



Institutt for teknologi og sikkerhet

Resiliens og Sårbarhet i Norske Smart Byer:

Hvordan smart byer påvirker norsk transportsektor

Stian Wachelin Pollen

Masteroppgave i Samfunnssikkerhet SVF-3920

Vår – Juni 2022

Antall ord: 15 777



Sammendrag

Denne oppgaven undersøker hvordan konseptet Smart City eller smart by påvirker samfunnssikkerheten i Norge. Smart by er et konsept som har fått stor internasjonal oppmerksomhet de senere årene. Konseptet er utviklet i stor del som et for å møte de klimautfordringene vi står ovenfor. Derfor ønsket jeg med denne oppgaven å undersøke hvordan denne trenden innenfor byutviklingen med fokus på klimatilpasning påvirker andre deler av samfunnssikkerheten. Spesifikt tar oppgaven for seg hvordan smart by konseptet påvirker resiliensen eller sårbarheten til norske byer. Derfor er følgende problemstilling lagt til grunn for oppgaven «Er fremtiden mer resilient eller mer sårbar med Smart byer i Norge?»

Oppgaven er en kvalitativ studie og baserer seg på en dokumentanalyse av 7 sentrale dokumenter som legger føringer for smart by arbeid i Norge. Det teoretiske bakteppet for oppgaven tar utgangspunkt i teori om resiliens, sårbarhet, risiko samt teori på smart by som konsept. Oppgavens funn viser at smarte tiltak kan bygge resiliens dersom det legges til grunn i arbeidet. Videre viser funnene at frem til nå at transportsektoren innehar de resiliente evnene til å håndtere og gjenopprette etter en hendelse, men at disse evnene kan minske dersom ikke aktsomhet utøves i utviklingen av nye smart by prosjekter da disse kan gi økt sårbarhet gjennom å fjerne redundans i systemet og tilføye nye avhengigheter.

Nøkkelord: Resiliens, Resilience, Sårbarhet, Risiko, Smart by, Smart city, Digitalisering, IKT, IoT

Forord

Denne oppgaven markerer avslutningen på mitt toårige masterstudium i samfunnssikkerhet ved Universitetet i Tromsø – Norges arktiske universitet. Med det vil jeg rekke en takk til alle kunnskapsrike og dyktige forelesere gjennom studiet som har gjort sitt beste for å tilrettelegge i en tid med pandemi og usikkerhet.

Jeg vil takke venner, nære og kjære for støtten i den krevende tiden som det er å skrive en masteroppgave. Jeg vil spesielt takke mine kontorkamerater for faglige diskusjoner, vennskap og motivasjon til å møte opp på universitetet hver dag. Uten dere hadde ikke dette arbeidet vært mulig. Til slutt vil jeg takke min veileder Masoud Naseri for oppfølgingen gjennom arbeidet.

Tromsø 20.06.2022

Stian W. Pollen

Innholdsfortegnelse

<i>Sammendrag</i>	1
<i>Forord</i>	2
1 <i>Introduksjon</i>	5
1.1 Samfunnsutfordringer gjennom tidene	5
1.2 Smart byen	6
1.2.1 Definisjon av Smart by.....	8
1.2.2 Smart by i verden	11
1.2.3 Smart by i Norge	12
1.2.4 Utfordringer med Smart by	12
1.2.5 Slemme problemer med Smart byen	13
2 <i>Teoretiske tilnærminger</i>	15
2.1 Risiko	15
2.1.1 Akseptabel risiko, risikostyring og risikopersepsjon	15
2.2 Sårbarhet	16
2.2.1 Kaskadefeil.....	17
2.2.2 Avhengigheter og infrastruktur	17
2.2.3 New Public Management	18
2.3 Resiliens	19
2.3.1 Resiliens definisjon	20
3 <i>Metode</i>	23
3.1 Forskningsstrategi	23
3.2 Dokumentanalyse	23
3.2.1 Fordeler og ulemper	24
3.2.2 Dokumentutvalg	25
3.3 Validitet	27
3.4 Relabilitet	27
4 <i>Empiri</i>	29
4.1.1 Økonomi.....	29

4.1.2	Teknologi	29
4.1.3	Flere aktører	31
4.1.4	Samfunnssikkerhet	33
4.1.5	Klima.....	36
4.1.6	Smart by i Norge	37
4.1.7	Stordata.....	39
4.1.8	Oppsummering funn dokumentanalyse.....	40
5	<i>Diskusjon</i>	41
5.1	FS1: Hva er spesielt for Norge når man skal iverksette smart by initiativer? .	41
5.2	FS2: Hvordan påvirker smartby initiativer innenfor transport egenskapen resiliens hos Norske byer?	44
5.2.1	Evnen til å forutse	44
5.2.2	Evnen til å håndtere.....	46
5.2.3	Evnen til å gjenopprette.....	47
6	<i>Konklusjon</i>	48
7	<i>Litteraturliste</i>	50

1 Introduksjon

1.1 Problemstilling og forskningsspørsmål

Målet med denne oppgaven er å belyse hvordan smarte byer påvirker sårbarheten og resiliens til byer. Smart by ble valgt som tema for oppgaven etter å ha identifisert dette som en trend innenfor byplanlegging, og et tema som virker og bli mer og mer aktuelt i samfunnet. Fokuset for denne oppgaven vil spesielt bli på hvordan smarte by innenfor transportsektoren påvirker sårbarhet og resiliens, men på grunn av at smart by er så tett koblet utvikling i IKT vil temaer innenfor digitalisering og cybersikkerhet bli belyst i oppgaven. Videre er målet å vise hvordan staten legger til rette for smartby initiativer gjennom reguleringer og retningslinjer. For å utforske dette har jeg valgt følgende problemstilling med to tilhørende forskningsspørsmål for å besvare problemstillingen.

Problemstilling: Er femtiden mer resilient eller mer sårbar med Smart byer i Norge?

FS1: Hva er spesielt for Norge når man skal iverksette smart by initiativer?

FS2: Hvordan påvirker smartby initiativer innenfor transport egenskapen resiliens i Norske byer?

1.2 Samfunnsutfordringer gjennom tidene

Mennesker har vært utsatt for farer og trusler gjennom alle tider. Trusselbilder endrer seg over tid og i et byplanleggings perspektiv har den industrielle revolusjon og nyligere teknologiske revolusjoner i form av IKT-teknologi hatt enorm påvirkning for hvilke trusler som møtes og må håndteres for å oppnå et sikrere samfunn i dag. Regjeringen definerer 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.*» (Meld. St. 5 (2020-2021)). Denne definisjonen viser noe av kompleksiteten som samfunn må håndtere, de mest alvorlige truslene samfunnet står ovenfor stopper ikke ved landegrensene. Dagens samfunn er mer globalisert og utfordringer som menneskeskapt klimaendringer, tette koblinger i globale ikt-nettverk, finans og produksjonssystemer påvirker sårbarheten i samfunnet (Engen et al., 2016).

De første sporene etter større tettsteder som kan vi kan kalle for by dukker opp rundt 3000 år f.Kr., og hvordan man har sikret byer har reflektert hvilke trusler man opplevde. Etter hvert ble

det bygd murer rundt byene, og bymuren var et viktig forsvarsverk mot ytre fiender gjennom et par tusen år. Etter oppfinnelsen av kanonen ble bymuren et mindre egnet sikringstiltak og byer stod over ett nytt trusselbilde. Videre fra 1700-tallet opplevde byene en økt urbanisering og bebyggelsen ble stadig tettere. I de nordiske landene var den nye bebyggelsen gjerne bygget i trematerialer, og kombinasjonen av tett bebyggelse, bruken av åpen ild til oppvarming, matlaging og belysing ga liv til en ny og større trussel for beredskapen. Bybrannen er fremdeles en del av trusselbildet, men sikringstiltak i form av lover, reguleringer og brannberedskap har resultert i mindre alvorlige konsekvenser. Videre endret byene seg under den industrielle revolusjonen og truslene kom i større grad innenfra. Truslene kom nå i form av store sosiale forskjeller som medbrakte sykdommer, kriminalitet og helseproblemer. (Engen et al., 2016).

