremgangsmåte i den forbindelse er bli kjent-møter. De kan foregå både fysisk og digitalt. Ofte involverer de også en form for sosial omgang, blant annet felles måltider. En annen måte er de allerede nevnte besøkene. Denne organisasjonen deltar dessuten på flere øvelser som utføres i fellesskap med andre organisasjoner, både i Norge og utenlands. Foruten andre aktører i den finansielle infrastrukturen har de også kontakt med relevante aktører utenfor finanssektoren. Dette inkluderer blant annet politiet, telekommunikasjonsaktører og Cyberforsvaret. Noe av hensikten med samarbeidet de fører med eksterne aktører er å danne seg et bilde av hva de har av ressurser for å håndtere cyberangrep. Slik blir informantens organisasjon mer forutsigbare for samarbeidspartnerne deres i og med at de blir kjente med organisasjonens kapasitet og hva de reelt sett kan bidra med i tilfelle cyberangrep eller andre tilsiktede IKT-hendelser.

5.1.6 Manglende kommunikasjonskanaler

Som nevnt i kapittel 4 forsøkte jeg å etablere kontakt med en sentral aktør innenfor mobilbetalinger, men denne organisasjonen avslo å delta på grunn av manglende kapasitet. Ingen av mine informanter ga uttrykk for, verken direkte eller indirekte, at de har utstrakt kontakt med denne aktøren. Dersom det medfører riktighet at dette selskapet mangler kapasitet til å bistå i en oppgave som forsøker å finne forbedringspotensial for beredskapen i dennes sektor, er det å forstå som et funn i seg selv. Selv ikke på direkte spørsmål i oppfølgingsfasen har jeg fått inntrykk av at det er utstrakt kontakt med denne virksomheten, snarere tvert imot. Det later derfor til at det er begrenset hvor involvert den aktuelle aktøren er i forbindelse med betalingsterminaler. Virksomheten er heller ikke representert i BFI, men en informant som selv deltar på møtene i BFI antar at selskapet vil bli en del av BFI etter hvert.

5.2 Interorganisatorisk samarbeid 16. mai 2022

Det andre forskningsspørsmålet var: «Hvordan fungerte det interorganisatoriske samarbeidet mellom aktørene i finanssektoren under bortfallet av betalingsterminalene 16. mai 2022 og hvilken lærdom trakk de ut av det?».

5.2.1 Sammendrag av 16. mai 2022

Gangen i det som skjedde med betalingsterminalene og de konsekvensene det fikk ble kort forklart i kapittel 1.1 og i Tabell II i kapittel 2.4. For ordens skyld er det på plass med en liten oppfriskning av hva som faktisk skjedde. Den følgende fremstillingen bygger på mediebaserte kilder og informasjon informanter har kommet med under intervjuene.

Under ses en samling av bilder og overskrifter som alle ble publisert i forbindelse med 16. mai-hendelsen i 2022. De er hentet fra ulike nasjonale og lokale aviser rundt omkring i landet med innslag fra Kristiansand i sør til Longyearbyen i nord. Avbildet er minibankkøer, kontantbetaling, Carl I. Hagen som ikke fikk kjøpt alle varene han ville og en sportsforretning som stengte i påvente av at betalingsterminalene skulle komme tilbake i funksjon.

Bildekollasjen er laget med bilder og tekst hentet fra Bjørnstad m.fl. (2022), Foss m.fl. (2022), Mortensen og Dahl (2022), NTB (2022a), NTB (2022b), NTB (2022c), Nygaard m.fl. (2022) og Øystå (2022). I tillegg er det hentet overskrifter fra artikler bak betalingsmurer som skjuler artikkelforfatter(ne). Dette gjelder Adressa (2022), Aftenbladet (2022), BT (2022) og S-N (2022).

På formiddagen 16. mai 2022 medførte en nettverksendring hos leverandøren Nets til problemer med mange betalingsterminaler. Nettverksendringen førte til en feil i kommunikasjonen fra Nets og ut til kundene deres i telekommunikasjonsinfrastrukturen. Betalingsterminaler med fast forbindelse, som utgjør omkring halvparten av terminalene i landet, ble rammet av feilen og fikk derfor ikke kontakt med resten av betalingssystemet. Dermed fungerte de ikke (Meld. St. 18 (2022-2023), s. 50). Dette resulterte i lange minibankkøer og problemer med å få kjøpt diverse varer. Noen minibanker gikk dessuten tomme for kontanter (BFI, 2023, s. 5). Særlig en dagligvarekjede og Vinmonopolet ble hardt rammet (Kvatningen m.fl., 2022; Fallmyr m.fl., 2022). Det er opp til hvert enkelt utsalgssted å avgjøre hvorvidt de ønsker å ta i bruk reserveløsning for sine betalingsterminaler og hvilken terminalleverandør de ønsker å bruke. En teknisk feil hos den ene leverandøren førte til at reserveløsningen ikke fungerte i offline-modus i deres betalingsterminaler. Alle brukersteder som brukte terminaler fra den spesifikke leverandøren, ble dermed ofre for en følgefeil og var dermed ute av stand til å ta imot kortbetalinger overhodet (Meld. St. 18 (2022-2023), s. 50). Totalt var det rundt 130 000 norske betalingsterminaler som var berørt av begge feilene samtidig (se f.eks. Jutkvam m.fl., 2022 og Nave m.fl., 2022). At dette inntraff nettopp på 16. mai, må vi anta bidro til å forsterke hvordan allmuen oppfattet hendelsen i negativ forstand. Det store pressefokuset mens det pågikk, og som til dels er gjengitt i bildet ovenfor, underbygger det.

5.2.2 Vurdering av alvorlighetsgraden

Mens dette var en stor sak i det offentlige rom, hadde informantene ulike oppfatninger om hvor alvorlig hendelsen egentlig var.

På den ene siden anså noen informanter dette som en slags storskalaøvelse. Det har utvilsomt sammenheng med at de representerte virksomheter som ikke var direkte involvert i gjenopprettingen og hvor beredskapstiltakene deres fungerte som ventet. På den andre siden forklarte informant 5 at denne hendelsen ble vurdert til å være en 1-hendelse på en skala fra 1 til 5, hvor 1 er den mest alvorlige. Følgelig satte denne virksomheten full krisestab.

Informant 4, som observerte hendelsen utenfra, hadde inntrykk av at hendelsen var begrenset til noen få leverandører og brukersteder.

Hendelsen ble vurdert som alvorlig nok til at den ble omtalt i både Finanstilsynets ROS-analyse for 2023 (s. 39) og i BFIs årsrapport for 2022 (s. 4-5), men samtidig ikke så alvorlig at den fikk særlig spalteplass i noen av rapportene. Det hører med til historien at disse rapportene har begrenset størrelsesomfang og hendelsene vies sjelden mer enn den plassen de behøver for

å beskrive problemet, hva som ble rammet og hvordan det ble løst. Vanligvis er det snakk om et fåtall linjer med tekst.

5.2.3 Forståelse av hendelsen

Innledningsvis i hendelsen ble flere parter involvert for å skaffe seg en forståelse for hva som faktisk hendte. Finanstilsynet har kontakt med Nordic Financial Computer Emergency Response Team (NFCERT) i forbindelse med de fleste sikkerhetshendelser og oppfordrer samtlige aktører, også de som ikke er medlemmer i NFCERT, om å dele informasjon om enhver sikkerhetshendelse med dem (Finanstilsynet, 2023, s. 37). Selv om hendelsen 16. mai 2022 ikke var en sikkerhetshendelse, men en driftshendelse, ble aktører som jobber opp mot sikkerhetshendelser tatt med inn i vurderingsarbeidet. De forstod tidlig at dette ikke var snakk om en sikkerhets- eller cyberhendelse, og var derfor ikke involvert i den videre håndteringen av hendelsen.

Det er dessuten vanlig og forventet at feil meldes inn fortløpende uavhengig av feilens natur, årsak og størrelsesorden. Enkelte ganger vil man ikke vite hvor omfattende en feil kan vise seg å være og derfor meldes samtlige feil inn. Informant 2 nevnte at de har varslingslister som brukes til det formålet. Det er meldeplikt for større hendelser. Eksakt hva som utgjør en større hendelse er litt flytende, men at hendelsen har en varighet på minst en time er et utgangspunkt. Slike hendelser skal meldes inn til informantens organisasjon. Den er blant de som stiller krav til de ulike operatørene i verdikjeden for betalingskort på det norske markedet, som inkluderer selve kortterminalene.

Feilen som forårsaket hendelsen 16. mai 2022 var blitt påpekt i forkant. Den var med andre ord kjent for aktørene og trengte i mindre grad et samspill mellom dem for å få rettet den opp. Det ble tidlig klart for de involverte hvem som måtte gjøre hva for å rydde opp i problemet.

5.2.4 Kommunikasjon

I og med at det tidlig fremstod som tydelig for de involverte hva som var galt og hva som krevdes for å få betalingsterminalene tilbake i normal drift måtte de som var direkte involvert gjøre den jobben de skulle for å få systemene opp igjen. Underveis var det like fullt behov for å kommunisere med andre berørte parter.

Som nevnt ovenfor meldes alle feil fortløpende til relevante aktører. Feilen skal derfor tidlig ha blitt kommunisert ut, men enkelte virksomheter hadde behov for tettere oppfølgning

enn andre. Telekommunikasjonssektoren var involvert ettersom det var deres kabler som var rammet av kommunikasjonsfeilen og leverandøren hadde utstrakt kontakt med dem. Ifølge informant 5 prioriterte denne også kommunikasjon utad til offentligheten mens hendelsen pågikk, så vel som den tekniske håndteringen av situasjonen.

Den samme informanten uttrykte også glede over hvor godt den ene reserveløsningen for betalingsterminaler fungerte. Som jeg dokumenterer i kapittel 5.3.3 ble det gjennomført omkring 800 000 vellykkede transaksjoner med denne reserveløsningen 16. mai 2022.

5.2.5 Endringer i BFIs sammensetning

Kun en av informantene var personlig representert i BFI i løpet av våren 2023 og var derfor den eneste med direkte innsikt i hva som foregår på møtene. Vedkommende oppfattet det ikke som nødvendig å gjøre noen endringer i sammensetningen av BFI på bakgrunn av 16. mai-hendelsen. Hendelsen avdekket ikke noe behov for å ta inn nye medlemmer i utvalget og antydet heller ikke at noen av de eksisterende medlemmene hadde utspilt sin rolle der. På generelt grunnlag påpekte informanten at endringer i sammensetningen kan skje i fremtiden basert på utviklingen på leverandørsiden av den kritiske finansielle infrastrukturen, for eksempel grunnet fusjoner, oppkjøp eller andre markante endringer som påvirker sammensetningen i den finansielle infrastrukturen. På forespørsel ble særlig ett selskap trukket frem som aktuelt for fremtidig medlemskap, nemlig det samme selskapet som ikke hadde kapasitet til å bistå meg i dette prosjektet.

5.2.6 Oppfølging av hendelsen

Som nevnt ovenfor var feilen som forårsaket hendelsen påpekt i forkant av at den inntraff. Av den grunn mente informant 3, som observerte den utenfra, at selv om den garantert ble fulgt opp i etterkant, kan enkelte aktører hatt liten interesse av å gå videre med den. Feilen var kjent fra før av og kunne derfor utbedres uten altfor store diskusjoner.

Representanten for kortselskapet jeg var i kontakt med fortalte at de hadde kontakt med leverandøren av betalingsterminaler som hadde en feil i sine løsninger som medførte at reserveløsningen ikke fungerte på flere av deres terminaler. Denne feilen forsterket problemene hos utsalgssteder som benyttet seg av denne terminaltypen. Kontakten gikk ut på å få klarhet i eksakt hva feilen gikk ut på og hvorfor feilen oppstod. Feilen ble utbedret en måneds tid etter at hendelsen fant sted 16. mai 2022.

Informant 4, som har direkte kjennskap om hva foregår på BFIs møter, bekreftet at hendelsen var gjennomgått i BFI og at det var tatt skritt for å lære av hendelsen. At dette er tilfellet bekreftes også ved at hendelsen er nevnt i utvalgets årsrapport for 2022 (BFI, 2023).

Leverandøren hvor den opprinnelige feilen fant sted rapporterte at de hadde tatt grep og utbedret feilen som skapte problemer for kommunikasjonen på nettverket.

Det er også verdt å minne om at det er rapporteringsplikt og at alle slike hendelser skal meldes inn til Finanstilsynet. Dette inngår i Finanstilsynets vurderinger i forbindelse med deres årlige ROS-analyser. Men som en informant var inne på kan det være i enkelte bedrifters egeninteresse å rapportere på en måte som er fordelaktig for dem selv med tanke på fremtidige bransjekrav.

5.3 Innretting av beredskapen for betalingsterminaler

Det tredje og siste forskningsspørsmålet var: «Hvordan innretter finanssektorens aktører beredskapen for betalingsterminaler?».

5.3.1 Risikoanalyser

Ifølge informant 3, som har bred erfaring fra forskjellige virksomheter i den finansielle infrastrukturen, har finansnæringen nedprioritert beredskapen de siste 20 årene. Beredskapsnivået har stort sett ligget på et minimum av det de er lovpålagt å ha. Dette endret seg imidlertid for et drøyt år siden. Den endrede sikkerhetssituasjonen i Europa etter at krigen i Ukraina startet i februar 2022, som jeg nevnte i kapittel 2.4, bidro til økt bevissthet rundt sikkerhet og beredskap. Informant 4 var også inne på at flere bankkollapser i nyere tid, som Silicon Valley Bank i mars 2023 (se f.eks. Fang m.fl., 2023), kan ha bidratt til økt fokus på beredskap ettersom det er ulovlig å ta risikoer som kan velte bedriften.

Den samme informanten som mente at finansnæringen i lang tid nedprioriterte beredskapen fortalte også at beredskapen hos de kommersielle aktørene generelt sett er innrettet slik at de tar utgangspunkt i spesifiserte hendelser for deretter å vurdere hvordan de kan håndtere dem hvis de inntreffer. Hendelsestypene svinger fra det helt banale, som søling av brus eller annen væske på en betalingsterminal, til det mer omfattende, som langvarig strømbrudd. Aktørene jobber opp mot utsalgsstedene for å vurdere risikoene og iverksette tiltak for å håndtere dem. Informant 2 fortalte at flere kommersielle aktører har bilaterale avtaler seg

imellom og at de utveksler risikoanalysene med hverandre. Disse deles dessuten med Finanstilsynet to ganger i året, vanligvis før jul og påske.

At beredskapen dimensjoneres på bakgrunn av spesifiserte risikoanalyser ble bekreftet av informant 5, som representerte en av de kommersielle aktørene. I denne virksomheten utarbeides risikoanalysene på grunnlag av et rammeverk som setter kriteriene for hvilken type krisestab som skal tas i bruk. Hvilke tiltak som anses som nødvendige avhenger av feilkategoriseringer. Alvorlige feil medfører flere tiltak. Kritiske feil vil føre til at det nedsettes en krisestab. Også hvor mange som berøres av problemet vil ha innvirkning på hvilket tiltaksnivå bedriften legger seg på. I tilfeller hvor det foreligger en mistanke om et problem som foreløpig er uidentifisert vil det, så langt det lar seg gjøre, bli håndtert likt som et kjent problem. Når det settes krisestab skaleres denne opp, fordi de heller vil ha en for stor krisestab for deretter å nedjustere størrelsen på den etter hvert som de får bedre oversikt over situasjonen fremfor å sette en for liten krisestab og risikere å komme bakpå i hendelseshåndteringen.

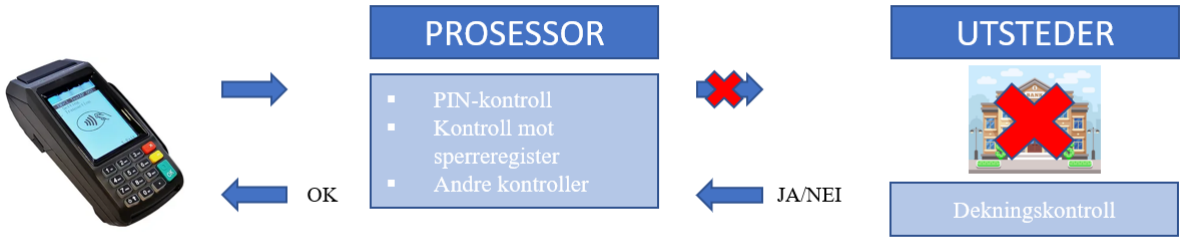
Også aktører som ikke er kommersielle bruker risikoanalyser av spesifikke hendelser som grunnlag for risikostyringen i sektoren. Det overordnede trusselbildet for finanssektoren tegnes på bakgrunn av risikoscenarioene som brukes av Direktoratet for samfunnssikkerhet og beredskap (DSB). Alle hendelsene som DSB har tatt for seg ble analysert av en av aktørene i den finansielle infrastrukturen med særlig blikk på hvordan de kan påvirke finanssektoren, både nasjonalt og regionalt. Deres vurdering var at to til tre av scenarioene kunne påvirke finansnæringen og utarbeidet risikoer og tiltak på bakgrunn av disse vurderingene. Tiltakene de kom frem til har enten allerede blitt gjennomført eller er i ferd med å bli det.

Informant 4 representerer en aktør som tilbyr informasjon om trusselbildet i den finansielle infrastrukturen. Vedkommende fortalte at det er opp til hver enkelt organisasjon å avgjøre hva de gjør med det tilbudet og hvorvidt de ønsker å ta den informasjonen med i betraktningen når de gjennomfører sine risikovurderinger. Hvorvidt finanssektoren vil evne å stå imot særdeles omfattende og krevende hendelser var noe informanten trakk i tvil.

5.3.2 Stand-in processing (STIP)

Et tiltak som er i bruk er det som kalles «Stand-in processing», vanligvis forkortet til STIP. Dette er en beredskapsløsning som skal sørge for at betalingsterminaltransaksjoner gjennomføres selv om deler av betalingsinfrastrukturen har driftsproblemer. I kapittel 2.3 forklarte jeg i korte trekk hvordan en betalingsterminal virker når alt går som det skal. Verdikjeden ble oppsummert i Figur V. I Figur XII, som er å finne nedenfor, er den samme

figuren gjengitt, men i dette tilfellet mislykkes betalingsterminalen i å oppnå kontakt med kortutstederen, det vil si banken eller kredittkortselskapet, for å utføre en dekningskontroll. Dermed er det umulig for betalingsterminalen å vite om kortinnehaveren har tilstrekkelige tilgjengelige midler for å gjennomføre transaksjonen. En mislykket dekningskontroll kan forårsakes av flere grunner. Vanligst er manglende forbindelse som medfører brudd eller forsinkelse i kommunikasjonen mellom prosessor og kortutsteder. Som nevnt i kapittel 2.3 befinner prosessoren seg i et eksternt datasenter. Dette kan ikke bare skape lange køer i butikkene, men i særlig krevende situasjoner også utgjøre en fare for samfunnssikkerheten ved å vanskeliggjøre innkjøp av nødvendighetsvarer. Det er her STIP kommer inn i bildet.



Figur XII. Forenklet transaksjonsflyt uten kontakt mellom betalingsterminalen og kortutstederen.

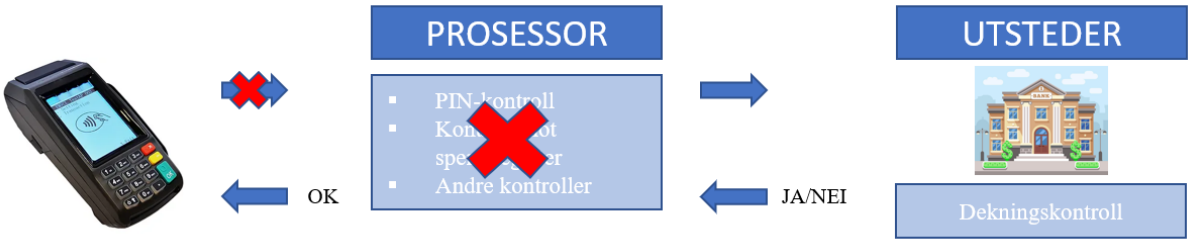
STIP vil slå inn for alle korttransaksjoner unntatt barne- og ungdomskort. Disse utgjør omkring ti prosent av alle transaksjoner. Forklaringen på hvorfor denne korttypen er unntatt følger senere.

Dersom prosessoren ikke oppnår kontakt med kortutstederen i løpet av noen få sekunder, vil STIP aktiveres. Det spiller ingen rolle hvorfor det er manglende kontakt mellom dem. STIP kommer inn uansett og verken kortholderen eller brukerstedet merker noe til at STIP har vært i aksjon. I praksis gjennomføres en STIP-transaksjon ved at prosessoren gjennomfører dekningskontrollen på vegne av kortutstederen på bakgrunn av en beløpsgrense som er satt av den aktuelle utstederen. Fordi terminalen kan godkjenne transaksjoner på kreditt inntil gitte summer, hvor store summer varierer fra kort til kort ettersom beløpsgrensen som nevnt settes av kortutstederen, risikerer kortholderen å gjennomføre et kjøp de ikke egentlig har dekning for. Det er også grunnen til at barne- og ungdomskort er unntatt fra denne ordningen. Tanken er at mindreårige ikke skal risikere å sette seg selv i gjeld på den måten. Når prosessoren etter hvert får kontakt med kortutstederen igjen, overføres transaksjonen til kortutstederen og pengene blir trukket fra kortholderen.

De ferskeste tallene i skrivende stund (juni 2023) tilsier at omtrent 0,2 prosent av transaksjonene i norske betalingsterminaler gjennomføres ved hjelp av STIP. Til sammenligning fikk jeg anslått at andelen lå et sted mellom 0,5 og 1 prosent i 2006. Disse tallene inkluderer planlagt nedetid for vedlikehold eller lignende hos kortutstederen. Det vil også aktivere STIP. 16. mai-hendelsen i 2022 skyldtes problemer knyttet til prosessoren og som figuren ovenfor viser betydde det at STIP ikke var løsningen som avlastet problemene. Det gjorde derimot reserveløsningen.

5.3.3 Reserveløsning

Det finnes flere varianter av en reserveløsning, men den mest utbredte i Norge kommer fra BankAxept. Den fungerte etter planen 16. mai 2022 og sørget for at omkring 800 000 transaksjoner ble gjennomført mens problemene med betalingsterminaler pågikk. Beskrivelsen som følger under, er basert på BankAxepts reserveløsning og den er unik for Norge. Det er opp til hvert enkelt brukersted, det vil si butikkjeder og andre fysiske utsalgssteder, om de ønsker å ha reserveløsning. Utsalgsstedene er ikke pålagt å ha den. Fra et forretningsståsted betyr det at man i verste fall vil være ute av stand til å motta kortbetalinger. Hva det kan resultere i fikk vi demonstrert 16. mai 2022 da enkelte brukersteder enten hadde en reserveløsning som ikke fungerte eller ikke hadde aktivert den. I minibankene var det tilløp til kaos og noen av dem gikk som tidligere nevnt tomme for kontanter. Hva som skal til for at reserveløsningen skal tas i bruk er illustrert i Figur XIII under.



Figur XIII. Forenklet transaksjonsflyt uten kontakt mellom betalingsterminal og tjenesteleverandør.

Reserveløsningen gjør seg gjeldende i tilfeller hvor betalingsterminalen ikke oppnår kontakt med prosessor eller at prosessoren har driftsproblemer. En årsak til dette kan være teknisk svikt, for eksempel at terminalen har mistet nettverkstilgangen. Hva som forårsaker slik teknisk svikt, vil også kunne variere avhengig av om terminalen er fast eller mobil. Forskjellen mellom dem

ble kort beskrevet i kapittel 2.4, men for oppfriskningens skyld kan det kort gjentas at en betalingsterminal med fast tilkobling vil være koblet til systemet på en annen måte enn en terminal med mobil tilkobling. Eksempelvis vil den fastkoblede bruke en nettverkskabel rett inn i terminalen, mens en mobil løsning kan være avhengig av mobildata eller en annen trådløs tilkobling for å fungere. 16. mai 2022 var det kun fastkoblede terminaler som var rammet av feilen som førte til bortfallet. Uavhengig av bortfallets opphav er resultatet det samme. Betalingsterminalen får ikke kontakt med prosessoren og transaksjonsprosessen stopper opp. Det blir umulig å gjennomføre de nødvendige kontrollene som kreves for at den kan starte på neste skritt i kjeden, som er dekningskontrollen hos kortutstederen. Følgelig oppstår dette problemet for tidlig i prosessen til at STIP kan komme inn for å avlaste det, men i disse tilfellene kan reserveløsningen redde transaksjonen. Den gjør det ved å lagre transaksjonsinformasjonen på betalingsterminalen og har derfor ikke behov for ekstern kommunikasjon.

Vanligvis skriver betalingsterminalen ut en debiteringsnota som må signeres av den som betaler kombinert med en manuell kontroll av dennes identitet gjennom fremvisning av gyldig ID, kontroll av signatur og notering av legitimasjonens referansenummer. En oversikt over hva som utgjør de forskjellige ID-enes referansenummer er oppgitt på BankAxepts nettsider og fremgår også av avtalen utsalgsstedet skriver under på for å få tilgang på deres reserveløsning. Notaen er brukerstedets verdipapir som bekrefter at transaksjonen har blitt korrekt gjennomført. Under normale omstendigheter vil transaksjonen gå gjennom som normalt så fort betalingsterminalen på nytt oppnår ekstern kontakt, men dersom terminalen får en permanent funksjonsfeil eller det av andre årsaker besluttes at det er nødvendig å kontrollere transaksjonen må brukerstedet fremvise debiteringsnotaen for å få utbetalt beløpet. Mistanke om svindel er et eksempel på noe som vil resultere i en kontroll av en transaksjon. Det finnes rutiner for å avdekke slik aktivitet. Notaen må videre oppbevares på et trygt sted hvor uvedkommende ikke får tilgang til den i minimum tolv måneder. Prinsippet for kreditt er det samme for reserveløsningen som for STIP. Siden betalingsterminalen ikke får opprettet den kontakten den behøver for å gjennomføre transaksjonen på normal måte må den gi kreditt til kortholderen. Hvis kjøpsbeløpet overstiger 2500 kroner, må transaksjonen manuelt godkjennes av kortusteder. Dette fås per telefon og en autoriseringskode må påføres debiteringsnotaen (BankAxept, 2023b).

Reserveløsningen aktiveres uansett hva som medfører bortfallet i kontakten mellom betalingsterminalen og prosessoren. Den dekker alle tenkelige og utenkelige hendelser fra at internettkabelen har løsnet fra terminalen til at alle satellitter er ute av funksjon som følge av en solstorm, et angrep fra utenomjordiske vesener eller hva som helst. Det spiller ingen rolle

hva årsaken er. Så lenge betalingsterminalen ikke oppnår kontakt med prosessoren vil reserveløsningen være på. Riktignok under forutsetning av at selve betalingsterminalen fortsatt virker. Grunnen til at reserveløsningen også omtales som offline reserveløsning er nettopp fordi den er funksjonell når terminalen er frakoblet internett og/eller betalingssystemet som sådan. Som nevnt i kapittel 2.4 og som informant 1 uttrykkelig poengterte, vil flere typer hendelser medføre bortfall av andre og muligens viktigere tjenester. Hvis kraftnettet kollapser og man blir stående uten strøm over tid, vil andre ting enn betalingsterminaler bli prioritert for umiddelbar utbedring. Enkelte ekstremsituasjoner vil dessuten kunne gjøre betalingssystemet ubrukelig. Det mest åpenbare eksempelet er en invasjon av en fremmed makt som erstatter det norske betalingssystemet med et annet, men da vil oppgaven for å få betalingsterminalene og den øvrige finansielle infrastrukturen opp på beina igjen ligge hos okkupanten forutsatt av at det er noe de har interesse av å gjøre.

Det er forskjell på hvor lenge reserveløsningen fungerer for ulike brukersteder. Ordinær tid er seks timer. Teknisk sett fungerer reserveløsningen utover de seks timene, men hvis noe går galt etter de seks timene står brukerstedet selv for hele den økonomiske risikoen. Innenfor de seks timene tar brukerstedet derimot ingen risiko og er garantert å få oppgjør forutsatt av at selgeren har utført avtalte kontroller, herunder signatur- og legitimasjonskontroll. Mer interessante fra et samfunnssikkerhetsperspektiv er de brukerstedene som kan få tilgang til reserveløsningen i 168 timer, altså syv døgn. Denne løsningen tilbys til nasjonale og regionale utsalgssteder som selger nødvendighetsvarer, altså mat, drivstoff og/eller medisiner. Dermed omfattes dagligvareforretninger, bensinstasjoner og apoteker av denne ordningen. Foruten at det er en nasjonal eller regional kjede som selger nødvendighetsvarer er det også krav om at deres betalingsterminal(er) har kapasitet til å lagre transaksjoner i syv døgn. Dette er viktig fordi samtlige transaksjoner som utføres med offline reserveløsning lagres i terminalen inntil den får kontakt med nettverket igjen og kan prosessere transaksjonene som normalt.

Fra og med 1. juni 2023 fases det inn en oppdatering som skal gjøre reserveløsningen enda lettere og motvirke kødannelser. Alle betalingskort utstedt etter 1. juni 2023 vil kunne ta i bruk offline reserveløsning med PIN i stedet for legitimering ved signatur. Dette forutsetter samtidig at betalingsterminalen også er oppdatert. Alle kortterminaler som allerede har støtte for reserveløsning, vil være oppdaterte innen 1. juni 2024. Oppdateringen vil bli utført av terminalleverandøren og det enkelte brukerstedet trenger ikke å foreta seg noe. I stedet for at det skrives ut en debiteringsnota som må signeres, verifiseres og oppbevares godkjennes betalingen med kortholderens PIN-kode. Der det tidligere kom en nota med plass til signatur- og legitimasjonskontroll vil det i stedet stå «Godkjent med PIN». Ikke bare skal dette gjøre

reserveløsningen raskere, enklere og mer effektiv i bruk, men skal også gjøre prosessen sikrere. Dette blir faset inn i det norske markedet over en treårsperiode og skal være fullstendig implementert 1. juni 2026 når alle betalingskort utstedt før 1. juni 2023 har utløpt og blitt erstattet av nye kort.

Andelen reserveløsningstransaksjoner ligger normalt på rundt 0,05 til 0,1 prosent, men 16. mai-hendelsen økte den til 0,57 prosent. Som nevnt ble rundt 800 000 transaksjoner gjennomført ved hjelp av offline reserveløsning den dagen. Til sammenligning ble andelen reserveløsningstransaksjoner anslått til å ligge mellom 1 og 2 prosent i 2006.

5.3.4 Kriseledelse

Reserveløsningen er et beredskapstiltak som bidrar til at betalingsterminalene skal fungere selv når det av en eller annen grunn er kluss ett eller flere steder i verdikjeden. Hvis det oppstår en krise krever det ofte mer enn å satse på at reserveløsningen klarer brasene. Hvordan avgjør aktørene hvilket beredskapsnivå de skal legge seg på under en krise og hvordan settes kriseledelsen sammen?