I moderne tid har byplanlegginger lagt mer vekt på hvordan skape byer som fungerer godt i form av helse, rekreasjon, gode bomiljø, effektiv transport og en fornuftig mellom og lokalisering av ulike funksjoner som boliger, industri og transport. Fra 1900-tallet har igjen fokuset på trusler endret seg, truslene fra indre og ytre fiender har fått mindre betydning for samfunnssikkerheten, og i dag er kanskje forurensning, miljø bærekraftig utvikling og klimaendringer ledende for byplanleggingen. Sikkerhet har alltid vært en sentral del av byplanleggingen gjennom tidene, nye teknologiske fremskritt har ført til nye muligheter for samfunnet, samtidig som de har brakt endringer i trusselbildet. (Engen et al., 2016). De teknologiske nyvinningene innenfor IKT har igjen påvirket dagens trusselbilde.

Det er noen av disse utfordringene som har gitt fødsel til konseptet Smart by. Smart byer har potensiale til å assistere i håndteringen av globale utfordringer knyttet drivhusgasser og menneskeskapt klimaendringer. Men her oppstår spørsmålet om smarte byer også øker sikkerhetsrisikoen for andre hendelser. Det er viktig å poengtere at innovasjoner som kan gjøre så mye positivt i sivilsamfunnet også åpner nye muligheter for aktører som ønsker å forårsake skade eller forstyrrelser. Lite har blitt skrevet knyttet smart city og sikkerhet frem til nå. (Nutall et al., 2020)

1.3 Smart byen

En rekke norske byer og kommuner arbeider nå med prosjekter innenfor rammen av det som kalles «smart city» eller på norsk «smarte byer eller kommuner» (Kommunal- og moderniseringsdepartementet, 2019). Selve begrepet smart city fenomenet har bred internasjonal interesse, men begrepet har blitt utfordret da det problematisk å presisere siden

det defineres ulikt av forskjellige teknologiske perspektiv og det ikke finnes krav til hva en Smart by skal bestå av (Al Nuaimi, Al Neyadi, Mohamed, & Al-Jaroodi, 2015, Parris, 2020).

Mange definisjoner av smart city eksisterer, men ingen har blitt universelt akseptert enda (Cocchia, 2014). Googler man begrepet smart city finner man resultater knyttet bærekraftige by initiativer, veikart for å øke grønn vekst og livskvalitet, nytten av IKT infrastrukturer, behovet befolkningsinvolvering i beslutningstakingen, behovet for å redusere digitale forskjeller og så videre. Selve definisjonen har vist seg flyktig, og noe av hinderet ligger i merkelappen «Smart». Selv begrepet smart er tvetydig og andre har brukt begreper som: Digital by, koblet by, intelligent by, kunnskaps by og grønn by for å beskrive samme kvaliteter som man finner i en smart by. Smart by er en politisk trend drevet av internasjonale institusjoner, for å implementere tilstrekkelige initiativer for å blant annet håndtere klimaendringene og redusere klimafotavtrykket.

Konseptet Smart City oppstod først på 90 tallet, på denne tiden var fokuset påvirkningen av ny informasjon og kommunikasjon teknologi på moderne infrastruktur i byer (Samih, 2019). Siden den gang har vi gått igjennom tredje generasjon (3G)-, fjerde generasjon (4G)- og står i dag ovenfor utbygging av femte generasjonsnettverk (5G) som vil gi enda større muligheter for Smart by initiativer. Samtidig har definisjonen vokst for å ta inn stadig nye aspekter, og viser en endring i tråd med samfunnsutviklingen. For å vise hvordan begrepet smart by har forandret seg over tid, og hvordan man forstår smart by i dag kan man i tabellen under se en rekke forskjellige definisjoner av begrepet. Det må fortsatt presiseres at ingen av disse er satt som en universell standard, og definisjonen av smart by virker og være ulikt for forskjellige satsinger. et lite utsnitt av ulike definisjoner av Smart City konseptet.

1.3.1 Definisjon av Smart by

Referanse	Definisjon
Hall et al. (2000)	En by som overvåker og integrerer forhold for alle sine kritiske infrastrukturer, inkludert veier broer, tunneller, jernbane, flyplasser, havner, kommunikasjon, vann, kraft og større bygninger, for å bedre optimalisere ressursene sine planlegge forebyggende vedlikehold, og overvåke sikkerhetsaspekter samtidig som de maksimaliserer tjenestene til innbyggerne.
Harrison et al. (2010)	En by som kobler sammen den fysiske infrastrukturen, IKT infrastrukturen, den sosiale infrastrukturen og forretningsinfrastrukturen for å utnytte byens kollektive intelligens.
Caragliu et al. (2011)	En by er smart når den investerer i menneskelig og sosial kapital og tradisjonell (transport) og moderne (IKT) kommunikasjon infrastruktur som fremmer bærekraftig økonomisk vekst og høy livskvalitet, sammen med klok forvaltning av naturlige ressurser gjennom deltakende styring.
EU (2022)	En smart by går utover bruk av digitale teknologier for bedre ressursbruk og mindre utslipp. Det betyr smartere urbane transportnettverk, oppgradert vannforsyning og renovasjonsanlegg og mer effektive måter å lyse og varme bygninger på. Det betyr også en mer interaktiv og responderende byadministrasjon, tryggere offentlige rom og møte behovene til en aldrende befolkning.

Sett ut fra tabellen kan man se at det er litt ulikt fokus område hos de forskjellige forfatterne. Hall et al. (2000) har fokus på overvåkning av kritisk infrastruktur for å optimalisere for å optimalisere byen. Ti år senere setter Harrison et al. (2010) fokus på sammenkobling mellom IT-, sosial- og forretningsinfrastruktur for bedre benyttelse av den kollektive kunnskapen i byen, men sier heller ikke noe om hva de ønsker å oppnå. Caragliu viser til investeringer i menneskelige, tradisjonelle og moderne infrastrukturer for å skape bærekraftig økonomisk vekst, øke livskvaliteten, bærekraftig håndtering av naturlige ressurser gjennom deltakende demokrati. Her kommer det frem klare mål man jobber mot, og bærekraftighet blir større fokus i smartby definisjoner i moderne definisjoner. Caragliu legger også fokus på deltakende demokrati for at en by skal være en smart by. I den Norske definisjonen av smart by fra Kommunal- og Moderniseringsdepartementet ser vi fokus på å forbedre de offentlige tjenestene gjennom bruk av digitalteknologi for å gjøre byer til bedre steder og bo og arbeide i. I likhet med den norske smart by definisjonen ser vi i EU sin definisjon at håndtering av klima- og miljøutfordringene satt som en sentral del av smart by definisjonen. EU sin definisjon er også den første som nevner trygge offentlige rom som en del av definisjonen og. Ingen av disse definisjonene nevner resiliens, robusthet eller sårbarhet eksplisitt, men 3 av 5 fokuserer på miljøaspektet av smart by.

Smart by har oppstått ut fra tre ulike deler: EU, som fokuserer på miljømessige krav, den digitale delen, basert på tidligere erfaringer av digitale byer og den kulturelle delen, som er, det menneskelige og sosiale kapital som er i stand til å bygge smarte samfunn. Jo større byen er, jo verre er deres klimaavtrykk, og jo større nytte har byene av smart by tiltakene, også jo større by, jo større er fordelene av data, kunnskapsdeling og Internett-tjeneste tilbud. (Cocchia, 2014). For denne oppgaven vil definisjonen til Caragliu et al. (2011) være sentral, men EU (2022) er inkludert ettersom flere norske byer har søkt støtte i EU smart by-programmer eller blir en del under EØS-avtalen (Meld. St. 20, 2020-2021, EU, 2022).