Noe er allerede redegjort for i kapittel 5.3.1 i forbindelse med ene organisasjonens rutiner for krisestab. Hvilket beredskapsnivå bedriften til informant 5 legger seg på avhenger av graden av berørte parter. Jo flere berørte parter, jo høyere beredskapsnivå. Hvis dette overgår en viss grense, blir det satt krisestab. Det som kan legges til her er at den krisestaben som iverksettes er tydelig definert ut fra hva slags krise de har med å gjøre. Den er også separert slik at de har en for interne forhold, det vil si feilsøking, -gjenoppretting med mer, og en for kommunikasjonen utad. Den siste vil være i kontakt med andre organisasjoner og eventuell presse.

Tilsvarende har organisasjonen til informant 4 også tydelige rutiner for hvilket beredskapsnivå de legger seg på under en krise. De tilpasser nivået sitt ut fra hvor kritisk en hendelse kan utvikle seg til å bli, men de har også hensyn til hvordan medlemmer og andre samarbeidspartnere oppfatter situasjonen. Denne organisasjonen tar sikte på å legge seg på det samme beredskapsnivået som dem. Hvis de vurderer hendelsen som mer alvorlig enn informantens organisasjon, fortalte informanten at de forsøker å matche medlemmenes og samarbeidspartnernes beredskapsnivå. Som jeg beskriver nærmere i neste underkapittel er det daglige virket i denne virksomheten innrettet ganske likt som i en krisesituasjon og øvelser. De har også klart definerte roller i kriseledelsen som følgelig samsvarer med den rollefordelingen de har i normalsituasjoner.

5.3.5 Egne øvelser

Det kommersielle selskapet til informant 5 gjennomfører øvelser på egenhånd i tillegg til sammen med andre. Noen ganger fremprovoserer de feil i systemene for å finne ut av hvordan beredskapsløsningene fungerer i praksis. De har egne nødaggregater i form av to til tre helikoptermotorer som skal sikre strømforsyningen til datasentrene og annen kritisk virksomhet som kreves for å drifte betalingsterminalene i lang tid ved et eventuelt omfattende strømbrudd. De skal også sørge for at de kan foreta kontrollerte nedstengninger dersom det blir behov for det. Øvelsene deres er ment å forberede dem på redundante datasentre og også bistå dem med tanke på datasentrenes skalerbarhet. Bedriften jobber primært med to datasentre hvor den aktive har mulighet til å trigge den passive, mens den passive kan sørge for økt kapasitet ved behov. De skalerer opp og ned ut fra forventninger om aktivitet. I forbindelse med handelsdagen Black Friday skalerer de for eksempel betydelig opp. Øvelsene de gjør i egen regi er ofte knyttet opp mot skalerbarhet og redundans, slik at betalingsterminalene til enhver tid er funksjonelle samtidig som driften av dem ikke krever for mye kraft.

Den samme virksomheten leier tidvis også inn eksterne som skal gjennomføre datainnbrudd hos dem. Samtlige ansatte i selskapet blir dessuten underlagt et treningsprogram som skal hjelpe dem med å avdekke scam-, phishing-angrep og lignende. De har en egen avdeling som fra tid til annen sender ut denne typen meldinger for å øke oppmerksomheten og bevisstheten blant de ansatte, samt for å lære dem opp slik at de blir flinkere til å oppdage reelle forsøk. Den ansattes posisjon i selskapet er irrelevant i denne sammenhengen. Absolutt alle ansatte mottar disse meldingene.

Denne bedriften var den jeg fysisk gjennomførte intervjuet hos, og det var tydelig at de hadde sikkerheten på området i tankene. Det var satt opp fysiske barrierer med adgangskontroll (inngangskort) hvis man skulle komme seg særlig forbi resepsjonsområdet. Hvordan dette er løst ved de øvrige informantenes fysiske arbeidsplasser fikk jeg ikke observert ved selvsyn i og med at jeg ikke var til stede for å gjennomføre intervjuene der.

Informant 4, som jobber opp mot tilsiktede hendelser, fortalte at de har jevnlige øvelser, men at de som oftest skjer i samarbeid med andre. Gitt organisasjonens natur er ikke det overraskende. Av samme grunn er mye av det de gjør i øvelser og hendelser mer preget av at arbeidsoppgavene stort sett ligner på den daglige driften. Det som har størst sjanse for ikke å være rutinepreget i tilfelle en hendelse, er det eventuelle behovet for mediehåndtering og kommunikasjon utad.

Kortselskapet jeg var i kontakt med fortalte at de setter tydelige testkrav til betalingsterminalene. Enhver terminal som kommer med støtte for reserveløsning skal kontrolleres før den tas i bruk. Ellers setter de og Bits krav til hvordan betalingsterminalene skal fungere og de krever at det etterleves. De gjennomfører altså ikke øvelser relatert til betalingsterminaler på egenhånd, men overlater det ansvaret til leverandører og brukere.

5.4 Oppsummering

I løpet av dette kapittelet har jeg presentert det empiriske materialet jeg har samlet inn ved hjelp av intervjuer og kontakt med personer som jobber i den finansielle infrastrukturen. Det var organisert slik at hvert delkapittel tok for seg ett forskningsspørsmål med tilhørende underkapitler for å gjøre det mer leselig og systematisert. Dette kapittelet danner grunnlaget for det neste kapittelet. Der skal det empiriske materialet drøftes i lys av oppgavens teoretiske rammeverk: resiliens i form av DRMG.

6 Drøfting

Drøftingen i dette kapittelet tar utgangspunkt i funnene som ble presentert i forrige kapittel og teorien jeg redegjorde for i kapittel 3. Med utgangspunkt i teoriene om resiliens og DRMG ser jeg nærmere på empirien for å komme nærmere et svar på hvorvidt anvendelse av konsepter innen resiliens kan forsterke beredskapen for norske betalingsterminaler. Kapittelet er organisert i henhold til forskningsspørsmålenes rekkefølge og samsvarer dermed med organiseringen av både det foregående kapittelet og presentasjonen av de brukte kapabilitetskortene i kapittel 3.3. Følgelig drøfter jeg først hvordan finanssektoren har tilrettelagt for å fremme tverrorganisatorisk felles forståelse, etterfulgt av hvordan det interorganisatoriske samarbeidet fungerte under 16. mai-hendelsen i 2022 og til slutt hvordan beredskapen for betalingsterminalene er innrettet i den finansielle infrastrukturen. Hvert delkapittel innledes med en repetisjon av det aktuelle forskningsspørsmålet.

6.1 Fremme tverrorganisatorisk felles forståelse

«Hvordan legger aktørene i finanssektoren til rette for å fremme felles forståelse på tvers av organisasjoner i forbindelse med beredskapen for betalingsterminaler?» var

forskningsspørsmålet som legger grunnlaget for den følgende drøftingen. Spørsmålet tok utgangspunkt i kapabilitetskortet for å fremme felles forståelse for tverrorganisatorisk samarbeid i krisehåndtering.

Som nevnt i kapittel 3.3.2 muliggjøres kapabilitetskortet for å fremme tverrorganisatorisk felles forståelse av at det allerede er etablert nettverk for det (DARWIN, 2018, s. 14). At Beredskapsutvalget for finansiell infrastruktur (BFI) finnes og er i drift ble brukt som argumentasjon for å se nærmere på dette kortet. Funnene viser at det ikke bare er BFI som er et etablert nettverk i finanssektoren. Det finnes flere møteplasser hvor aktørene kan møtes både formelt og uformelt.

BFI er det mest formelle organet hvor dette foregår. Alle medlemmer har møteplikt og man skal ha gode grunner for å melde forfall. Det er også tydelig at ansatte som ikke personlig deltar på BFIs møter har en viss grad av innsikt i det som skjer av aktivitet der gjennom kollegaer som sitter i utvalget, men utstrekningen av dette varierer fra organisasjon til organisasjon. Dette er gjenstand for en kort diskusjon i neste delkapittel. I denne sammenhengen er det av større interesse at BFI organiserer felles kriseforberedende øvelser. Dette skjer minst en gang i året og temaet for øvelsen endrer seg fra år til år. Arrangøren av beredskapsøvelsen roterer også. Det kan bidra til at deltakerne over tid blir bedre kjent med hvordan de andre medlemsorganisasjonene arbeider. Disse rutinene oppfyller langt på vei en av kapabilitetskortets anbefalinger om å organisere felles kriseforberedende øvelser. Gjennom øvelsene blir deltakerne blant annet kjent med hverandres terminologi og ressursbruk, slik anbefalingen tar til orde for (Ibid., s. 15). Dermed er det rimelig å anta at risikoen for misforståelser og tvetydighet i en krisesituasjon er redusert på et overordnet nivå. Men kapabilitetskortet er ment å tilrettelegge for at alle involvert i krisehåndteringsarbeidet skal bli kjent med andre organisasjoners arbeidsrutiner, ressursbruk med mer (Ibid., s. 14 & 17). Det er ikke tilfellet med BFIs kriseøvelser. Hver organisasjon deltar med maksimalt et fåtall personer. Dessuten fremstår det som tilfeldig i hvilken grad medlemsorganisasjonene sprer kunnskapen de erverver seg der med kollegaene i egen organisasjon. Samtidig er det verdt å understreke at øvelsen i 2017 bidro til en utvidelse av reserveløsningen. Øvelsene fungerer tilsynelatende godt i den forstand at de er med på å oppdage hull i beredskapen, men det er mer relevant for kapabilitetskortet for å oppdage skjørhet (Ibid., s. 91) enn det som er tilfellet her. Kanskje kan det være et tema for videre studier.

Det virker ikke som om BFI arrangerer noen workshops eller andre arrangementer for å tilrettelegge for informasjonsdeling og felles forståelse, slik det aktuelle kapabilitetskortet anbefaler (Ibid., s. 14-15). Riktignok er en av BFIs oppgaver å varsle og informere ved

hendelser (Finanstilsynet, 2010), men det ser ikke ut til at utvalget gjør grep som skal være forebyggende på den måten DARWIN legger opp til. Her kommer andre arenaer på banen, blant annet Driftsforum for XYZ verdikjede. Som navnet tilsier, består driftsforumet av organisasjoner tilknyttet betalingskortets verdikjede. Ettersom møtevirksomheten blant annet tar for seg både det som allerede har skjedd og det som planlegges å skje fungerer møtene godt med tanke på at medlemmene skal få et tydelig overblikk over alt som foregår i verdikjeden. Det betyr at aktørene kan tilpasse aktivitetene sine basert på hva de andre foretar seg og følgelig redusere risikoen for at feil oppstår eller forsterkes som følge av sviktende kommunikasjon. Driftsforumet er et eksempel på en type nettverk som deler informasjon og later til delvis å oppfylle anbefalingen om å organisere workshops for informasjonsdeling (DARWIN, 2018, s. 14-15). Det gjennomføres ikke den typen aktiviteter som kapabilitetskortet anbefaler, eksempelvis presentasjoner som redegjør for den enkelte organisasjonens arbeidsmetoder, tilgjengelige ressurser osv., men kan fungere som en kryssfertilisering mellom de deltakende organisasjonene (Ibid., s. 15). Kryssfertilisering viser til en utveksling som tilrettelegger for utvidelse og/eller produktivitet på tvers av ideer, kulturer og kategorier (Merriam-Webster, 2023). Verdikjeden for betalingskort er, som vist i kapittel 2.3, lang og inkluderer mange parter. Siden driftsforumet inkluderer aktører i hele verdikjeden og utfører et viktig arbeid med å spre bevissthet på tvers av organisasjonene må det sies å være en tilrettelegger for nettopp kryssfertilitet og derigjennom delvis oppfylle kapabilitetskortets anbefaling (DARWIN, 2018, s. 15 & 22).

Også andre møteplasser finnes, men jeg har ikke sett noen indikasjoner på at disse er innrettet med et særlig blikk på å fremme felles tverrorganisatorisk forståelse. Det later heller til at det er litt vilkårlig hva som blir gjort i det henseende. Dessuten virker det som om det er stor grad av variasjon med tanke på forklaring av begrepsbruk. STIP er et system som flere misforstår. Det er forståelig at det ikke alltid er tid til å forklare hva det går ut på for de som trenger en innføring eller oppfriskning, men det fremstår som mer eller mindre tilfeldig når slikt blir forklart og når det ikke blir det. Dermed er det tenkelig at dette også gjelder for andre faguttrykk og terminologier og kan i verste fall føre til misforståelser i kritiske situasjoner. I den akutte krisefasen fremhever Hollnagel m.fl. (2011) at det er viktig å kunne skille mellom det som haster og det som er viktig (s. 284). Manglende forståelse på tvers av organisasjonene kan bidra til en redusert evne for dette og i verste fall medføre redusert effektivitet i krisehåndteringen, slik Hollnagel m.fl. (2011) advarer mot (s. 283).

Aktørene i den norske finanssektoren later til å være flinke til å besøke hverandre, slik kapabilitetskortet legger opp til (DARWIN, 2018, s. 15), men det skjer som oftest i egen regi

og ikke som et ledd i et målrettet arbeid i et etablert nettverk. Det betyr at vilkårligheter avgjør hvilke organisasjoner som har god innsikt i andre aktørers ressurser og prosedyrer. De pålagte årlige kontrollene (QSA-ene) som aktørene påkreves kan ikke regnes med i denne sammenhengen. For hver enkelt aktør blir dette dermed et ressursspørsmål. Dermed er det den interne politikken i hver organisasjon som avgjør hvorvidt dette prioriteres og det kan være vanskelig å rettferdiggjøre å bruke ressurser på dette i førkrisefasen (Ibid., s. 14). Hvis det medfører riktighet at den ene aktøren ikke hadde kapasitet til å snakke med meg i et kvarter, som var den tilmålte tiden jeg spurte om, oppfatter jeg som urovekkende. Jeg kan ikke avskrive muligheten for at det var en unnskyldning for å slippe å snakke med meg, men jeg må forholde meg til den informasjonen jeg blir servert. I så fall er det liten grunn til å tro at denne virksomheten vil ta initiativ på egenhånd for å fremme felles forståelse eller andre aktiviteter som forsterker beredskapssamhandling. Kanskje har også andre aktører manglende kapasitet og ressurser til å delta på denne typen aktiviteter. Virksomheter som befinner seg i en slik posisjon kan ha godt av å være del av et organ hvor de i mindre grad behøver å ta initiativ selv.

Jeg mener at beredskapsevnen for betalingsterminaler kan forsterkes ved å ta i bruk DRMG i den hensikt å fremme felles tverrorganisatorisk forståelse for krisehåndteringsarbeidet. Dette foregår allerede på noen arenaer, men som diskusjonen ovenfor viser virker dette arbeidet å være preget av tilfeldighet. Med tilfeldighet mener jeg i denne sammenhengen at det ikke er et bevisst fokus på å fremme felles tverrorganisatorisk forståelse. Det er heller å forstå som et ubevisst biprodukt av arbeidet som foregår på de forskjellige møteplassene og i de ulike nettverkene. Min anbefaling er derfor at man enten utvider BFIs mandat eller får på plass et organ dedikert til tverrorganisatorisk samarbeid hvor en av arbeidsoppgavene bør være å fremme tverrorganisatorisk forståelse. Det beste vil antakelig være å opprette et nytt organ som i tillegg tar over denne ansvaret for å varsle og informere ved behov og dermed kan avlaste BFI, men dette bør finanssektoren selv gjøre en vurdering av. Opprettelsen av et forum eller annen type nettverk kan skje ved hjelp av kapabilitetskortet for nettverksetablering (Ibid., s. 23-33). På den måten vil det ligge et bevisst arbeid til grunn som vil være målrettet og sannsynligheten for at aktører nedprioriterer deltakelse i denne typen arbeid reduseres fordi det blir mindre ressurskrevende for dem å delta. Beredskapsarbeidet vil følgelig ha gode forutsetninger for å forbedres og effektiviseres. For virksomhetene kan resultatet bli at de totalt sett bruker mindre ressurser på beredskapsarbeidet siden de vil få bedre oversikt over hvordan de øvrige organisasjonene kan komplementere deres ressurser og vice versa. På den andre siden kan det også avskrekke enkelte organisasjoner fra deltakelse i og med at noen av deres konkurrenter kan spekulere i dette for å øke sin egen profitt på deres

bekostning. Eksakt hvordan en etablering skal foregå må avklares, men siden flere bedrifter har forpliktende kontrakter med hverandre på andre områder kan noe lignende være en mulig løsning. Sannsynligvis blir det lettere for de nyankomne i de ulike organisasjonene å få en helhetlig oversikt over ulike faguttrykk og annen relevant terminologi siden de gjennom det nye nettverkets arbeid kan få langt større innsikt i og kjennskap med andre relevante aktører i bransjen fremfor at det skjer når man har tid til det.

Til slutt er det verdt å legge til at det finnes flere arenaer for erfarings- og informasjonsutveksling i finanssektoren utover BFI og de later til å fungere godt. Kanskje er det mulig å utvide mandatet til et av disse organene for å koordinere det tverrorganisatoriske samarbeidet i stedet for å etablere et nytt. Muligens oppfatter også finanssektoren det foreslåtte tiltaket som overflødig og til dels også som utfordrende med tanke på at bedrifter må ha anledning til å tilbakeholde informasjon fra konkurrentene sine. Uansett vurderer jeg det dithen at beredskapsevnen i finanssektoren hemmes av at det ikke eksisterer et organ som koordinerer og tilrettelegger for det tverrorganisatoriske samarbeidet, herunder også den tverrorganisatoriske forståelsen. Dette vil ikke kun være til gagn for beredskapsevnen tilknyttet betalingsterminaler, men hele den norske finansielle infrastrukturen.

Det neste delkapittelet tar også for seg et kapabilitetskort med det samme forutgående kravet. Siden jeg allerede har tatt til orde for at det bør etableres et organ som målrettet skal tilrettelegge for tverrorganisatorisk samarbeid, vil det ikke komme som noen overraskelse at det også gjelder der, men en diskusjon om eksakt hva som kan forbedres og hvordan det kan gjøres er like fullt på sin plass.

6.2 Interorganisatorisk samarbeid 16. mai 2022

«Hvordan fungerte det interorganisatoriske samarbeidet mellom aktørene i finanssektoren under bortfallet av betalingsterminalene 16. mai 2022 og hvilken lærdom trakk de ut av det?» var det andre forskningsspørsmålet og er utgangspunktet for drøftingen i dette delkapittelet. Det ble skapt på grunnlag av kapabilitetskortet om å dele informasjon om roller og ansvarsområder blant organisasjonene involvert i krisehåndteringen.

Først og fremst må jeg innrømme at jeg gikk inn i denne oppgaven med en oppfatning om at 16. mai-hendelsen i 2022 var alvorligere enn den reelt sett var. Derfor krevde ikke hendelsen like stor grad av interorganisatorisk samarbeid som jeg så for meg da jeg lagde forskningsspørsmålet og det er jo et funn i seg selv. De empiriske dataene bærer likevel preg av det. Som jeg problematiserte i metode-kapittelet kan det faktum at informantene selv er

insidere i finanssektoren bidra til at materialet jeg samlet inn er noe skjevt og ikke forteller den fulle og hele sannheten. Samtidig er den historien som har blitt fremlagt for meg vært konsistent fra alle informantene og derfor er det grunn til å tro at hendelsen ikke var på langt nær så alvorlig som man kunne få inntrykk av i avisene mens den pågikk og umiddelbart etterpå. Resultatet er at det følgende delkapittelet kan være av begrenset verdi for å vurdere hvordan det interorganisatoriske samarbeidet i den norske finanssektoren faktisk fungerer når en uønsket hendelse inntreffer og hvordan den følges opp for å lære av den. Om ikke annet bør det i hvert fall gi en indikasjon på hvordan resiliens kan forbedre beredskapsevnen i den finansielle infrastrukturen. Vel og merke hvis det faktisk er noe å forbedre.

I førkrisefasen er det viktig at det finnes møteplasser hvor representanter for organisasjonene kan utveksle informasjon (Ibid., s. 34). Som dokumentert i kapittel 5 og drøftingen relatert til å fremme felles tverrorganisatorisk forståelse eksisterer det flere møtearenaer hvor dette foregår. Hvorvidt virksomhetene forsøker å følge resiliens-tankegangen generelt eller retningslinjene anbefalt av DRMG spesielt undersøkte jeg ikke og kan derfor ikke uttale meg sikkert om akkurat det. Men basert på den øvrige drøftingen i dette kapittelet er det liten grunn til å tro at så er tilfellet. For eksempel jobbes det nærmest utelukkende opp mot spesifikke hendelser og derfor er det lite sannsynlig at organisasjonene har koordinert roller og ansvarsområder for generiske kriser, slik kapabilitetskortet for å forsterke kapasiteten overfor ventede og uventede hendelser anbefaler (Ibid., s. 47).

Det jeg har bedre grunnlag for å uttale meg om er at 16. mai-hendelsen ble forstått svært ulikt av aktørene og det henger sammen med hvordan de opplevde den. Det indikerer at de ulike organisasjonene hadde en god forståelse av hva deres rolle var og hvilke ansvarsområder de hadde mens hendelsen pågikk. Tidlig i hendelsesforløpet ble flere aktører involvert for å få fullstendig klarhet i hva som skjedde. Dette tyder på at *sensemaking* prioriteres under hendelseshåndtering og selv om denne krisen ikke viste seg å være særlig skyggebelagt (Klein, 2009, s. 10) var ikke det gitt innledningsvis. Dette underbygges av at en virksomhet eksplisitt fortalte at de håndterer ukjente problemer som kjente inntil de får bedre oversikt over situasjonen. De bedriver *sensemaking*. Denne tilnærmingen er i tråd med ideer om resiliens (Steen m.fl., 2023, s. 1). Problemet 16. mai 2022 ble raskt identifisert og kategorisert som en driftshendelse. Fremgangsmåten forstår jeg som helt i tråd med den Klein legger opp til. I stedet for å avvente situasjonen i påvente av tilstrekkelig og/eller god nok informasjon valgte de å gå bredt ut fra starten og være proaktive. Den passiviteten som Klein advarer mot ble dermed unngått (Klein, 2009, s. 151). Hele finansnæringen lot til å gå fullt og helt inn for å få oversikt over hendelsen så raskt som mulig og satte alle kluter til i det henseende fremfor å komme

bakpå i påvente av mer og/eller bedre informasjon. Etter at problemet var identifisert ble det også klart at det var kjent. Det var altså en hendelse de hadde erfaring med å håndtere. Dermed var det begrenset hvor utstrakt det interorganisatoriske samarbeidet i realiteten ble. De fleste visste hva som måtte gjøres for å rette opp i feilen og hvem som måtte utbedre den. Følgelig fremstår det som tydelig at aktørene i den finansielle infrastrukturen har et klart bilde på hvem som gjør hva når det oppstår hendelser de har erfaring med, slik det gjorde 16. mai 2022. At det var kontakt mellom organisasjonene underveis viser dessuten at de hadde kontroll på hvem som skulle kontaktes under en krise. Kortselskapet hadde for eksempel kontakt med den terminalleverandøren som hadde en feil som gjorde reserveløsningen defekt for å få oversikt over problemets natur. Dermed er det tilstrekkelig grunnlag for å hevde at de generelle anbefalingene om hvem som skal kontaktes og hva aktørene bør ha god nok kjennskap om langt på vei er oppfylt (DARWIN, 2018, s. 34), ikke minst fordi BFI også har nettopp varsling blant sine ansvarsområder. De vet hvem som skal kontaktes i en krise, hva de relevante rollene for håndteringen av en spesifikk krise er og hvilke ansvarsområder som er de viktigste for de rollene. Der det derimot skorter på etterlevelsen av resiliens i denne sammenhengen er oversikten over roller og de tilhørende ansvarsområdene i den akutte krisefasen. Det kan ikke vurderes på bakgrunn av 16. mai-hendelsen, men inntrykket mitt er basert på den tilsynelatende totale mangelen på å innrette beredskapen for generiske kriser, som er gjenstand for diskusjon i neste delkapittel.

I etterkant ble hendelsen gjenstand for oppmerksomhet i relevante fora. Den ble viet plass både i BFIs årsrapport for 2022 (BFI, 2023, s. 4-5) og Finanstilsynets ROS-analyse for 2023 (Finanstilsynet, 2023, s. 39). Et BFI-medlem bekreftet at hendelsen var diskutert der og at det var tatt grep for å lære av den. Det fremgår ikke at det ble arrangert ekstraordinære møter eller andre aktiviteter for å diskutere denne hendelsen spesifikt eller for å finne ut av om det var behov for å revurdere rollefordelinger og ansvarsområder, slik kapabilitetskortet mener er påkrevd i etterkant av en krise (DARWIN, 2018, s. 37). Dette henger mest sannsynlig sammen med at hendelsen ikke var alvorlig nok til at det ble ansett som nødvendig. Dessuten tyder det meste på at det ikke forekommer noen bevisst og målrettet koordinering som samsvarer eller ligner på de anbefalingene som finnes i DRMGs retningslinjer. Det er vanskelig å arrangere koordineringsmøter hvis tanken aldri har slått en.

Siden graden av interorganisatorisk samarbeid for å håndtere situasjonen var langt mindre enn jeg i utgangspunktet forventet, er det også begrenset hvor mye det var å lære av hvordan samarbeidet fungerte. Likevel var det noe interaksjon mellom de involverte og, som Hollnagel påpeker, er det kun der et system opererer i et helt stabilt og forutsigbart miljø at det

ikke finnes grunnlag for læring (Hollnagel, 2018, s. 36). 16. mai-hendelsen viser helt tydelig at miljøet norske betalingsterminaler drives i ikke kan karakteriseres som helt stabilt og forutsigbart. I så fall ville ikke hendelsen funnet sted. Følgelig bør det være mulig å lære noe av hendelsen og dermed redusere sjansen for at lignende uønskede hendelser oppstår og/eller forsterke evnen til å håndtere fremtidige utfordringer (Steen m.fl., 2023, s. 3). Noen grep har blitt tatt i finanssektoren på bakgrunn av hendelsen, men det handler først og fremst om å utbedre feilens opphav, slik at den ikke oppstår på nytt. Det gjelder både for tjenesteleverandøren hvor den opprinnelige feilen oppstod og hos terminalleverandøren hvor en annen feil forverret situasjonen. Hvorvidt dette er utbedret på en måte som gjør at feilen ikke vil føre til et nytt bortfall får tiden vise. Sånn sett kan man si at akkurat dette er i overensstemmelse med Hollnagels poeng om at det er viktigere å vite hvorfor noe skjedde enn hvor ofte det skjedde (Hollnagel, 2018, s. 37). Utbedring av tekniske feil er likevel på siden av den læringen jeg var ute etter. Jeg var interessert i hva de lærte av det interorganisatoriske samarbeidet. Det later til å ha fungert fint i den utstrekning det var snakk om noe interorganisatorisk samarbeid. Jeg fikk ikke inntrykk av at kontakten mellom aktørene var problematisk, verken under eller etter hendelsen – heller tvert imot. Kanskje er det derfor jeg i liten grad har fått inntrykk av at man gjorde noe for å lære av samarbeidet? At holdningen i sektoren er at de skal lære av det som ikke fungerte fremfor det som faktisk fungerte? Hvis det er tilfellet tyder det på at resiliens ikke utgjør noen betydelig del av sikkerhetsarbeidet, ettersom det i dette perspektivet er vel så viktig å lære av det som fungerte som det som ikke fungerte (Steen m.fl., 2023, s. 4), men kildegrunnlaget er altfor tynt til å si noe sikkert om den saken.

Når det gjelder å vurdere endringer i medlemsmassen i relevante grupper, som også er en anbefaling i etterkrisefasen (DARWIN, 2018, s. 37), ble det ikke vurdert som nødvendig å gjøre noen utskiftninger som følge av 16. mai-hendelsen i BFI. Utvalget gjør derimot jevnlig vurderinger som medfører at nye medlemmer innlemmes og eksisterende medlemmer fjernes. BFI lever sånn sett opp til det retningslinjene anbefaler i den forbindelse og selv om varsling og informering er blant utvalgets oppgaver, er det samtidig ikke et koordineringsorgan spisset inn mot samarbeid på tvers av organisasjoner på lik linje med det som anbefales av DRMG. Kanskje bør BFIs mandat utvides eller kanskje driftsforumet for verdikjeden til betalingskort er en mer passende kandidat, men det beste ville vært om det ble etablert et dedikert organ med utgangspunkt i retningslinjene (Ibid., s. 23-33), som jeg argumenterte for i forrige delkapittel.

Totalt sett er det vanskelig å vurdere hvor godt informasjonsdelingen knyttet til fordelingen av roller og ansvarsområder fungerte under 16. mai-hendelsen i 2022. Til dels fordi jeg innledningsvis overvurderte dens alvorlighetsgrad, men også delvis fordi finanssektoren i

liten grad later til bevisst å ta med resiliens-perspektiver i sitt beredskapsarbeid. Som jeg tok til orde for i forrige delkapittel kunne et organ dedikert til å koordinere og tilrettelegge for samarbeid på tvers av organisasjonene forbedret og effektivisert beredskapsevnen til både finanssektoren generelt, men også betalingsterminaler spesielt. Ved hjelp av en mer helhetlig tilnærming og bruk av resiliens ser jeg et forbedringspotensial for informasjonsdelingen i den norske finansielle infrastrukturen.

6.3 Innretting av beredskapen for betalingsterminaler

«Hvordan innretter finanssektorens aktører beredskapen for betalingsterminaler?» var det siste forskningsspørsmålet og danner bakteppet for drøftingen som følger i dette delkapittelet. Dets utgangspunkt var kapabilitetskortet som går ut på å forsterke kapasiteten for å tilpasse seg overfor både ventede og uventede hendelser.

I kapittel 5.3.1 dokumenterte jeg hvordan beredskapsplanleggingen i den norske finansielle infrastrukturen fremstår utad. Gjennomgangsmelodien er at den gjøres med basis i tradisjonelle risikoanalyser, for eksempel ROS-analyser. Ingen av informantene nevnte at det ble utført mer omfattende analyser, slik som beredskapsanalyser. Det kan være tilfeldig eller forglemmelser fra deres side, men kan også tyde på at finanssektoren stort sett holder seg til risikoanalyser når de utarbeider beredskapen generelt og for betalingsterminaler spesielt. Kanskje kan det ses i lys av at beredskapsinnsatsen på feltet de siste 20 årene har vært innrettet etter de pålagte kravene og ikke så mye mer, men det blir for spekulativt å forfølge den tanken. Finansnæringen er uansett ikke lovpålagt å utføre noe utover risikoanalyser så lenge de følger norske og internasjonale standarder (Forskrift om systemer for betalingstjenester, 2019, § 4). Årsaken kan like gjerne være at eksempelvis beredskapsanalyser er overflødige i den forstand at omfanget til en hendelse som rammer betalingsterminaler ofte krever færre ressurser enn store kriser som setter liv i umiddelbar fare. Behovet for en gjennomarbeidet beredskapsanalyse vil antakelig være større for en bybrann enn et langvarig bortfall av betalingsterminaler. Bybrannen i Ålesund i 1904 førte for eksempel til at 850 hus brant ned og over 10 000 ble hjemløse, mens kun 230 hus forble uskadde av brannen som varte i 15 timer (Kjølås, 2021).