I et forsøk på å destillere de ulike tilnærmingene mot forståelsen av smart byer pekte Richter et al. (2015) ut seks karakteristikk:

- 1) Tilgjengelighet og kvalitet av IKT infrastruktur. IKT er ofte ansett som den viktigste av karakteristikkene av smart by, IKT legger til rette for den essensielle kommunikasjonen og

infrastrukturen nødvendig for «smart» aktivitet, inkludert sensor system, sky teknologi, energistyring og overvåking via smart nettverk.

2) Urban innovasjon, næringslivets engasjement er essensielt for å smart by initiativer. Ofte er ikke offentlige investeringer ikke tilstrekkelig for å drive kost-intensive smart urban vekst, næringslivet som representerer det private kapitale markedene er nødvendig for å innføre nok penger. For å tiltrekke disse må det offentlige bidra med å legge til rette med fordelaktige forhold. Disse to første karakteristikene er essensielle for om en by kan bli ansett som smart.

3) Sosial inkludering og tilgang på offentlige tjenester er en del av smarte byer. Denne karakteristikken har blitt utvidet til å inkludere ikke bare tilgangen på offentlige tjenester, men også muligheten til å være med å forme tjenestene til byen. Nøkkelen til dette er engasjement av byens borgere og ha deres representasjon i diskusjoner.

4) Vekst fra høyteknologiske og kreative industriens bidrag til urban vekst er en annen karakteristikke av smart city. Her er de myke infrastrukturene i det menneskelige og sosiale dimensjonene som er i fokus. Denne karakteristikken handler om kunnskapsnettverk (f.eks. gjennom høyt kvalifiserte arbeidstakere) og viktigheten å legge til rette for å tiltrekke seg kreative og ferdighetsfulle menneskelige ressurser for å utvikle smart byen.

5) Tett knyttet de andre karakteristikene er rollen sosial kapital og relasjonell kapital spiller. Relasjoner knyttet mellom individer legger til rette for læring, og samfunnet i en smart by må tilpasse seg og drive med kontinuerlig innovasjon. Borgere, økonomier og styresmakter er nødt til å være kompetent nok til å benytte IKT-løsningene i smart byen for å kunne høste fordelene av smart byens innføring. Når de sosiale og relasjonelle kapitalene blir ignorert av en by, kan det oppstå sosial polarisering, hvor det oppstår klasseskiller med de som er i stand til å dra fordelene av teknologien og de som ikke har kompetansen til å benytte teknologien som faller baki samfunnet (som kan føre til økonomisk polarisering)..

6) Den siste karakteristikken av en Smart City involverer sosial- og klimabærekraftighet. Den økonomiske og urbane veksten av en smart city må ta de hensyn til de begrensede ressursene. I byer med høy befolkningskonsentrasjon kan bruken av ressurser og produksjonen av søppel bli umåtelig stor, og behovet for bærekraftige løsninger som smart strømnett, smart programvare eller smarte trafikk system. (Richter et al. 2015, Parris, 2020)

1.3.2 Smart by i verden

Urbane sentere har lenge vært en drivkraft for økonomisk vekst og muligheter. I følge MGI (2011) prediksjoner vil de topp 600 urbane sentrene i verden stå for nesten 60 prosent av global BNP med 20 prosent av verdensbefolkning innen 2025. UNEP (2018) prosjekterer en økning av mennesker som bor i urbane områder fra 54 prosent (tall fra 2015) til 66 prosent innen 2050, det vil gi en befolkningsvekst i urbane områder på 2.4 milliarder og legge press på nye og eksisterende byer. Samtidig som den urbane befolkningen vil øke så utgjør byer i dag omtrent 3 prosent av landmassen på jorda, allikevel står de for rundt 72 prosent av det globale drivhusgassutslippet (EU, 2020). Med økningen av befolkningen i urbane områder vil forvalterne bli nødt til å håndtere en økning av teknologiske, sosiale, fysiske og organisatoriske utfordringer stammende fra en økt kompleksitet i samfunnet. Eksisterende utfordringer vi har i dag som luftforurensing, kriminalitet, sløsende energiforbruk opphoping av trafikk, manglende infrastruktur og offentlige tjenester kan forverres basert på valgenes som tas i byplanlegging. IT giganter som Cisco eller IBM har visjoner om byer hvor bygninger, veier, strøm nett og søppelhåndtering er sammenkoblet gjennom et tett nettverk av sensorer og trådløs teknologi, med permanent datadeling og maskin-til-maskin (M2M) integrering (Carvalho, 2015)

På verdensbasis har en rekke byer allerede innført SC initiativer. Byene strekker seg fra Paris, London, Toronto, New York Rio de Janeiro, Hong Kong, Tokyo med flere. Dette har vært initiativer som har søppelhåndteringseffektivisering, el-kjøretøy, smart strømnett, smartapplikasjoner for byer og innenfor offentlig transport for å nevne noen (Ejaz & Anpalagan, 2019). Innenfor smart byen spiller fenomenet tingenes internett eller Internet of Things (IoT) en sentral rolle. IoT er kommunikasjons paradigme som tillater hverdagslige objekter å kommunisere med hverandre gjennom internett. IoT paradigmet er særlig interessant i innføringen av en smart by da myndigheter er avhengig av Informasjon og Kommunikasjons Teknologier (IKT) for å utvikle smarte løsninger for å møte dagens utfordringer. I følge IoT analytics (2018) var topp tre IoT prosjekter i 2018 smart byer, sammenkoblet industri og sammenkoblede bygninger. Videre har Wood (2020) prosjektert at smart by markedsandelen er forventet å vokse fra 410.8 mrd. USD i 2020 til 820.7 mrd. USD innen 2025, med en sammensatt årlig vekstrate (CAGR) på 14 prosent.

1.3.3 Smart by i Norge

I en offentlig utredning fra 2000 gitt av Justis og politidepartementet stod det Dagens samfunn er mer sårbart enn før. En svikt i noen få avgjørende samfunnsfunksjoner kan føre til at store deler av samfunnet får omfattende problemer. Svikt i telekommunikasjon og kraftforsyning kan virke spesielt lammende for samfunnet. Forhold som bidrar til at vi står ovenfor nye sikkerhetsutfordringer er blant annet 1) de teknologiske endringene, 2) den økende kompleksiteten i samfunnet, 3) det økende kostnads og effektiviseringspresset, 4) reduksjon i bemanningen i mange virksomheter, 5) Utsettingen av offentlige tjenester til kommersielle virksomheter (NOU 2000:24, s.6). Selv om det har gått 20 år siden denne utredningen, og utviklingen innenfor teknologi har vært enorm så er budskapet like sentralt i dag.

Rambøll (2018) kunne identifisere 51 kommuner som jobbet med SC. De kunne vise til at SC samles i klynger rundt de store byene. På Vestlandet fant de 17 kommuner engasjert i Greater Stavanger og smart-kommuneprosjektet «Stavanger Smart Region», på Østlandet er 15 kommuner tilknyttet prosjektet «Smart Innovation Norway» (2022), og i Midt- og Nord-Norge har EU gitt Trondheim stempelet «smart by» og skal fungere som fyrtårn-by i prosjektet EU horisont (Trondheim kommune, 2021). I Bodø kommune har de Smartby-prosjekter innenfor transport og arkitektur gjennom bruk av IoT og sensorer (Bodø kommune, 2021).

1.3.4 Utfordringer med Smart by

Det er tydelig at smart by vil få stor betydning både i Norge og på verdensbasis er kan det være Selv om største delen av den globale BNP blir produsert i byer så er også ulikheten i byer størst, og dersom ikke de styres riktig kan de negative effektene overgå de positive (Monzon, 2015). En smart city kan følge den fysiske verden i sann tid og stå for intelligente løsninger til både byens lokale og besøkende med tanke på transport, helse, miljø og energi. Midlertidig dukker det opp spørsmål knytter sikkerhet og personvern i smart by tiltak. Når byer blir smartere, kan mennesker lide fra en serie av sikkerhets og personverns trusler knyttet til sårbarhetene av smart by applikasjonene (Zhang et al., 2017).