Viktigere enn å spekulere i hvorfor risikoanalyser foretrekkes fremfor beredskapsanalyser er det for denne studien at informantene var samstemte i at beredskapsarbeidet tar utgangspunkt i spesifiserte hendelser. Det later til å være et bredt spekter av hendelser som analyseres på flere nivåer. Ikke bare involveres brukerstedene i arbeidet, men risikoanalysene deles også mellom aktørene til gjensidig nytte. Finanstilsynet får også innsyn i

dem to ganger i året og kan dermed ta dem med i sine beregninger når de utvikler sine årlige ROS-analyser. Alt tyder på at finanssektoren holder seg til det Hollnagel omtaler som beskyttende sikkerhet (Hollnagel, 2018, s. 6-7 & 15) i sitt beredskapsarbeid og som Klein (2009) mener er utilstrekkelig og i verste fall skadelig i møte med komplekse situasjoner (s. 249). Det vil si at det ledende sikkerhetsparadigmet i finansbransjen er en variant av fremgangsmåten jeg beskrev for beredskapsarbeid i kapittel 3.1 og som var basert på blant annet Eriksen m.fl. (2021), Lunde (2019) og Njå m.fl. (2020). Den generelle beredskapen fremstår som svært hendelsesspesifikk og jeg fikk ingen indikasjoner på at det utarbeides generiske og tilpasningsdyktige responsplaner, slik DRMG tar til orde for (DARWIN, 2018, s. 47). I den ene virksomheten jobber de så langt det er mulig med uidentifiserte og ukjente problemer som om de er kjente inntil de får bedre oversikt over hvilket konkret problem de står overfor. Dette fungerer fint når man håndterer noe man kjenner til fra før, altså i Kleins gatelys, men kan gjøre vondt verre hvis hendelsen viser seg å være av ukjent natur eller på annen måte oppføre seg annerledes enn det man er vant med (Klein, 2009, s. 246). Samtidig er det ikke til å stikke under en stol at det også kan oppfattes som en antakelsesbasert vurdering av en ukjent og/eller tvetydig situasjon (Lipshitz og Strauss, 1997, s. 153), som taler til bedriftens fordel i et resiliensperspektiv. Uansett vil beredskapen lettere kunne tilpasses ved å benytte retningslinjene i DRMG når uidentifiserte problemer oppstår (DARWIN, 2018, s. 51) i og med man ikke har noen garantier for at det uidentifiserte og/eller ukjente problemet vil oppføre seg på samme måte som problemer man har erfaringer med. Sorte svaner (Taleb, 2010, s. xxii; Aven og Thekdi, 2022, s. 51), perfekte stormer (Aven, 2022a, s. 53), slemme problemer (Martin, 2019, s. 42; Klein, 2009, s. 212) og andre skyggebelagte problemer kan oppstå. Kombinert med en hendelsesspesifikk sikkerhetstilnærming kan det i verste fall forverre situasjonen, især hvis hendelsen er av en slik karakter at den nåværende beredskapskapasiteten ikke strekker til (Klein, 2009, s. 237). Både på dette feltet og i det generelle beredskapsarbeidet i finanssektoren vil det være mye å hente på å anvende konsepter innen resiliens generelt og DRMG spesielt. Den ene informanten mente at det i særdeles spesielle og utfordrende situasjoner var lite sannsynlig at den finansielle infrastrukturen var sterk nok til å stå imot. Professor Gjøsteen har den samme bekymringen hvis finansindustrien står overfor et målrettet angrep (Solli, 2022). Resiliens er ikke et magisk formular som vil gjøre finanssektoren usårbar, men den vil bidra til å øke dens evne til å håndtere mer komplekse, uoversiktlige og tvetydige hendelser.

Deler av beredskapen som er direkte knyttet opp mot betalingsterminaler må derimot sies å være helt i tråd med resiliens-tankegangen. Både STIP og reserveløsningen er beredskapsløsninger hvor den bakenforliggende årsaken til feilen ikke har noen betydning.

Uansett hvor i verdikjeden det er et problem vil en av disse løsningene slå inn og rydde opp slik at transaksjonen kan gå som normalt. Systemet venter ikke på noen form for beskrivelse av problemet. Det går til aksjon med en gang det er et brudd i verdikjeden helt i tråd med resiliens-tankegangen (Klein, 2009, s. 151). Jeg er fristet til å omtale løsningene som forbilledlige eksempler på resiliens. Hver enkelt betalingsterminal som er utstyrt med dem er i prinsippet sikret mot både ventede og uventede hendelser. Det er noen forskjeller mellom DRMG-retningslinjens anbefalinger og måten disse tiltakene fungerer på, men tankegangen er lik. STIP og reserveløsningen er utrolig tilpasningsdyktige, akkurat slik DRMG ønsker å bygge opp under (DARWIN, 2018, s. 47-48 & 51), om enn ved at de fungerer på samme måte hver gang uavhengig av hva problemet er. Selve løsningene er statiske, men er utformet slik at de tilpasser seg til enhver utfordring og løser dem. Likhetene mellom STIP og reserveløsningen på den ene siden og ideen om hvordan responsfasen skal arte seg innen resiliens på den andre (se f.eks. Hollnagel, 2018, s. 29-31) er store. For eksempel vet systemene ikke bare når og hvordan de skal starte (Ibid., s. 29), men de vet også akkurat når de skal avslutte (Ibid., s. 31).

Norske betalingsterminaler er ikke pålagt å være tilkoblet en reserveløsning og som 16. mai-hendelsen viste kan terminalfeil medføre bortfall av den. En manglende oppdatering av reserveløsningens kapasitet førte dessuten til «Påskehendelsen» i 2011. Med andre ord er ikke reserveløsningen feilfri og som NOU 2015: 13 var inne på vil bortfall av BankAxepts reserveløsning medføre de største konsekvensene (s. 175-176). Derfor er det positivt at ulike terminaltyper har forskjellig tilkobling til reserveløsningen. Hvis en av dem har driftsproblemer finnes det fortsatt andre terminaler som ikke har det. Dermed blir salg av nødvendighetsvarer et organisatorisk problem for de(n) kjeden(e) som er rammet, men det vil ikke bli et samfunnssikkerhetsproblem siden nødvendighetsvarer fortsatt kan kjøpes hos kjeder som bruker en annen terminalleverandør. Dermed blir risikoen for et komplett sammenbrudd redusert. 16. mai-hendelsen viste hvordan dette fungerte i praksis og er et godt eksempel på denne risikospredningen. Riktignok opplevde flere dagligvarekjeder økte kødannelser i kassene ettersom det er tidkrevende å skrive og fylle ut debiteringsnotaene, men denne typen køer er ingen trussel mot samfunnssikkerheten. Dessuten fases en forbedret reserveløsning inn fra og med 1. juni 2023 som skal forhindre lignende kødannelser i fremtiden.

Reserveløsningen skal fungere i opptil syv døgn for nødvendighetsvarer. I realiteten kan den holde ut i mer enn en uke. Den kan være i funksjon så lenge terminalen har kapasitet til å lagre transaksjoner uten å behandle dem, men da er det brukerstedet som står for den økonomiske risikoen. I en langvarig krisesituasjon hvor det fortsatt er mulig å betale ved hjelp av reserveløsningen er det nærliggende å tro at det ville blitt tilrettelagt for at reserveløsningen

kan være i bruk over de syv tilmålte døgnene, for eksempel ved å lempe på den økonomiske risikoen butikkene tar. Hvis brukerstedene i tillegg har betalingsterminaler i reserve kan de ta i bruk terminaler som fortsatt har lagringskapasitet for å forlenge tidsrommet de evner å motta kortbetalinger på. Teoretisk vil det også være mulig å få tilgang på nye terminaler fra leverandørers lagre, men i en langvarig krise kan det være lite gjennomførbart. Hvis krisen er så langvarig at betalingsterminalene er avhengige av reserveløsningen i over en uke har samfunnet antakelig større og mer akutte problemer enn å få betalingsinfrastrukturen på fote igjen. Rent teoretisk er det like fullt ingenting i veien for at reserveløsningen kan brukes også utover den avtalefestede uka og følgelig øke samfunnets resiliens overfor bortfall av betalingsterminaler. Dette passer overens med tanken om at hendelseshåndteringen krever enten forberedte tiltak med tilstrekkelige ressurser eller ha stor nok fleksibilitet til at man kan anskaffe tilstrekkelig med ressurser ved behov (Hollnagel m.fl., 2011, s. 284). STIP og reserveløsningen er forberedte tiltak med tilstrekkelige ressurser til å vare i minst en uke og det er mulig å få tilgang til flere ressurser i form av betalingsterminaler med lagringsplass ved behov hvis kjedene har noen terminaler i reserve.

Det er vanskelig å se at det finnes konkrete måter å forbedre STIP og reserveløsningen på ved hjelp av DRMG ettersom begge tiltakene samsvarer med tankegangen som ligger til grunn for resiliens. Derimot er det nærliggende å tro at det finnes et forbedringspotensial for systemene som drifter dem. Tidligere hendelser og øvelser har vist at feil kan oppstå. Når vi samtidig ved at mesteparten av beredskapsarbeidet i finanssektoren er basert på risikoanalyser med tilhørende spesifiserte tiltak betyr det at beredskapen for STIP og reserveløsningen sannsynligvis også har det som grunnlag. Det åpner for spørsmålet om hvor godt skodd tiltakene i realiteten er. Vil de for eksempel være i stand til å håndtere en perfekt storm? Jeg har ikke undersøkt verken STIP eller reserveløsningen som sådan i denne oppgaven, men det kan være et interessant tema for videre studier.

Rutiner for krisehåndteringen i finanssektoren finnes utover STIP og reserveløsning. Særlig den ene virksomheten jeg var i kontakt med virker å operere i henhold til ideene som bygger opp under resiliens. De har lignende roller uavhengig av om de er i en normal- eller krisesituasjon og vil derfor ha bedre forutsetninger for å kjenne til de rette prosedyrene og retningslinjene når nødsituasjoner oppstår. I tillegg vil de ansatte sannsynligvis være mer komfortable og ha høyere selvtillit i oppgaveutførelsen. Dette er i full overensstemmelse med kapabilitetskortet om at krisehåndteringen bør være basert på de daglige rutinene (DARWIN, 2018, s. 47) og ser ut til å være normen i bransjen. Inntrykket mitt er at alle har tydelige rutiner for krisehåndteringen og klare rollefordelinger som er avklart på forhånd. En av de andre

virksomhetene setter for eksempel en stor krisestab innledningsvis for deretter å nedjustere etter hvert som de får bedre oversikt og kontroll. Også det er helt i tråd med DRMGs anbefaling om at man bør diagnostisere situasjonen tidlig i den akutte krisefasen før man justerer planen (Ibid., s. 49). Dette kan også gjøre bedriften bedre egnet til å håndtere komplekse og tvetydige situasjoner, som slemme problemer, fordi de gradvis kan tilpasse seg situasjonene de står overfor (Klein, 2009, s. 246) og fremgangsmåten kan også forstås å leve opp til Kleins ideal om ikke å avvente informasjon før man foretar seg noe (Ibid., s. 151).

I forbindelse med øvelser organisasjonene gjennomfører på egenhånd som grunnlag for å teste og eventuelt utbedre beredskapen er det grunn til å sette spørsmålstegn ved hvor representative funnene mine er. Dataene tilsier at bare en av de deltakende virksomhetene i realiteten utfører øvelser for seg selv. Riktignok stilles det tydelige testkrav som betalingsterminalene må bestå før de kan ta i bruk reserveløsning, men selve øvelsene knyttet til terminalene er forbeholdt leverandører og brukere, ikke kravstillerne. Alt i alt er det empiriske materialet for tynt til å trekke noen brede slutninger om effekten av øvelser som utføres på egenhånd for finanssektoren som helhet, men jeg har grunnlag for å uttale meg om den ene virksomhetens praksis. Øvelsene som den ene bedriften utfører er ment å forbedre ytelsen deres, blant annet ved å finne et optimalt ytelsesnivå som ikke er for lavt slik at betalingsterminalene lider eller for høyt slik at de bruker mer ressurser enn nødvendig. Det passer godt overens med definisjonen for resiliens som ligger til grunn i denne oppgaven. Ifølge den er resiliens «et uttrykk for hvordan folk, alene eller sammen, håndterer hverdagssituasjoner – store og små – ved å tilpasse ytelsen deres etter forholdene» (Hollnagel, 2018, s. 14-15). Dessuten er det også godt samsvar med ideen om ikke å kaste bort verdifulle ressurser (Ibid., s. 31). Virksomheten søker også å være proaktiv og i forkant ved å skalere driften i henhold til svingninger i bruken av betalingskort, som i forbindelse med Black Friday. Proaktiv resiliens går nettopp ut på det å være i forkant av hendelsene for på den måten å unngå uønskede hendelser eller for å dempe effektene av dem (Stavland og Bruvoll, 2019, s. 12). På den andre siden kan det også forstås som et uttrykk for at de forholder seg til kjente mønstre og er lite tilpasset plutselige og uventede endringer (DARWIN, 2018, s. 46-47), men etter mange tiår med kortbruk i et relativt stabilt og forutsigbart miljø er dette etter all sannsynlighet noe som bransjen har svært god oversikt over og derfor hører hjemme i Kleins gatelys (Klein, 2009, s. 230). Den samme bedriften vedlikeholder og øker kontinuerlig bevisstheten hos alle sine ansatte rundt ulike former for ondartede meldinger ved å sende slike ut til dem fra tid til annen, altså en slags lavskalaøvelse. Dette er en form for læringsprosess de lar alle ansatte gjennomgå hvor hensikten er å forbedre samtlige ansattes ferdigheter med å avsløre fiendtlige forsøk på å trenge

gjennom sikkerhetsbarrierene deres og derved forsterke organisasjonens evne til å håndtere fremtidige utfordringer (Steen m.fl., 2023, s. 3). Dessuten indikerer det at virksomheten prioriterer å bruke tid og ressurser på læring. Noen må analysere reelle angrepsforsøk og utarbeide meldinger som ligner såpass at de går for å være ekte, for deretter å distribuere dem til de ansatte. Det er en konstant pågående prosess og er derfor ressurskrevende, hvilket er i pakt med læring som en av resiliensens hjørnesteiner (Hollnagel, 2018, s. 39-40). Hvorvidt dette tas med i betraktningen når de senere utvikler beredskapen sin kan være et utgangspunkt for fremtidige studier da det faller utenfor denne oppgavens rammer.