Denne oppgaven har hovedfokus på hvordan smart city initiativer knyttet transport påvirker resilience. For å forstå dette kan vi se hvordan man oppnår smart mobilitet. En smart by arkitektur inkorporerer sansene komponenter, heterogen nettverksinfrastruktur. De sansende komponentene er kan benytte ting som bærbare enheter, industrielle sensorer og smart enheter

(f.eks. smarttelefoner, smart meter og overvåkningskamera). Disse sensende komponentene er knytningen mellom den fysiske verden og informasjons verden. De sensende enhetene kan enten være satt ut av offentlige, private enheter eller båret av brukerne.

Samling av stordata er en av hjørnesteinene i utviklingen av smart city. Stordata fra engelske Big Data er et uttrykk man som har fått stor oppmerksomhet i nyere tid. Stordata er store datavolumer satt sammen av mange ulike datakilder med både strukturerte, ustrukturerte og sanntids data (Meld. St. 22 (2020-2021) s. 9). Stordata genereres av online transaksjoner, e-post, videoer, lyd, bilder, logger, poster, søk, helsedata, sosiale nettverk-interaksjoner, forsknings data, sensor og mobiltelefoner og deres nettverk. Denne dataen lagres i databaser som raskt vokser massivt og skaper vanskeligheter i å fange, forme, lagre, håndtere, dele analysere og visualiser gjennom typiske programvare for databaser (Sagiroglu & Sinanc, 2013, s. 42). Mobiltelefondata (MTD) er en av de viktigste kildene til Stordata og tjenester knyttet til transport og mobilitet er særlig avhengig av samtids data fra innbyggerne (Julsrud & Krogstad, 20).

Her åpnes et av problemene ved Smart by og Stordata, meste av den informasjonen som genereres er av lite til ingen interesse, og er nødt til å bli filtrert og komprimert i stor grad før de bringer nytte. Utfordringen som da oppstår, er hvordan definerer vi disse filtrene på en måte så de ikke forkaster nyttig informasjon. Ofte dataene som samles inn i et format er uegnet til analyse og krever videre prosessering for å kunne gi noen nytte. Videre er det ofte ukritisk antatt at når IKT-løsninger og digitalisering av byfunksjoner implementeres, at de umiddelbart bidrar til mer bærekraftig urban utvikling. Dette er en for enkel tankegang og glemmer å ta hensyn til noen av de slemme problemene «Wicked problems» smart byen kan medbringe.

1.3.5 Slemme problemer med Smart byen

«Wicked problems» eller slemme problemer er svært utfordrende problemer som er unike og vanskelige å definere, kategorisere og løse (Engen et al., 2016). I smart byen har man utfordringer knyttet IKT. En av hoved grunnene til å innføre smart by prosjekter er å redusere klima utslippene. IKT kan bidra med å gjøre byer mer energi effektive, men det å gjøre noe mer energieffektivt kan frembringe effekten energirebound hvor man har mer energieffektive løsninger som gjør at forbrukeren velger flere og mer kraftige elektroniske utstyr, og i stede for en reduksjon i energiforbruk ender man med en økning i forbruk over tid. Det har vist seg over

tid at en effekt hos mennesker til å rettferdiggjøre klimafiendtlige handlinger gjennom et fenomen kalt «negativ spillover» hvor mennesker som handler på en bærekraftig måte på et punkt bruker dette til å rettferdiggjøre å handle på en klimaskadelig måte i andre situasjoner. (Colding et al., 2019).

Colding et al. (2019) viser til at det oppstår en konflikt når gjenstander som smarttelefonen stadig tar større plass i samfunnet og utfører flere oppgaver. Med den økende bruken av smarttelefonen oppstår det en tilsvarende reduksjon av alternativer som bruk av betaling gjennom kontanter eller bankkort. Denne utviklingen får betydningen for offentlighetens valgmuligheter og når en teknologisk gjenstand som smarttelefonen blir for dominant, og lukker muligheten for alternative eller supplerende løsninger økes avhengigheten av gjenstanden. Dette kan og har fått betydning for forbrukere som kan bli presset til å ta valg som ikke er i deres beste interesse.

Som nevnt tidligere er deltakelse viktig for smartbyutviklingen, og smart byens grunnsten stordata legger til rette for at innbyggerne deltar gjennom deres sansende enheter. Her er en utfordring at det oppstår klasseskiller ved at stordataanalysene kun blir basert på de som har tilgang på sansende enheter eller internett. Videre vil teknologisk automasjon påvirke hverdagslivene til innbyggerne i smart byene, faren med dette er at det kan gjøre det vanskeligere å forstå egen påvirkning på miljøet siden det oppstår distanse mellom handling og konsekvens. Når automasjon øker svekkes situasjonsbevisstheten og behovet for å lære manuelle ferdigheter. Fra et resiliens perspektiv vil det å stole på fullt automatiserte systemer være risikabelt. (Colding et al., 2019).

2 Teoretiske tilnærminger

I dette kapittel vil jeg presentere oppgavens teoretiske rammeverk. Hensikten med dette kapittelet er å presentere hvilke tilnærminger som legges til rette for analysen av empiriske funn. Johansen et al (201) bruker begrepet teoretisk perspektiv som noe for å undersøke et fenomen fra en spesiell synsvinkel eller ut fra en bestemt betraktningssmåte. Å velge perspektiv betyr at oppmerksomheten rettes mot et spesielt område av fenomenet og handler om å avgrense og rette oppmerksomheten mot spesifikke felt eller fagområder. For denne oppgaven blir disse perspektivene førende

2.1 Risiko

Risiko blir ofte forbundet med noe negativt og truende, selve ordet ser ut til å stamme fra det italienske *risicare* som betyr «å våge». Denne kan vise til de positive sidene ved risikotaking, nemlig at det kan bidra til økonomisk fremgang og gevinst (Aven, 2015). En tradisjonell beskrivelse av risikobegrepet har gjennom begrepene sannsynlighet og konsekvens. Risiko har da blitt beskrevet som sammenhengen mellom sannsynligheten for at en hendelse kan inntreffe, og de konsekvensene hendelsen har dersom den inntreffer (SN-ISO, 2009 Lunde, 2014). Denne måten å forstå risiko er allikevel ikke dekkende nok og faglitteraturen på risiko skiller seg i to retninger. Der den første måten risiko ble beskrevet tar hensyn til de hendelser og konsekvenser fagfolk har kunnskaper om, har den andre betydningen av risiko mening der usikkerheten er ved hendelser som mennesker ikke har kunnskaper om, og som dermed ikke kan kvantifiseres (Hafting, 2017).

2.1.1 Akseptabel risiko, risikostyring og risikopersepsjon

Vi ønsker normalt å omgi oss med det vi oppfatter som akseptabel risiko som står i forhold til de verdiene vi forsøker å skape (Lunde, 2014). En måte å gjøre dette på er gjennom risikostyring, man vil aldri kunne forhindre alle hendelser, kriser og katastrofer og man er nødt til å leve med restrisiko. Restrisiko er den risikoen vi sitter igjen med etter forebyggende tiltak (Kruke, 2017). Norsk standard definerer risikostyring som (2009) koordinerte aktiviteter for å rettlede eller å styre en organisasjon med hensyn til risiko. Denne definisjonen sier oss lite om forståelsen risikobegrepet, men Aven (2015) sin definisjon av risikostyring viser mer hva som ligger bak: *«Risikostyring forstås som alle tiltak og aktiviteter som gjøres for å styre risiko. Risikostyring handler om å balansere konflikten mellom å utforske muligheter på den ene siden*

og å unngå tap, ulykker og katastrofer på den andre siden.» Denne definisjonen viser bedre at i risiko ligger det også muligheter. For beslutningstakere som skal innføre smarte tiltak i Norge handler det nettopp om denne styringen av risikoen.