Det er liten tvil om at det generelle beredskapsarbeidet i den norske finansielle infrastrukturen tar utgangspunkt i det som kalles beskyttende sikkerhet (Ibid., s. 15). Etter mitt skjønn har finansbransjen like fullt et strålende utgangspunkt å bygge videre på. Det foregår en omfattende kartlegging og det er åpenbart at de har veldig god oversikt, forståelse og kontroll over hendelser de til en viss grad er kjente med. Altså de hendelsene som Klein mener befinner seg i skinnet fra gatelys (Klein, 2009, s. 230). Samtidig later det til å være stor grad av samsvar mellom daglig drift og håndtering av nødsituasjoner, som fremgår som et sentralt aspekt i DRMG (DARWIN, 2018, s. 47). Implisitt antyder empirien dessuten at aktørene enten gjenkjenner flere av de felles komponentene ved de forskjellige truslene eller i det minste har grunnlag for å gjøre det, for eksempel ved at flere av dem utveksler risikoanalyser med hverandre og således har et godt datagrunnlag for dimensjonering av beredskap. Hvis de bruker det som utgangspunkt for å utvikle generiske responsplaner som kan tilpasses forskjellige situasjoner i henhold til det retningslinjene (Ibid.) og andre konsepter innen resiliens anbefaler (se f.eks. Klein, 2009, s. 247; Hollnagel m.fl., 2011, s. 6-8; og Renn, 2008, s. 179) vil beredskapsevnen for betalingsterminaler forsterkes. Det samme vil den for så vidt gjøre generelt i hele den finansielle infrastrukturen. Den vil bli mer kapabel og bedre rustet til å håndtere trusler som ifølge Klein er gjemt i skyggene (Klein, 2009, s. 10) og som følgelig er mindre kjente. Konkret for betalingsterminaler må STIP og reserveløsning igjen fremheves som beredskapsløsninger det oser resiliens av.

Alt i alt har finansindustrien alle forutsetninger for å bygge videre på den eksisterende beredskapen og forbedre den ved hjelp av resiliens og DRMG. Hvis det stemmer at bransjen er i ferd med å gjennomgå et paradigmeskifte hvor man i større grad gjennomfører sikkerhetstiltak som går utover de reguleringskravene sektoren er underlagt, er dette et strålende tidspunkt å fase resiliens inn i sikkerhetsarbeidet.

6.4 Oppsummering

I dette kapittelet har jeg drøftet forskningsspørsmålene med utgangspunkt i teori og empiri. Jeg oppfatter det slik at finanssektoren generelt har god beredskap for betalingsterminaler, men at næringen i hovedsak baserer seg på beskyttende sikkerhet. Bransjen har alle forutsetninger for å forbedre beredskapsevnen ved å anvende konsepter og metoder innen resiliens. Dette er temaet i neste og siste kapittel.

7 Konklusjon

Før jeg starter på konklusjonen er det verdt å minne om problemstillingen en siste gang:

«Hvordan kan anvendelse av konsepter og metoder innen resiliens forbedre finanssektorens beredskapsevne for betalingsterminaler?»

Det er dette jeg har forsøkt å besvare gjennom denne oppgaven. I forrige kapittel trakk jeg konklusjoner for hvert enkelt forskningsspørsmål. De kan oppsummeres ved at det er mange positive aspekter ved beredskapsevnen i den finansielle infrastrukturen, men at sikkerhetstankegangen i hovedsak bærer preg av å være innrettet etter prinsippene i beskyttende sikkerhet. Resiliens er ment å komplementere dette og dermed heve både det totale sikkerhets- og ytelsesnivået. Derfor er svaret ja på hvorvidt resiliens kan forbedre beredskapsevnen i finanssektoren og for betalingsterminaler. Det bereder grunnen for et konkret svar på problemstillingen.

Som nevnt i kapittel 6.1 og 6.2 legges det til rette for tverrorganisatorisk samarbeid til en viss grad. Det finnes flere fora hvor det gjøres mye bra arbeid med tanke på å spre relevant informasjon til de øvrige aktørene i sektoren og dette bidrar utvilsomt til at partene får bedre oversikt over det som skjer. Driftsforumet for betalingskort er et godt eksempel på et nettverk som sørger for å redusere risikoen for at feil skal oppstå i verdikjeden knyttet til betalingsterminaler grunnet manglende oversikt over hva de andre aktørene foretar seg. Det jeg derimot savner er et organ som kan tilrettelegge og koordinere det tverrorganisatoriske samarbeidet under en krisehåndtering. Riktignok står BFI for varsling og informering ved hendelser og det er vel og bra, men det gjøres lite eller ingenting konkret for å bygge opp samarbeidsevnen i forkant av kriser. Empirien indikerer dessuen at det ikke er alle tilknyttet

finanssektoren som har like god forståelse for diverse faguttrykk og terminologier. Det kan medføre ekstra problemer når en krise inntreffer. Et slikt organ kan sørge for å gjennomføre tiltak som vil forbedre det tverrorganisatoriske samarbeidet under en krise. Det trenger ikke nødvendigvis å være eksklusivt for betalingsterminaler. Hvor bredt det bør favne kan en utredning i regi av for eksempel BFI slå fast. De har gjennomført andre utredninger på vegne av den finansielle infrastrukturen tidligere. En innføring av resiliens i form av retningslinjene som anbefales av DRMG for temaet som omhandler å støtte koordinering og synkronisering av fordelte oppgaver vil forbedre beredskapsevnen. Risikoen for misforståelser og unødvendig tidsbruk på avklaringer som allerede kunne vært unnagjort i førkrisefasen vil følgelig synke.

Den største hemskoen rundt beredskapen for betalingsterminaler er at all beredskapsplanlegging er hendelsesspesifikk. Det betyr at finanssektoren står dårligere rustet til å håndtere skyggebelagte trusler. Når jeg likevel sitter med inntrykket av at beredskapen er god er det i stor grad på grunn av STIP og reserveløsning. Selve betalingsterminalene og systemene som støtter opp om dem er meget godt utstyrt for å håndtere alle slags problemer i verdikjeden. Det skal mye til for at funksjonen deres skal falle bort, men historien har vist at de ikke er ufeilbarlige. Sjansen for at en svært alvorlig hendelse skal oppstå er kanskje liten, men konsekvensene av et langvarig bortfall av betalingsterminaler kan sette samfunnssikkerheten i fare. Beredskapsevnen for betalingsterminaler kan forbedres ved hjelp av resiliens og DRMG. Riktignok kan det ikke være et absolutt bolverk, men responsplaner som er mer fleksible og tilpasningsdyktige, slik DRMG anbefaler, vil gjøre finansbransjen bedre skodd til å håndtere også skyggebelagte trusler. Risikoen for at beredskapen kommer til kort i møte med slike trusler vil ikke forsvinne, men kan reduseres ved at beredskapsressursene ikke er innrettet etter konkrete hendelser og heller har større rom for individuell tilpasning i møte med ukjente kriser.

Totalt sett kan beredskapsevnen den finansielle infrastrukturen har for betalingsterminaler sammenfattes med en referanse til bladet *Historie*. Jeg har vært abonnent siden dets oppstart i 2005 og i en årrekke var en av bedømmingene «rom for forbedringer» hvis man fikk en middelmådig poengsum i bladets quizer. Jeg oppfatter beredskapsevnen for betalingsterminaler som bedre enn middelmådig, men det er like fullt rom for forbedringer. Bruk av resiliens og DRMG er en måte denne forbedringen kan gjennomføres. Ikke bare vil det forsterke beredskapen for betalingsterminaler, men det vil også medføre en bedret beredskapsevne andre steder i den finansielle infrastrukturen.

7.1 Videre forskning og studier

Gjennom arbeidet med denne oppgaven kom jeg over en rekke områder som kunne vært gjenstand for nærmere studier. Som nevnt valgte jeg de kapabilitetskortene jeg gjorde fordi jeg ønsket å maksimere mine egne sjanser for å få samlet inn tilstrekkelig med data for å få gjennomført studien. Faktum er at det er mulig å oppdrive mye data i finanssektoren. Alle informantene jeg snakket med var svært behjelpelige og jeg er helt sikker på at jeg kunne fått tilgang til langt mer data enn jeg trodde var mulig da prosjektet startet. Det følgende er noen eksempler på muligheter for videre studier.

Hvis man vil fortsette å grave i betalingsterminalene er reserveløsningen et veldig aktuelt studietema. Hva som kreves for at den skal fungere og hvordan man kan forbedre systemet som holder den i drift er noe jeg gjerne skulle visst mens jeg skrev denne oppgaven. På mange måter står og faller betalingsterminalene på reserveløsningen.

Det er også mulig å se nærmere på hvordan samhandlingen mellom finans- og telekommunikasjonssektoren fungerer i praksis. Kan anvendelse av metoder og konsepter innen resiliens bidra til å forbedre det tverrorganisatoriske samarbeidet dem imellom? På samme måte kan det være aktuelt å se på samspillet mellom finans- og kraftsektoren.

Jeg fant indikasjoner på at finansnæringen søker å oppdage skjørhet i beredskapen sin. Hvorvidt det faktisk stemmer og hvordan man eventuelt kan forbedre den evnen er et annet eksempel på noe som kan være aktuelt for nærmere undersøkelser.

Et spor jeg nesten forfulgte innledningsvis i datainnsamlingen var å finne ut av hvordan brukerstedene opplever bruken av betalingsterminaler fra et beredskapsperspektiv. I hvilken grad er de kjente med deres rolle i beredskapsarbeidet? Det er til syvende og sist hos brukerstedene at betalingsterminalen brukes og der de lokale beredskapstiltakene må være på plass. Eksempler på innfallsvinkler er hvordan butikkjedene tilrettelegger for dette internt eller hvordan samhandlingen mellom terminalleverandøren er med de ulike brukerstedene som tilbyr nødvendighetsvarer.

Jeg fant få indikasjoner på at resiliens bevisst ble brukt i beredskapsarbeidet på de feltene jeg undersøkte. Derfor kan en mulighet være å se på flere måter resiliens kan forbedre beredskapsevnen i den finansielle infrastrukturen ved hjelp av resiliens og kapabilitetskortene i DRMG.

Dette var noen eksempler på mulige emner for videre forskning og studier. Inntrykket mitt er at finanssektoren generelt er lite studert ut fra et samfunnssikkerhetsperspektiv. Dermed

er det et utall muligheter for forskning på feltet. Beredskapen i sektoren er god, men det er fortsatt rom for forbedringer.

8 Referanseliste

Aarønæs, L. (2019, 28. september). *Stormer fra sola kan slå oss ut*. Forskning.no. https://forskning.no/energi-forsvarets-forskningsinstitutt-partner/stormer-fra-sola-kan-sla-oss-ut/1570064.

Adressa. (2022, 16. mai). *Betalingstrøbbel i hele landet: – Jeg forsøkte flere terminaler*. Adresseavisen. https://www.adressa.no/okonomi/i/dnAgkX/betalingstrobbel-i-hele-landet-jeg-forsokte-flere-terminaler.

Aftenbladet. (2022, 16. mai). *– Hæ, er kortterminalene nede?* Stavanger Aftenblad. https://www.aftenbladet.no/lokalt/i/7dk3ew/hae-er-kortterminalene-nede.

Andersen, P.B. & Liseter, I.M. (2022, 7. januar). *Elektromagnetisk puls*. Store Norske Leksikon. https://snl.no/elektromagnetisk_puls (Besøkt 9. mars 2023).

Andersen, S.S. (2006). Aktiv informantintervjuing. *Norsk statsvitenskapelig tidsskrift* (2006:03), s. 278-298.

Aven, T. (2022a). *Risiko og risikovitenskap*. Universitetsforlaget.

Aven, T. (2022b, 10. august). Robusthet. I *Store Norske Leksikon*. https://snl.no/robusthet (Besøkt 26. januar 2023).

Aven, T. (2023, 26. januar). Sårbarhet. I *Store Norske Leksikon*. https://snl.no/s%C3%A5rbarhet (Besøkt 26. januar 2023).

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

Bach, D. (2021, 17. august). *Mastercard faser ut magnetstripen*. E24. https://e24.no/internasjonal-oekonomi/i/G3P2KQ/mastercard-faser-ut-magnetstripen.

BankAxept. (2023a). *Kom i gang med BankAxept*. BankAxept. https://bankaxept.no/tjenester/kom-i-gang (Besøkt 29. mars 2023).

BankAxept. (2023b). *Prosedyre for reserveløsning*. BankAxept. https://bankaxept.no/prosedyre-for-reserveloesning (Besøkt 23. mai 2023).

BankAxept. (2023c). *Reserveløsning – alltid på*. BankAxept. https://bankaxept.no/tjenester/reserveloesning (Besøkt 29. mars 2023).

BBC. (2018, 27. mars). *When is a diplomat really just a spy?* BBC. https://www.bbc.com/news/newsbeat-43556816.

Betalingssystemloven. (1999). *Lov om betalingssystemer m.v.* (LOV-1999-12-17-95). Lovdata. https://lovdata.no/dokument/NL/lov/1999-12-17-95.

BFI. (2007, 20. mars). *Årsrapport 2006*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2006.pdf.

BFI. (2008, 18. mars). *Årsrapport 2007*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2007.pdf.

BFI. (2010, 4. mars). *Årsrapport 2009*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2009.pdf.

BFI. (2012, 31. januar). *Årsrapport 2011*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2011.pdf.

BFI. (2014, 31. mars). *Årsrapport 2012*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2013.pdf.

BFI. (2015, 15. februar). *Årsrapport 2013*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2014.pdf.

BFI. (2016, 5. april). *Årsrapport 2015*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2015.pdf.

BFI. (2018, 8. mars). *Årsrapport 2017*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2017.pdf.

BFI. (2020, 1. mars). *Årsrapport 2019*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2019.pdf.

BFI. (2021, 1. mars). *Årsrapport 2020*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2020.pdf.

BFI. (2022, 1. mars). *Årsrapport 2021*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/arsrapport-bfi-2021.pdf.

BFI. (2023, 9. mars). *Årsrapport 2022*. Beredskapsutvalget for finansiell infrastruktur. https://www.finanstilsynet.no/contentassets/fd161162f9214140a4c7f84d001407b8/beredskapsutvalget-for-finansiell-infrastruktur-bfi--arsrapport-2022.pdf.

Bjørnstad, G.H., Andersen, J.E., Eriksen, N., Gimse, L.M., Grinde, M., Drake, S. & Andersen, Ø. (2022, 16. mai). *Kortterminaler nede i hele Norge*. Børsen. https://borsen.dagbladet.no/nyheter/kortterminaler-nede-i-hele-norge/76113665.

Blaikie, N. & Priest, J. (2019). *Designing Social Research* (3. utg.). Polity Press.

Bodø kommune. (2018). *ROS Bodø 2018: Helhetlig risiko- og sårbarhetsanalyse*. Bodø kommune. https://bodo.kommune.no/getfile.php/134395-1551103145/Om%20Bodø%20kommune/Sikkerhet%20og%20beredskap/Beredskapsforum%20Salten/ROS%20Bodø%202018%20Helhetlig%20risiko-%20og%20sårbarhetsanalyse.pdf.