Opplevelsen av risiko er ofte ikke objektiv, og i vår vurdering av risiko finner man også risikoopplevelsen (risikoperspektiv). Risiko kan oppleves større av emosjonelle prosesser som frykt, bekymring og angst (Aven, et al., 2017). Innenfor teknisk-naturvitenskapelig fagtradisjon har fokuset vært beregning og analyse av risiko ved bruk av matematiske, statistiske og fysiske modeller. I denne sammenhengen uttrykkes risiko ofte kvantitativt, med beredinger som hyppighet, frekvens eller sannsynligheter knyttet til opptreden av uønskede hendelser (Njå, et al., 2020). Risikoen vil alltid være vurdert av noen. De sannsynlighetene som blir beregnet, er sett gjennom perspektivet på den som regner. Risikoene som blir beregnet gjennom sannsynligheter og kunnskapsdimensjonene er ikke et uttrykk for den objektive virkeligheten, men menneskelige konstruksjoner og prognoser om mulige utfall i fremtiden (Engen et al., 2016). Selv om eksperter anser lekfolks oppfatning av risiko som helt irrasjonelle, har lekfolks oppfatning stor betydning i beslutningstakingen (Njå, et al., 2020). Beslutningene fattes ofte på bakgrunn av politiske meninger hvor både ekspertvurderingen og lekfolks oppfatning vil påvirke hvor man trenger tiltak.

2.2 Sårbarhet

Sårbare systemer er mer åpne for angrep, skade eller negative konsekvenser gitt en akutt situasjon, det er derfor viktig å ha forståelse for at sårbarhet ikke er statisk, men er i stadig endring. Engen et al. (2016) forstår sårbarhet som et systems forutsetninger for eller manglende evne til å fungere under og etter at det utsettes for en uønsket hendelse. Justis- og beredskapsdepartementet (2019) beskrev sårbarhet som et uttrykk for manglende evne til å motstå en tilsiktet handling eller uønsket hendelse, samt manglende evne til å gjenoppta sin funksjon. Det beskriver de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet.

Sårbarhet kan oppfattes som betinget risiko gitt en hendelse, en påkjenning eller en form for eksponering. Når vi snakker om et system er sårbart, mener vi at sårbarheten er vurdert å være stor. Poenget er at risikoen vurderes (ved hjelp av konsekvensangivelser, sannsynligheter og

bakgrunnskunnskap) å være høy forutsatt at systemet utsettes for en initierende hendelse. Hvis vi vet at systemet ikke har effektive barrierer eller beredskapssystemer dersom en feil skulle oppstå i systemet, vil vi si at sårbarheten er stor (Aven, 2015). Dermed er baksiden av dette at et system anses som trygt dersom antall uønskede hendelser holdes nede på akseptabelt nivå.

I en smart by vil det være mange ulike systemer som er koblet sammen for å kunne levere sine tjenester. Et system av systemer beskriver hvordan smarte byer omfatter flere systemer som samhandler i komplekse forhold, inkludert integrasjonen og interaksjonen med andre systemer for å gi nye funksjoner til byen, funksjoner som systemene ikke kunne gitt alene. Men disse systemene er ofte heterogene utviklet med ulike teknologier og data format, og eid av ulike distinkte organisasjoner som kan bringe utfordrer til utviklingen av smart byen (Cavalcante, 2017)

2.2.1 Kaskadefeil

Et slikt kompleks system som en smart by vil gi muligheten for kaskadefeil. Kaskadefeil oppstår når en svikt i en komponent utløser følgefetil på andre komponenter som forårsaker omfattende skader på hele systemet, miljøet og samfunnet (Xing, 2021). I en smart by vil det forekomme et nettverk med mange ulike noder som er koblet sammen. En kaskadefeil kan oppstå som at en tungt belastet node går tapt og dermed initierer en kaskadefeil ved at jobben til den tapte noden må redistribueres til andre noder i nettverket. Denne redistribueringen kan føre til at andre noder overgår sin kapasitet og får dem til å feile. Selv om den overbelastede noden ikke feiler, kan beskyttelsesmekanismer designet inn i nettverket gjøre at den blir stengt ned uansett, i et forsøk på å unngå nodefeil. Dermed kan nummeret nodefeil eller overbelastede noder øke og spre seg gjennom nettverket. I spesielt alvorlige tilfeller kan hele nettverket bli påvirket (Ash & Newt, 2007)

2.2.2 Avhengigheter og infrastruktur

Med infrastrukturer så finnes det naturligvis flere avhengigheter. Den raske teknologiske konvergensen på elektrisitet som den dominerende energisektoren og den digitale tilkoblingen er avgjørende for at alle infrastrukturnettverk skal fungere. Dette blir forsterket av de overordnede retningene av teknologisk endring. Beslutningstakere av infrastrukturer møter de på et trilemma mellom sikkerhet på tilgang og kvalitet, kostnader og karbonutslipp. 1) Sikkerhet på tilgang og kvalitet: For transport vil tilgang og kvalitet i første ledd handle om tilgangen på infrastruktur, men like viktig kan pålitelighet være (hvor stor del av tiden infrastrukturen faktisk

fungerer). For transport nettverk er reisetid den viktigste faktoren, ved siden av pålitelighet av reisetid, sikkerhet og komfort er andre kvalitetsrelaterte faktorer for passasjerer. 2) Kostnader: Infrastrukturs tjenester er finansiert gjennom en rekke bruker kostnader sammen med skatt. Siden infrastruktur er svært kostnadsintensive, må man ta nøysomme vurderinger over hvordan de finansielle byrdene skal støttes over livet til infrastrukturen for maksimere verdien over infrastrukturs levetid. 3) Karbonutslipp: Infrastruktur kan hjelpe og beskytte miljøet, men slike fordeler kommer sjelden uten kostnader. Mens fornybar energi tilfører lite forurensede forsyninger, ofte med null marginalkostnader, så er kan kostnaden av nye forsyningsanlegg og nødvendige justeringer for distribuerings- og overførings-infrastrukturer være høy. (Hall, 2019).

Noen av de største bekymringene knyttet avhengigheten som oppstår mellom infrastrukturer er knyttet natur katastrofer og sikkerhetsbrudd. Disse avhengighetene kan være knyttet geografisk: to eller flere systemer er lokalisert i samme fysiske område. Fysisk: en fysisk output fra ett system er nødvendig input for et annet, Cyber: informasjon produsert i et system påvirker operasjonen i et annet og menneskelig: Det er delt avhengighet av mennesker, f.eks. arbeider, organisatoriske eller sosiale system.

Seidu et al (2020) pekte til at den største risikoen til infrastruktur er volatiliteten til myndighetene og talte for nødvendigheten av en konsekvent infrastrukturpolitikk for å strømlinje prosessen for å redusere kostnads og tidsoverskridelse, og for å øke forutsigbarheten knyttet til kostnad og tid. Vel designet infrastruktur har blitt vist å ha økonomiske fordeler ved å øke økonomisk vekst og produktivitet. Infrastruktur er kronisk underfinansiert siden etterspørselen generelt er høyere enn tilbudet. Nummeret muligheter for kommersielle infrastruktur prosjekter er begrenset, siden tradisjonelt sett har infrastruktur gitt lave avkastninger. Investorer ønsker å unngå risikoen involvert i slike prosjekter, noe som kan resultere i at myndighetene må stille som garantist. (Seidu et al, 2020).

2.2.3 New Public Management

Under påvirkning av new public management (NPM) så har eierskapet, operasjon og vedlikehold av mange kritiske infrastrukturer blitt delt mellom et økt nummer av offentlig og private aktører. NPM er en betegnelse på transformasjonen av offentlig virksomheter mot en mer forretningsmessig styring tilnærmet markedet med fokus på å kutte kostnad og gjøre mer med mindre gjennom prosesser som outsourcing og strømlinjeproduksjon (Cedergren, 2018). NPM har gjort at industrier har i større grad blitt selvregulerende, mens staten etablerer lover

og reguleringer som de forsøker å kontrollere at blir møtt. Hvordan disse blir møtt er i stor grad opp til industriene selv (Bjelle & Sydnes, 2019)

2.3 Resiliens

I PST (2021) sin årlige trusselvurdering heter det: Samtidig som utviklingen av 5G og IoT gjør at stadig flere kommuner vil digitalisere, samkjøre og automatisere deler av sin virksomhet. Smartby-teknologien skaper nye avhengigheter og bidrar til at det utvikles sensitiv informasjon innenfor stadig nye samfunnsområder. Det gir også fremmede stater nye etterretnings- og sabotasjemål de mulig kan true.

I senere år har det vært et skifte på fokuset fra å beskytte gjennom forebyggende tiltak, til et fokus på å skape resiliens. Denne utviklingen anerkjenner at man aldri kan full beskyttelse, og det å oppnå ønsket nivå av beskyttelse ikke er kostnadseffektiv i møte med de faktiske truslene (Pursiainen, 2018). Resilience er nok et ullent begrep og brukes på tvers av en rekke fagdisipliner og har derfor en rekke ulike definisjoner. Opprinnelig stammer begrepet fra det Latinske ordet “resiliere”, som betyr å “å sprette tilbake” (Hosseini, Barker Ramirez-Marquez, 2015). Her har litteraturen på resiliens skilt seg i to retninger, den ene retningen fokuserer på ordets opprinnelse «å sprette tilbake» og viser til mens den andre retningen har fokusert på «å sprette fremover»».

Giacometti (2018) beskriver å sprette tilbake tilsier et systems evne til å returnere til normal posisjon ved å rekonstruere tidligere parametere etter den initierende hendelsen, mens å sprette fremover krever å finne en ny normal med å erstatte bestemte parametere med nye.

Å sprette tilbake vil oppstå når en enhet klarer å absorbere en forstyrrelse uten å forandre sin fundamentale kjerne og returnere til normaldrift, og en enhet kan sprette fremover dersom de underliggende faktorene ble fundamental forandret og å gå tilbake til normaldrift ble en umulighet. I et slik tilfelle kan fjerningen av uproduktive aktiviteter åpne for en ny fase av vekst og dermed etablere en ny normal. Selv om denne beskrivelsen av resiliens ikke er dekkende nok for alle ulike fasetter av begrepet resiliens så fanger det grunnprinsippet i Resilience.

Aven (2015) bruker begrepet om en enhets evne til å kjenne igjen, tilpasse seg og absorbere variasjoner, endringer, forstyrrelser og overraskelser. Aven er opptatt av hvordan systemet vil

fungere også hvis det eksponeres for en kilde eller hendelse vi ikke har tenkt på. Weick & Sutcliffe (2015) ser på resiliens som en miks av erfaring, pågående handling, intuitiv rekalkibrering, ofte basert på en minimal allerede eksisterende struktur. Begrepets voksende popularitet har fått noen forskere til å kritisk påpeke at det virker som alt og alle kan, og bør bli, resilient (Cedergren et al., 2018). I et forsøk på å konkretisere begrepet resiliens har jeg lagd et lite utdrag av definisjoner fra ulike fagdisipliner.

2.3.1 Resiliens definisjon

Forfatter	Definisjon	Fokus
UNDRR, n.d	Evnen til et system eller samfunn som er utsatt for farer til å motstå, absorbere, imøtekomme, tilpasse seg, transformere og komme seg etter en hendelse på en rettidig og effektiv måte, inkludert gjennom bevaring og gjenoppbygging av dens grunnleggende strukturer og funksjoner gjennom risikostyring.	Generisk
Boin et al, (2010)	Resiliens er kapasiteten til et sosialt system (f.eks. en organisasjon, by, eller samfunn) til å proaktivt tilpasse og komme seg etter forstyrrelser som er oppfattet av systemet til å falle utenfor den normale og forventede rammen av forstyrrelser.	Sosialt system
Norris et al. (2008)	En prosess som knytter sammen et sett adaptive kapasiteter til en positiv retning for funksjon og tilpasning etter en forstyrrelse	Samfunnsresiliens
Leipold & Greve (2009)	Et individs stabilitet eller raske bedring (eller vekst) under betydelige krevende forhold.	Psykologisk resiliens
Rose & Liao (2005)	Iboende evne og adaptive reaksjoner som gjør det mulig for bedrifter og regioner å unngå mulige tap	Økonomisk Resiliens

Rød et al. (2020)	Referer til de fysiske egenskapene hos kritisk infrastruktur, med fokus på deres evne til å motstå skade og minimere ethvert funksjonstap under en krise, eller raskt reparere den uønskede effekten	Teknologisk resiliens
-------------------	--	-----------------------

Felles for disse definisjonene er at man ser på resilience som en egenskap, istedenfor resultatet av en hendelse. Begrepet beskriver dermed ikke en statisk tilstand, men en evne til transformasjon i møte med påkjenninger. For smarte byer så kan vi benytte flere av disse definisjonene av resiliens fordi vi har det teknologiske aspektet av en smart by med sin infrastruktur og teknologiske artefakter og vi har den sosiale dimensjonen med menneskene som lever, jobber i byene og benytter seg og vedlikeholder teknologien i de smarte byene.

Når jeg i denne oppgaven snakker om resiliens i smarte byer oppstår spørsmålet, resilient mot hva? Et system kan være resilient mot en hendelse og, ikke resilient mot et annet (Aven, 2021) En smart by blir nødt til å håndtere moderne usikkerheter som naturhendelser, terrorisme, energi kriser og klimaendringer. For denne oppgaven vil fokuset være på hvor resilient den harde og myke infrastrukturen i smarte byer er. Samtidig belyse hvordan smarte byer har mange avhengigheter da en smart by er et system bestående av andre systemer. Enhver sivilisasjon er avhengig av infrastruktur systemer, inkludert transport vann, energi, telekommunikasjon, bank og finans (Cedergren et al., 2018, Hall 2019). Prosessen av digitalisering og elektrifisering fører til økt avhengighet mellom infrastrukturers nettverk, mens ressursknapphet som vann eller energi også fungerer til å intensivere avhengighetene (Hall, 2019). Smarte byer komplekse sosiotekniske system som krever koordinering av mange tekniske artefakter som skal fungere sammen med de menneskelige systemer som skal planlegge, levere, operere og vedlike holde disse systemene (Hall, 2019).

Resiliens i knyttet smart byen kan handle om trusler knyttet fysisk resiliens (angående å opprettholde fysiske enheter og ressurser under forekomsten av en forstyrrende hendelse og gjenopprette operasjoner raskt) til cyber resilience (angående å oppdage å beskytte mot ondsinnede cyber angrep og opprettholde evnen til trygg drift under angrepet) og kommunikasjons resiliens (med fokus på å opprettholde stabil og sikker kommunikasjon av informasjon i en hendelse med komponentfeil og trusler gjennom, for eksempel, robust routing protokoller eller nettverks selvorganisasjons teknikker (Xing, 2021).

Som vist i tabell 1 dekker ordet resiliens mange ulike forhold, men vi kan se noen sammenhenger i farene resiliens skal beskytte mot. Westrum (2006) legger tre ulike meninger til resiliens kan bety. 1) Resiliens kan bety evnen til å unngå at en hendelse inntreffer, 2) eller det kan bety evnen til å unngå at en hendelse går fra vondt til verre eller 3) det kan bety evnen til å komme seg etter en hendelse har inntruffet. Videre klargjør Westrum (2006) at det ikke er åpenbart at besittelsen av en av disse evnene til resiliens automatisk innebærer at man har de andre. Siden resiliens referer til noe et system gjør (en evne eller prosess) fremfor noe den har (et produkt), kan det ikke måles ved å telle spesifikke utfall som hendelser eller ulykker (Hollnagel, 2011).