Branlat, M. (Red.). (2018). *DARWIN Resilience Management Guidelines*. DARWIN. https://h2020darwin.eu/wp-content/uploads/2018/11/DARWIN-D2.4-DARWIN-Resilience-Management-Guidelines.pdf.
Brekke, P. (2013). *Den stormfulle sola*. Solarmax.
British Museum. (u.å.). *Banknote*. The British Museum. https://www.britishmuseum.org/collection/object/C_CIB-EA-260.
BT. (2022, 16. mai). *Kortproblemer over hele landet*. Bergens Tidende. https://www.bt.no/nyheter/lokalt/i/L5bMEV/kortproblemer-over-hele-landet.
Bøe, E., Gussiås, D.N. & Aaser, K. (2023, 7. juni). *Danske Bank forlater det norske privatmarkedet*. E24. https://e24.no/boers-og-finans/i/9z0KBW/danske-bank-forlater-det-norske-privatmarkedet.
Carter, J. (2023, 15. mars). *Northern Lights in New York Possible in Wake Of Historic 'Halo' On The Sun*. Forbes. https://www.forbes.com/sites/jamiecartereurope/2023/03/15/northern-lights-in-new-york-possible-in-wake-of-historic-halo-on-the-sun/.
Cedrini, V., Mancini, M., Rosi, L., Mandarino, G., Giorgi, S., Herrera, I., Branlat, M., Pettersson, J., Jonson, C-O., Save, L. & Ruscio, D. (2018). Improving resilience management for critical infrastructures–strategies and practices across air traffic management and healthcare. I S. Haugen, A, Barros, C. Gulijk, T. Kongsvik & J.E. Vinnem (Red.), *Safety and Reliability – Safe Societies in a Changing World* (s. 1319-1327). CRC Press. https://doi.org/10.1201/9781351174664.
Charlie Rose. (2009, 22. oktober). *Lee Kuan Yew* [Video]. Charlie Rose. https://charlierose.com/episodes/15567?autoplay=true.
CNG. (2005). *Sale: Triton VIII, Lot: 461*. Classical Numismatic Group. https://www.cngcoins.com/Coin.aspx?CoinID=57383#.
Computerworld. (2016, 3. august). *Slik hacker de betalingsterminalen*. Computerworld. https://www.cw.no/innovasjon-kuriosa-programmering/slik-hacker-de-betalingsterminalen/689688.
Conrad, J. (2022, 8. november). *China's Digital Yuan Works Just Like Cash – With Added Surveillance*. Wired. https://www.wired.com/story/chinas-digital-yuan-ecny-works-just-like-cash-surveillance/.
Dahlum, S. (2021, 9. mars). Validitet. I *Store Norske Leksikon*. https://snl.no/validitet (Besøkt 18. april 2023).
Danske Bank. (2023). *GOLD kundeprogram*. Danske Bank. https://danskebank.no/privat/dagligbank/kort-og-konto/gold (Besøkt 26. april 2023).
DARWIN. (2018). *DARWIN RESILIENCE MANAGEMENT GUIDELINES (DRMG Book)*. DARWIN. https://h2020darwin.eu/wp-content/uploads/2018/08/DRMG_Book.pdf.
De Rosa, M. (2023, 18. april). Kontantkutt kan spare bedrifter for 10 milliarder i året. *NTB/E24*. https://e24.no/naeringsliv/i/l3eBgA/kontantkutt-kan-spare-bedrifter-for-10-milliarder-i-aaret.
Dinero. (2023). *Test av Bank Norwegian Visa kredittkort*. Dinero. https://dinero.no/kredittkort/bank-norwegian/ (Besøkt 10. mai 2023).
DSB. (2016). *Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Direktoratet for samfunnssikkerhet og beredskap. https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf.
Engen, O.A.H., Gould, K.A.P., Kruke, B.I., Lindøe, P.H., Olsen, K.H. & Olsen, O.E. (2021). *Perspektiver på samfunnssikkerhet* (2. utg.). Cappelen Damm Akademisk.
Eriksen, J., Rake, E.L. & Sommer, M. (2021). *Beredskapsanalyse*. Cappelen Damm Akademisk.
European Central Bank. (2021). *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements* (November 2021). Den europeiske sentralbank. https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf.
Excelsecu (2023). *IoT Payment*. Excelsecu. https://www.excelsecu.com/productdetail/iotpayment02.html (Besøkt 29. mars 2023).
Fallmyr, S.S., Moland, A., Johansen, J.I., Thonhaugen, M. & Oskarsen, L.S. (2022, 16. mai). *Problemet er løst – nå kan du betale med kort igjen*. NRK. https://www.nrk.no/nordland/betalingsproblemer-pa-flere-butikker-rett-for-17.-mai-1.15968957.
Fang, L., Snellman, K., Zeisberger, C. & Munro, D.G. (2023, 21. mars). *Risks and Regulations: The Silicon Valley Bank Collapse*. INSEAD. https://knowledge.insead.edu/economics-finance/risks-and-regulations-silicon-valley-bank-collapse.
Finansavtaleloven. (2020). *Lov om finansavtaler* (LOV-2020-12-18-146). Lovdata. https://lovdata.no/dokument/NL/lov/2020-12-18-146/.
Finansforetaksloven. (2015). *Lov om finansforetak og finanskonsern* (LOV-2015-04-10-17). Lovdata. https://lovdata.no/dokument/NL/lov/2015-04-10-17/.
Finanstilsynet. (2010, 1. juni). *Beredskapsutvalget for finansiell infrastruktur (BFI). Mandat fastsatt av Norges Banks hovedstyre 11. oktober 2000 (oppdatert navneendring ved at Finanstilsynet overtok ledelse og sekretariat 01. juni 2010).* Finanstilsynet. https://www.finanstilsynet.no/contentassets/3f536be3fdab4f76a924ce55319a2afa/mandat-bfi.pdf.
Finanstilsynet. (2012, 28. mars). *Risiko- og sårbarhetsanalyse (ROS) 2011: Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)*. Finanstilsynet. https://www.finanstilsynet.no/contentassets/98f605c0caec4b048009cf6568ea10df/ros-analyse_2011.pdf.

Finanstilsynet. (2016, 27. mai). Betalingstjenester og betalingssystemer. I *Finanstilsynet*. https://www.finanstilsynet.no/forbrukerinformasjon/betalingstjenester-og-betalingssystemer/.
Finanstilsynet. (2017, 15. februar). *Beredskapsutvalget for finansiell infrastruktur (BFI)*. Finanstilsynet. https://www.finanstilsynet.no/tema/beredskapsutvalget-for-finansiell-infrastruktur-bfi/.
Finanstilsynet. (2023, 3. mai). *Risiko- og sårbarhetsanalyse (ROS) 2023: Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT)*. Finanstilsynet. https://www.finanstilsynet.no/contentassets/fbbc7ef2a0c9499fbb6fa68867ad697c/risiko-og-sarbarhetsanalyse-2023.pdf.
Finanstilsynet. (u.å.). *Risiko- og sårbarheitsanalyse for IKT-sikkerheit i finanssektoren*. Finanstilsynet. https://www.finanstilsynet.no/publikasjoner-og-analyser/risiko--og-sarbarhetsanalyse/ (Besøkt 28. februar 2023).
Fleming, J. (2022, 11. oktober). *RUSI Annual Security Lecture 2022*. GCHQ. https://www.gchq.gov.uk/speech/rusi-asl.
Forskrift om systemer for betalingstjenester. (2019). *Forskrift om systemer for betalingstjenester* (FOR-2019-02-15-152). Lovdata. https://lovdata.no/dokument/SF/forskrift/2019-02-15-152.
Foss, A.B., Eggesvik, O., Myhre, S.M., Sørenes, K.M. & Olsen, O. (2022, 16. mai). *Store problemer med kortterminalene landet rundt. Kunder fikk ikke betalt.* Aftenposten. https://www.aftenposten.no/norge/i/9KJ31l/store-problemer-med-kortterminalene-landet-rundt-kunder-fikk-ikke-betalt.
Freepik. (2023). *Bank building with cityscape*. Freepik.com. https://www.freepik.com/free-vector/bank-building-with-cityscape_13187569.htm#query=bank%20illustration&position=21&from_view=search&track=robertav1_2_sidr (Besøkt 26. april 2023).
Gram, T. (2020, 3. mars). *Vipps*. Store Norske Leksikon. https://snl.no/Vipps (Besøkt 9. mars 2023).
Gramnæs, M. (2023, 20. februar). *Raser mot Coop*. Dagbladet. https://dinside.dagbladet.no/okonomi/raser-mot-coop/78541926.
Grimstad, T., Thommessen, J.K., Strand, T., Nyborg, Ø. & Skei, L. (2023, 13. april). *Ansatte ved Russlands ambassade sendes ut fra Norge: - En trussel mot Norge*. NRK. https://www.nrk.no/norge/ansatte-ved-russlands-ambassade-utvises-fra-norge_-_-en-trussel-mot-norge-1.16372116.
Grønmo, S. (2023, 16. januar). *Kvalitativ metode*. Store Norske Leksikon. https://snl.no/kvalitativ_metode (Besøkt 13. april 2023).
Gullbekk, S.H. (1995). *En mynthistorisk tidsreise: Norges første mynt*. Universitetets myntkabinett. https://www.dokpro.uio.no/umk/tidsreise/995.html.
Hansen, S. (2020, 18. oktober). *Oslos røde spritsommer*. NRK. https://www.nrk.no/dokumentar/xl/oslos-rode-spritsommer-1.15172839.
Hatfield, M. (2023, 14. mars). *A Powerful Solar Eruption on Far Side of Sun Still Impacted Earth*. NASA. https://blogs.nasa.gov/sunspot/2023/03/14/a-powerful-solar-eruption-on-far-side-of-sun-still-impacted-earth/.
Hautemanière, M. (2016, 3. februar). *Betalingsterminalens historie*. Mobile Transaction. https://no.mobiletransaction.org/betalingsterminalens-historie/.
Hautemanière, M. (2019, 10. april). *Betalingsterminaler – en oversikt over typer, leverandører og priser*. Mobile Transaction. https://no.mobiletransaction.org/betalingsterminal-priser-aktorer/.
Hermelin, J., Bengtsson, K., Woltjer, R., Trnka, J., Thorstensson, M., Pettersson, J., Prytz, E. & Jonson, C-O. (2020). Operationalising resilience for disaster medicine practitioners: capability development through training, simulation and reflection. *Cognition, Technology & Work 22*, s. 667-683. https://doi.org/10.1007/s10111-019-00587-y.
History.com Editors. (2009, 29. oktober). *Maginot Line*. History Channel. https://www.history.com/topics/world-war-ii/maginot-line (Oppdatert 4. oktober 2022).
Hollnagel, E., Pariès, J., Woods, D.D. & Wreathall, J. (2011). *Resilience Engineering in Practice: A Guidebook*. CRC Press.
Hollnagel, E. (2018). *Safety-II in Practice: Developing the Resilience Potentials*. Routledge.
Ja til kontanter. (2022, 8. august). *Pressemelding: 130.000 betalingsterminaler gikk i svart: – Frykter digitalt betalingssystem kan kollapse*. Ja til kontanter. https://ja-tilkontanter.no/2022/08/08/130-000-betalingsterminaler-gikk-i-svart-frykter-digitalt-betalingssystem-kan-kollapse/.
Jensen, A.E. (2022, 13. juli). *Solstorm kan mørklegge jorden*. Illustrert Vitenskap. https://illvit.no/universet/solsystemet/solen/solen-hva-er-en-solstorm.
Jensen, M.H. (2019, 22. november). *Professor: - Jo, du kan nekte å ta imot kontanter*. ABC Nyheter. https://www.abcnyheter.no/penger/forbruker/2019/11/22/195627597/professor-jo-du-kan-nekte-a-ta-imot-kontanter.
Johnsen, G. (2023, 9. mai). *«For dårlig sikkerhetsnivå.» Ber om storsatsing mot cybertrusler*. Aftenposten. https://www.aftenposten.no/norge/i/onlk3B/for-daarlig-sikkerhetsnivaa-ber-om-storsatsing-mot-cybertrusler.
Jutkvam, M.T., Skau, J.E. & Gundersen, R.H. (2022, 16. mai). *Betalingsterminaler i butikker var nede i hele landet – feilen er rettet*. Nordstrands Blad. https://www.noblad.no/betalingsterminaler-i-butikker-var-nede-i-hele-landet-feilen-er-rettet/s/5-56-556787.
Kahneman, D. (2012). *Tenke, fort og langsomt*. Pax forlag. Oversatt av E. Lilleskjæret og G. Nyquist.

Kjølås, H. (2021, 19. november). *Ålesundsbrannen*. Store Norske Leksikon. https://snl.no/%C3%85lesundsbrannen (Besøkt 12. juni 2023).
Klein, C. (2012, 14. mars). *A Perfect Solar Superstorm: The 1859 Carrington Event*. History. https://www.history.com/news/a-perfect-solar-superstorm-the-1859-carrington-event.
Klein, G. (2009). *Streetlights and Shadows: Searching for the Keys to Adaptive Decision Making*. MIT Press.
Kronheim, E.H. (2022, 20. september). *Lekket dansk trusselrapport: Spår en ny kald krig*. TV2. https://www.tv2.no/nyheter/utenriks/lekket-dansk-trusselrapport-spar-en-ny-kald-krig/15064269/.
Kvale, S. & Brinkmann, S. (2015). *Det kvalitative forskningsintervju* (3. utg.). Gyldendal Akademisk. Oversatt av T.M. Anderssen og J. Rygge.
Kvatningen, R., Nymoen, M., Hjertholm, A., Bu, F., Tønnesen M.S. & Vik, J.N. (2022, 16. mai). *Kortproblemer skapte kaos i butikker over hele landet*. TV2. https://www.tv2.no/nyheter/innenriks/kortproblemer-skapte-kaos-i-butikker-over-hele-landet/14796651/.
Lee, D. (2013, 19. april). *Boston bombing: How internet detectives got it very wrong*. BBC. https://www.bbc.com/news/technology-22214511.
Lipshitz, R. & Strauss, O. (1997). Coping with Uncertainty: A Naturalistic Decision-Making Analysis. *Organizational Behavior and Human Decision Processes*, 69(2), s. 149-163.
Lode, S.C. (2022, 1. juli). *Ekspert om dataangrepet: Ikke mulig å forhindre*. VG. https://www.vg.no/nyheter/innenriks/i/oW5bEg/ekspert-om-dataangrepet-ikke-mulig-aa-forhindre.
Lundberg, J. & Johansson, B.J. (2015). Systemic resilience model. *Reliability Engineering & System Safety*, *141*, s. 22-32. https://doi.org/10.1016/j.ress.2015.03.013.
Lunde, I.K. (2019). *Praktisk krise- og beredskapsledelse*. 2. utg. Universitetsforlaget.
Luntz, S. (2023, 14. mars). *Earth Just Dodged One Of The Fastest Coronal Mass Ejections Ever*. IFLScience. https://www.iflscience.com/the-earth-just-dodged-one-of-the-fastest-coronal-mass-ejections-ever-67962.
Malm, M. & Resvoll, A. (2022, 1. september). *Cutters-sjef: - Jeg går heller i fengsel enn å tilby kontanter*. E24. https://e24.no/norsk-oekonomi/i/WRlgqQ/cutters-sjef-jeg-gaar-heller-i-fengsel-enn-aa-tilby-kontanter.
Martin, P. (2019). *The Rules of Security: staying safe in a risky world*. Oxford University Press.
Meininch, P. (2020, 4. mars). *Sjekk*. Store Norske Leksikon. https://snl.no/sjekk (Besøkt 9. mars 2023).
Meld. St. 5 (2020-2021). *Samfunnssikkerhet i en usikker verden*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000ddpdfs.pdf.
Meld. St. 10 (2016-2017). *Risiko i et trygt samfunn*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000ddpdfs.pdf.
Meld. St. 10 (2019-2020). *Høytflyvende satellitter – jordnære formål: En strategi for norsk romvirksomhet*. Nærings- og fiskeridepartementet. https://www.regjeringen.no/contentassets/81ef9083ea904edb953e3c7109f187f7/no/pdfs/stm201920200010000ddpdfs.pdf.
Meld. St. 18 (2022-2023). *Finansmarkedsmeldingen 2023*. Finansdepartementet. https://www.regjeringen.no/contentassets/2f9e7828fa724306afb815f10885a53d/no/pdfs/stm202220230018000ddpdfs.pdf.
Merriam-Webster. (2023). *Cross-fertilization*. Merriam-Webster Dictionary. https://www.merriam-webster.com/dictionary/cross-fertilization (Besøkt 11. juni 2023).
Moon, E. (2017, 19. oktober). *Volcanoes May Have Helped Bringing Down Ancient Egypt*. Pacific Standard. https://psmag.com/environment/volcanoes-may-have-helped-bring-down-ancient-egypt.
Mortensen, K. & Dahl, A.N. (2022, 16. mai). *Kort-kaos i hele Follo da bankterminalene gikk ned for telling*. Østlandets Blad. https://www.oblad.no/kort-kaos-i-hele-follo-da-bankterminalene-gikk-ned-for-telling/s/5-68-1162917.
Moskaliuk, J., Bokhorst, F. & Cress, U. (2016). Learning from others' experiences: How patterns foster interpersonal transfer of knowledge-in-use. *Computers in Human Behavior 2016*, *55*, s. 69-75. https://doi.org/10.1016/j.chb.2015.08.051.
NAOB (2023). *Resiliens*. Det Norske Akademis Ordbok. https://naob.no/ordbok/resiliens (Besøkt 24. januar 2023).
Nave, O.B., Bergo, I., Rosef, T. & Kristiansen, T. (2022, 16. mai). *Kortterminal-problemer er løst*. VG. https://www.vg.no/nyheter/innenriks/i/1OAMbe/kortterminal-problemer-er-loest.
Norges Bank. (2019, 27. juni). *Krisehandtering*. Norges Bank. https://www.norges-bank.no/tema/finansiell-stabilitet/Krisehandtering/.
Norges Bank. (2020, 27. august). *Om retten til å betale i kontanter*. Norges Bank. https://www.norges-bank.no/tema/Sedler-og-mynter/retten-til-kontantbetaling/.
Norges Bank. (2022, 24. november). *Digitale sentralbankpenger*. Norges Bank. https://www.norges-bank.no/tema/finansiell-stabilitet/digitale-sentralbankpenger/.
Norges Bank. (2022b). *Finansiell infrastruktur 2022*. Norges Bank. https://www.norges-bank.no/contentassets/7437af41dbd94dbfaee9e7f0d231a3ba/finansiellinfrastruktur_2022.pdf.

NOU 1996: 16. *Tiltak mot flom*. Nærings- og energidepartementet. https://www.regjeringen.no/contentassets/21e6f5f6fe424757a8d418a33259c223/no/pdfa/nou199619960016000dddpdfa.pdf.
NOU 2000: 24. (2000). *Et sårbart samfunn: Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Justis- og politidepartementet. https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf.
Njå, O., Sommer, M., Rake, E.L. & Braut, G.S. (2020). *Samfunnssikkerhet: Analyse, styring og evaluering*. Universitetsforlaget.
Oakley, N. (2016, 1. august). *Why you should never hand over your card to the server when paying with contactless*. The Mirror. https://www.mirror.co.uk/money/you-should-never-hand-over-8537697.
NSM. (2015). *Helhetlig IKT-risikobilde 2015*. Nasjonal Sikkerhetsmyndighet. https://nsm.no/getfile.php/133681-1592831865/NSM/Filer/Dokumenter/Rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf.
NTB. (2022a, 16. mai). *Feilen med bankterminaler er rettet*. ABC Nyheter. https://www.abcnyheter.no/nyheter/norge/2022/05/16/195846313/feilen-med-bankterminaler-er-rettet.
NTB. (2022b, 16. mai). *Feilen med bankterminaler er rettet*. Digi.no. https://www.digi.no/artikler/problemer-med-kortbetaling-i-hele-norge/519568.
NTB. (2022c, 16. mai). *Intern IT-feil skapte kortkaos*. Finansavisen. https://www.finansavisen.no/nyheter/bors/2022/05/16/7868173/intern-it-feil-skapte-kortkaos?zephr_sso_ott=Etdmj8.
NTB. (2022d, 28. juni). *Stortingets direktør vedtar gebyr fra Datatilsynet og sier opp sin stilling*. Digi.no. https://www.digi.no/artikler/steve-wozniak-ber-bransjen-bremse-ai-utviklingen/528729.
Nygaard, K., Reite, M.H. & Vegge, T.F. (2022, 16. mai). *Kortterminaler over hele landet fikk problemer*. Fædrelandsvennen. https://www.fvn.no/nyheter/lokalt/i/5G7E4E/kortterminaler-over-hele-landet-er-nede.
Odenwald, S. (2009, 13. mars). *The Day the Sun Brought Darkness*. NASA. https://www.nasa.gov/topics/earth/features/sun_darkness.html.
Paust, T. (2023, 8. mars). *Forsvarseksperter stiller seg skeptiske til nye sabotasjeteorier fremmet av anonyme kilder*. Nettavisen. https://www.nettavisen.no/nord-stream/sabotasje/utenriks/sabotasjeteoriene-det-ville-vart-en-katastrofe/s/5-95-960669.
PayJunction Team. (2019, 27. juni). *POS Credit Card Terminal: The Advanced Shopping Guide*. PayJunction. https://blog.payjunction.com/credit-card-terminal-guide.
PMO. (2023). *Mr LEE Kuan Yew*. Prime Minister's Office Singapore. https://www.pmo.gov.sg/Past-Prime-Ministers/Mr-LEE-Kuan-Yew (Besøkt 5. juni 2023).
Polit, D.F. & Beck, C.T. (2010). Generalization in quantitative and qualitative research: Myths and strategies. *International Journal of Nursing Studies, 47 (2010)*, s. 1451-1458.
Popper, M. & Lipshitz, R. (1998). Organizational Learning Mechanisms: A Structural and Cultural Approach to Organizational Learning. *The Journal of Applied Behavioral Science 1998, 34*, s. 161-179. https://doi.org/10.1177/0021886398342003.
Pripp, A.H. (2018, 3. september). *Validitet*. Tidsskrift for Den norske legeforening. https://tidsskriftet.no/2018/09/medisin-og-tall/validitet.
Regjeringen. (2020, 28. januar). *Beredskap i den finansielle infrastrukturen*. Regjeringen. https://www.regjeringen.no/no/tema/okonomi-og-budsjett/finansmarkedene/beredskap/id2353825/.
Regjeringen. (2022, 1. september). *Vil styrke forbrukernes rett til å betale med kontanter*. Regjeringen. https://www.regjeringen.no/no/aktuelt/vil-styrke-rett-til-kontanter/id2926186/.
Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World*. Earthscan from Routledge.
Rise, E. (2021, 6. mai). *Østre Toten kommune: – Dataangrepet har kostet oss mer enn 32 millioner*. Aktuell Sikkerhet. https://www.aktuellsikkerhet.no/cybersikkerhet-datainnbrudd-it-sikkerhet/ostre-toten-kommune-dataangrepet-har-kostet-oss-mer-enn-32-millioner/700321.
Sandø, T. (2014, 8. august). *Slik har vi betalt*. Stavanger Aftenblad. https://www.aftenbladet.no/okonomi/i/a4jda/slik-har-vi-betalt.
Sentralbankloven. (2019). *Lov om Norges Bank og pengevesenet mv.* (LOV-2019-06-21-31). Lovdata. https://lovdata.no/dokument/NL/lov/2019-06-21-31.
Shen, R. & Armstrong, R. (2015, 22. mars). *Modern Singapore's founding father, Lee Kuan Yew, dies at 91*. Reuters. https://www.reuters.com/article/uk-singapore-lee-death-idUKKBN0MI0TN20150322.
Skaar, J. (2018, 15. mai). *Elektromagnetisme*. Store Norske Leksikon. https://snl.no/elektromagnetisme (Besøkt 9. mars 2023).
Skaare, K., Paulsen, E.O. & Risvaag, J.A. (2022, 24. februar). *Mynt*. Store Norske Leksikon. https://snl.no/mynt (Besøkt 14. mars 2023).
Skaare, K. (2023, 20. januar). *Daler*. Store Norske Leksikon. https://snl.no/daler (Besøkt 14. mars 2023).

S-N. (2022, 16. mai). *Stig måtte sende kunder til minibanken: 130.000 kortterminaler var nede*. Stjørdals-Nytt. https://www.s-n.no/nyheter/i/8Qdq2E/stig-maatte-sende-kunder-til-minibanken-130-000-kortterminaler-er-nede-over-hele-landet.
Solli, M. (2022, 19. mai). *Dagen før 17. mai kollapset norske betalingsterminaler. Årsaken bekymrer sikkerhetsekspert.* Nettavisen. https://www.nettavisen.no/okonomi/betalingskaos-skaper-bekymring-skadepotensialet-er-enormt/s/5-95-494550.
SpareBank 1. (2023). *Hvordan få bankkort for ungdom?* SpareBank 1. https://www.sparebank1.no/nb/bank/privat/kundeservice/kort/hvordan-far-man-bankkort-for-ungdom.html (Besøkt 26. april 2023).
Stampe, P. (2021, 15. juli). *Pengenes historie: Fra konkylier til euro*. Historie. https://historienet.no/samfunn/handel/pengenes-historie-fra-konkylier-til-euro.
Stavland, B. & Bruvoll, J.A. (2019). *Resiliens – hva er det og hvordan kan det integreres i risikostyring?* (FFI-rapport 19/00363). Forsvarets forskningsinstitutt. https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2540/19-00363.pdf.
Steen, R., Haakonsen, G. & Steiro, T.J. (2023). Patterns of Learning: A Systemic Analysis of Emergency Response Operations in the North Sea through the Lens of Resilience Engineering. *Infrastructures 2023*, *8*, *16*. https://doi.org/10.3390/infrastructures8020016.
Steen, R. & Rønningsbakk, B. (2021). Emergent learning during crisis: A case study of the arctic circle border crossing at Storskog in Norway. *Risk Hazards Crisis Public Policy 2021*, *12*, s. 158-180. https://doi.org/10.1002/rhc3.12211.
Steffensen, E. & Weme, S. (2016, 23. mai). *Tilsyn med beredskapen i det elektroniske betalingssystemet mv.* Norges Bank. https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Brev-og-uttalelser/2016/2016-05-23-Brev/.
Stor norsk ordbok (2023). *Resiliens*. Ordnett. https://www.ordnett.no/search?language=no&phrase=resiliens (Besøkt 24. januar 2023).
Suvatne, S.S. & Gilbrant, J. (2023, 24. mars). – *Ny kald krig*. Dagbladet. https://www.dagbladet.no/nyheter/ny-kald-krig/78846490.
Sveriges Riksbank. (u.å.). *1661 – First banknotes in Europe*. Sverige Riksbank. https://www.riksbank.se/en-gb/about-the-riksbank/history/historical-timeline/1600-1699/first-banknotes-in-europe/ (Besøkt 27. mars 2023).
Sættem, J.B. (2016, 3. mars). – *Absolutt ingen grunn til å bruke kontanter*. NRK. https://www.nrk.no/norge/_-absolutt-ingen-grunn-til-a-bruke-kontanter-1.12833531.
Taleb, N.N. (2010). *The Black Swan: The Impact of the Highly Improbable*. 2. utg. Random House.
Torvund, O. (2022, 5. august). *Kredittkort*. Store Norske Leksikon. https://snl.no/kredittkort (Besøkt 9. mars 2023).
Trondsen, F. (2006, 8. september). *Kortterminalene nede*. Aftenposten. https://www.aftenposten.no/norge/i/eELw4/kortterminalene-nede.
Tvedt, T. (2012). *Nilen – historiens elv*. Aschehoug.
Vodacom. (2023). *Butikkdata*. Vodacom. https://www.vodacom.no/kassel%C3%B8sning-pos-betalingsterminal (Besøkt 26. april 2023).
Vieira, P. & Monga, V. (2022, 23. februar). *Canada Banks Unlock Trucker-Protest Accounts on Police Guidance*. Wall Street Journal. https://www.wsj.com/articles/canada-banks-unlock-trucker-protest-accounts-on-police-guidance-11645645493.
Waterfield, J. (2018). *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation: Interviewer Bias*. SAGE Publications. https://methods.sagepub.com/reference/the-sage-encyclopedia-of-educational-research-measurement-and-evaluation/i11424.xml (Besøkt 14. mai 2023).
Wilson, J.R. (2019, 19. november). *The new era of high-power electromagnetic weapons*. Military Aerospace Electronics. https://www.militaryaerospace.com/power/article/14072339/emp-high-power-electromagnetic-weapons-railguns-microwaves.
Woltjer, R. (Red.) (2015). *Consolidation of resilience concepts and practices for crisis management* (DARWIN D.1.1). DARWIN. https://h2020darwin.eu/wp-content/uploads/2017/10/DARWIN_D1.1_Consolidate_resilience_concepts_and_practices_for_crisis_management.pdf.
Yago, J. (2020). *The ABCs of EMP: A Practical Guide to Both Understanding and Surviving an EMP*. Dunimis Technology Inc.
Yin, R.K. (2018). *Case Study Research and Applications*. 6. utg. SAGE Publications.
Øystå, F. (2022, 16. mai). *Problemet med kortterminalene er løst*. Svalbardposten. https://www.svalbardposten.no/butikker/problemet-med-kortterminalene-er-lost/484275.
Åmås, T. (2021, 8. desember). *Husholdningenes betalingsvaner*. Norges Bank. https://www.norges-bank.no/bankplassen/arkiv/2021/husholdningenes-betalingsvaner/.

VEDLEGG A: Intervjuspørsmål

Forskningsspørsmål 1: Hvordan legger aktørene i finanssektoren til rette for å fremme felles forståelse på tvers av organisasjonene i forbindelse med beredskapen for betalingsterminaler?

- Hvordan gjennomføres felles øvelser med de andre aktørene? Deltar dere på øvelser utover det som skjer i regi av BFI?

- Hvor ofte besøker dere og/eller mottar dere besøk fra andre organisasjoner? Føler du at dere kjenner til grunnleggende rutiner, arbeidsmåter o.l. hos de andre aktørene?

- I hvilken grad mener du at dere burde oppsøke kontakt med aktører dere ikke er i dialog med pr. i dag?

- Hvordan påvirkes samarbeidet av at markedet er konkurransedrevet?

Forskningsspørsmål 2: Hvordan fungerte det interorganisatoriske samarbeidet mellom aktørene i finanssektoren under bortfallet av betalingsterminalene 16. mai 2022 og hvilken lærdom trakk de ut av hendelsen?

- Hva var deres rolle under hendelsen 16. mai 2022? Var dere involvert i feilrettingen på noen måte?

- Hvordan opplevde du at samarbeidet med de andre aktørene fungerte mens hendelsen pågikk?

- Hvordan ble hendelsen fulgt opp i etterkant? F.eks. i BFI, men også eventuell uformell oppfølging?

- Oppfatter du et behov for å inkludere nye medlemmer i BFI basert på dine erfaringer fra 16. mai og andre hendelser?

- Oppfatter du eventuelt at medlemmer i BFI er i ferd med å bli overflødige basert på erfaringene deres med tidligere hendelser?

Forskningsspørsmål 3: Hvordan innretter finanssektorens aktører beredskapen for betalingsterminaler?

- Hvordan går dere frem med tanke på utarbeidelsen av beredskapen for betalingsterminaler? Bruk av risikoanalyser? Utgangspunkt i spesifiserte hendelser? Andre fremgangsmåter?

- Hvilke faktorer mener du kan påvirke hvilket beredskapsnivå dere legger dere på under en pågående hendelse?

- Hvilke ansvarsområder har dere internt i tilfelle en krise oppstår? Har dere definerte roller i kriseledelsen?

- Hvor ofte gjennomfører dere øvelser på egenhånd?