Wreathall (2006) fant syv egenskaper høyt resiliente organisasjoner hadde: 1. Engasjement hos ledelsen. Ledelsen anerkjenner bekymringer og gir kontinuerlig og omfattende oppfølging. 2. Rettferdig kultur. Støtter rapportering av problemer og ser det som en mulighet for å lære om svakheter i organisasjonen. 3. læringskultur. Hvordan organisasjonen responderer til hendelser med fornektelse vs. reparasjon og endring. 4. Bevissthet. Samling av data som gir ledelsen innsikt i hva som foregår. 5. Beredskap, organisasjonen forutser problemer og forbereder seg på dem. 6. fleksibilitet evnen til å tilpasse seg nye eller komplekse problemer på en måte som maksimaliserer evnen til å løse problemet uten å forstyrre resten av systemet. 7 opasitet. Organisasjonen er bevisst på egne grenser og vet hvor nære de er kanten knyttet forringet forsvar og barrierer.

3 Metode

Hensikten med dette kapittelet er å argumentere og redegjøre for de metodiske valg som er tatt for å besvare oppgavens problemstilling. Denne oppgaven har benyttet en dokumentanalyse av offentlige dokumenter for å vise retning i utviklingen av smart by i Norge.

3.1 Forskningsstrategi

Samfunnsvitenskapelig metode omfatter både organisering og fortolkning av data som hjelper oss til å få en bedre forståelse av samfunnet (Riley 1963 i Holme & Solvang 1996). Metode skiller seg i to retninger kvantitativ og kvalitativ. Kort sagt stiller kvalitative og kvantitative ulike forskningsspørsmål. Kvalitativ metode defineres som former for datainnsamling som ikke har statistisk generalisering som formål, men ønsker å gi dybde, nyanser og/eller variasjonsmetning i fenomenet som undersøkes. Ved kvalitativ metode er opplegget mer fleksibelt, datainnsamling og analyse foregår parallelt, og de ulike fasene i forskningsprosessen overlapper hverandre mer enn ved kvantitative metoder (Halvorsen, 2008). Thagaard (2013) beskriver kvalitativ metode som godt egnet til studier av temaer som det er lite forskning på fra før, og hvor det er stort krav til åpenhet og fleksibilitet. Kvantitativ metode har som mål å skaffe data om et stort utvalg respondenter for å kunne generalisere disse til en enda større populasjon. (Iversen, 2011).

Denne oppgaven baseres på en kvalitativ metode, da kvalitativ metode har større fleksibilitet og rom for tolkning. Utfordringen i kvalitative forskningsopplegg er å få noe fornuftig ut av en stor mengde ustrukturerte data, redusere informasjonsmengden så den blir håndterlig, identifisere mønstre og lage rammeverk for å formidle innholdet (Johannesen et al. 2006)

3.2 Dokumentanalyse

Dokumentanalyse er en systematisk prosedyre for gjennomgang og evaluering av dokumenter (Bowen, 2009). Silverman (2013) sier det ikke finnes noen rett eller gal metode. Det finnes bare metoder som er bedre egnet for problemstillingen. Denne oppgaven tar form som en dokumentanalyse av relevante offentlige dokumenter og planverk som omhandler transportsektoren, digitalisering og samfunnssikkerhet i Norge. Dokumentanalysen finner sin data i dokumenter skrevet for et annet formål enn det som omfattes av forskningsprosjektet (Thagaard, 2013). Generelt kan man si at et dokument er språk fiksert i tekst og tid. Begrepet tekst er bredt omfavnende og inkluderer fotografier teknologier, fysiske objekter. (Lynggaard, 2012) En klassisk definisjon av et dokument er ethvert konkret eller symbolsk tegn som har

blitt bevart eller nedtegnet for det formål å representere, gjenskape eller påvise et fysisk eller intellektuelt fenomen. Nesten ingenting av betydning foregår uten at dokumenter er involvert. Om vi vil forstå samfunnet er det å studere og forstå dokumenter avgjørende. (Asdal & Reinertsen, 2021).

3.2.1 Fordeler og ulemper

Dokument analyse som metoder kommer med sine egne fordeler og begrensninger. Av viser fordeler Bowen (2009) at dokumentanalyser er:

- Effektiv metode: Dokument analyse er mindre tidskonsumerende og derfor mer effektiv enn andre undersøkelses metoder. Den krever dataseleksjon, isteden for data kolleksjon.
- Tilgjengelighet. Mange dokumenter er i tilgjengelige for det offentlige,
- Kostnad-effektive: Dokumentanalyser er mindre kostbare enn andre former for metode. Dataen er allerede samlet, og det som står igjen er for forskeren er å evaluere om innholdet og kvaliteten til dokumentene er tilstrekkelige.
- Ikke hindrende eller reaktive: Dokumenter blir ikke påvirket av forskningsprosessen, derfor blir ikke dokumentanalyse påvirket av refleksivitet som man finner i andre forskningsmetoder. Dette som f.eks. ved andre metoder hvor selve det at man observerer noe påvirker innsamlingen av data, siden hendelsene forløper annerledes på grunn av bevisstheten rundt situasjon.
- Stabilitet: Tillegg til å være ikke reaktive, er dokumenter stabile. Forskerens tilstedeværelser forandrer ikke hva som blir studert.
- Nøyaktighet: Inklusjonen av eksakte navn, referanser, og detaljer knyttet hendelser gjør dokumenter fordelaktige til forskningsprosessen.
- Dekning: Dokumenter gir bred dekning, de dekker lange tids perioder, mange hendelser og mange settinger.

Av begrensninger identifiserer Bowen (2009)

- Utilstrekkelige detaljer: Dokumenter er produsert uavhengig av forskningsprosjektet. Dette kan føre til at de ikke har nok detaljer til å besvare problemstillingen.
- Lav gjennfinnbarhet: Dokumentasjon kan noen ganger ikke være gjenfinnbare. Tilgang til noen dokumenter kan være bevisst blokkert

- Partisk selektivitet: I en organisatorisk sammenheng er de tilgjengelige dokumentene sannsynligvis på linje med bedriftens retningslinjer og prosedyrer, og i tråd med organisasjonens agenda.

Dokumentanalyse er passende å bruke i for å undersøke utvikling over en viss tidsperiode med henblikk på å identifisere stabilitet og forandring innenfor et gitt undersøkelsesområde (Lynggaard, 2012). Denne studien ønsker å se hvordan smartby initiativer har blitt tatt i bruk i Norge og hvilken betydning dette har for sårbarheten og resiliens. For å gjøre dette måtte jeg finne data som kunne belyse problemstillingen, som fulgte mine kriterier, og som var tilgjengelig. Data – flertall av latinske datum – betyr noe som er gitt, mens empiri kommer fra greske emperia som betyr forsøk, for denne oppgaven vil jeg bruke disse begrepene om hverandre og oppgaven baserer seg på empirien oppsummert i tabellen under Johannesen et al, 2006).

3.2.2 Dokumentutvalg

Kriteriene for at et dokument skulle bli inkludert i denne studien var at det dokumentene ikke kunne være eldre enn 5 år gamle. Dette på grunn av den raske teknologiske utviklingen gjør at tidligere publikasjoner blir irrelevant fordi de ikke inkorporer ny teknologi. Samtidig skulle dokumentene være gitt ut av regjeringens offentlige sider ettersom disse ville gi best representasjon om hvilken retning Norge er på vei. Til å starte å besvare problemstillingen ble Meld. St. 20 Nasjonal transportplan valgt ut som moderdokument, for å generere benyttet jeg snøballmetoden hvor det fulgtes dokumenter referert til i moderdokumentet og videre deres refererte dokumenter. I tillegg til dette ble det gjennomført søk på regjeringens sider for å sørge for at ikke andre relevante dokumenter gikk oversett.

Meldinger til stortinget har lagt stort grunnlag for denne oppgaven. Disse dokumentene har blitt valgt siden det i stor grad viser retningen i Norge. Disse dokumentene identifiserer utfordringer, muligheter og mål for samfunnet. I tillegg til dette gir de tydelighet med eksempler på tiltak gjort i Norge. I tillegg til disse dokumentene har jeg analysert innholdet i strategi for både samfunnssikkerhet i transport sektoren. I tillegg til dette har jeg analysert kartlegging for smarte byer i Norge, samt kartlegging og vurdering av stordata i offentlig sektor. Hver av disse dokumentene har fått en kode for å forenkle systematiseringen i empiri og diskusjonsdelen.

Dokumentnavn	Utgiver	År	Type	Kode
Meld. St. 20 Nasjonal transportplan 2022-2033	Samferdselsdepartementet	2020-2021	Melding til Stortinget	D1
Meld. St. 27 Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet	Kommunal – og moderniseringsdepartementet	2015-2016	Melding til Stortinget	D2
Meld. St. 22 Data som ressurs – Datadrevet økonomi og innovasjon	Kommunal – og moderniseringsdepartementet	2020-2021	Melding til Stortinget	D3
Meld. St. 5 Samfunnssikkerhet i en usikker verden	Justis- og beredskapsdepartementet	2020-2021	Melding til Stortinget	D4
Strategi for samfunnssikkerhet i transportsektoren	Samferdselsdepartementet	2020	Strategi	D5
Kartlegging og vurdering av stordata i offentlig sektor	Kommunal – og moderniseringsdepartementet	2016	Kartlegging	D6
Smarte byer og kommuner i Norge – en kartlegging	Kommunal – og moderniseringsdepartementet	2019	Kartlegging	D7

3.3 Validitet.

Utfordringen knyttet validitet er å samle inn data som er relevante for problemstillingen, for begrepet validitet kan vi også benytte gyldighet eller relevans (Halvorsen, 2008) Validitet handler om gyldigheten av de tolkningene undersøkelsen fører til (Silverman, 2013, Thagaard, 2014). Validitet blant annet om definisjonsmessig validitet. Definisjonsmessig handler om at det er godt samsvar mellom bruken av begreper i teoridelen, og i empiridelen (Halvorsen, 2008). For å oppnå dette i denne oppgaven har jeg forsøkt å presisere hva jeg mener med vært av de sentrale begrepene. Der jeg har lagt med flere definisjoner har jeg forsøkt å begrunne hvorfor de er en del av oppgaven, eller hvilken definisjon som vil bli sentral. For at oppgaven skulle ha høy troverdighet valgte jeg å ha dokumentanalyse av offentlige dokumenter som helt tydelig angir retningen og strategien for Norge. Med dette ville jeg unngå å ha informanter som ikke var kjent nok med hva smart by betyr for Norge ettersom begrepet Smart by fortsatt er veldig nytt.

3.4 Relabilitet

Data og empiri er ikke selve virkeligheten, men representasjoner av den. Virkeligheten er gjerne omfattende og kompleks, og data er mer eller mindre vellykkede representasjoner av virkeligheten (Johannessen et al. 2011). Relabilitet handler om forskningens pålitelighet (Thagaard, 2014). Ting som kan påvirke relabiliteten til forskningen er hva slags relasjoner forskeren har til datamateriale. Med dokumentanalyse har man fordelen at man ikke forholder seg til intervjuobjekter eller deltakende observasjon i felt som er vanlig for mange kvalitative studier. Dokumentene som har blitt brukt i studien er skrevet på vegne av organisasjoner som offentlige dokumenter. Dokumentene beskriver strategier og politiske retninger vedtatt på stortinget eller som faller under lovverk. Valget av disse dokumentene gjør at man unngår dokumenter som fremmer egne meninger, eller mangler dokumentasjon og nærhet til den som har ansvaret.

Selve begrepet relabilitet referer i utgangspunktet til om spørsmålet om en annen forsker benyttet seg av samme metoder som gitt i oppgaven, ville forskeren komme frem til samme resultat. Seale (1999 gjengitt i Thagaard 2014) skiller mellom intern og ekstern relabilitet. Ekstern reliabilitet er oftere vanskeligere å oppnå med kvalitative studier, da det knytter seg spørsmålet om repliserbarhet. Repliserbarhet handler om et forskningsprosjekt utført i en

situasjon kan gjentas av andre forskere i en annen situasjon. For å oppnå intern relabilitet må forskeren være konkret og spesifikk i innsamlingen og analyseringen av data. Dette har jeg forsøkt å oppnå ved å være transparent med hvilke dokumenter som er samlet inn, og kun benytte dokumenter som er offentlige og tilgjengelige.

4 Empiri

Dette kapittelet skal presentere funnene gjort i dokumentanalysen. Dokumentanalysen har tatt for seg ulike aspekter som ansett som relevant for smart by arbeid i Norge. Ut i fra dette har jeg valgt ut ulike tematiske gjengangere i dokumentene som vil få betydning for smart byen. Selv om noen av dokumentene ikke handler om smart by i seg selv, er de med på å belyse ulike aspekter som vil bli sentralt for smart by arbeid i Norge.

4.1.1 Økonomi

I D1 kommer det frem en av de mest sentrale utfordringene med infrastruktur i Norge, behovet for å binde sammen by og land og menneskene som bor der i er et langstrakt land som Norge med høye fell og lange fjorder gjør at planlegging og bygging av infrastruktur ofte er dyrt i Norge. Allikevel kan vi se at nivået på offentlige investeringer innenfor transportinfrastruktur er høyt i Norge sammenliknet med andre land som Tyskland, Storbritannia eller resten av Skandinavia. I tillegg til dette kan vi i D2 se at til tross for Norges topografi, så er Norge i verdenstoppen i tilbud av ekomtjenester. Siden 2003 er nivået på offentlige investeringer innenfor transport doblet seg målt mot BNP. Dette kan gi store muligheter dersom ressursene utnyttes godt. Befolkningsutvikling, bosetting, økonomisk vekst og nærings- og handelsmønstre er viktige drivere for transportbehovet i fremtiden.

I følge D2 er urbanisering og byvekst viktige drivere for Norges økonomiske utvikling. D2 legger vekt på byers attraktivitet og produktivitet, i tillegg gi storbyen stordriftsfordeler i form av større markeder, flere leverandører og større tjeneste- og infrastrukturtilbud. D3 viser til at den årlige verdiskapingen av norsk dataøkonomi er tilsvarende 150 milliarder kroner og dersom forholdene legges til rette kan dette dobles innen 2030. Til tross til at Norge tradisjonelt har hatt god økonomi understrekes det at de økonomiske rammene vil bli strammere i årene som kommer. De siste 10-15 årene har tiltak kunne blitt behandlet med utgangspunkt i at det ville oppstå økt handlingsrom i budsjettene fremover i tid. I fremtiden vil det være større grad av omprioriteringer og kutt som vil stille økte kost-nytte vurderinger til tiltak (D5).

4.1.2 Teknologi

Et digitaliseringsprosjekt er et utviklingsprosjekt eller endringsprosjekt hvor IKT-utgjør en sentral del, og som endrer arbeidsprosesser, organisering, regelverk eller teknologi. Norge er

allerede i en god posisjon for innføring av elektriske kjøretøy, i 2020 var andelen elektriske kjøretøy 53 prosent av nybilsalget og forventes å øke til 90 prosent i 2025 og videre til 95 prosent i 2030 (D1). Norge scorer generelt høyt i internasjonale rangeringer for IKT-utviklingen, men den raske utviklingen gjør at Norge hele tiden må forbedres for å kunne henge med og kunne utnytte digitaliseringens potensiale. Norges avhengighet av IKT er allerede stor og stadig økende. (D2).

D2 legger frem at intelligente transportsystemer (ITS) kan bidra til å løse flere av disse utfordringene. Dette går også igjen i D3, hvor bedre utnyttelse av data er nødvendig for å lykkes i overgangen til et mer bærekraftig samfunn og en grønnere økonomi. D2 definerer ITS som systemer for bruk av IKT-teknologi i transportsektorer. Formålet med ITS i Norge er å påvirke atferd og forbedre transportløsninger og trafikkavvikling slik at man oppnår bedre fremkommelighet, trafiksikkerhet, miljø, klima, tilgjengelighet og brukertilfredshet. I 2015 vedtok stortinget ITS-loven som gjennomfører EUs ITS-direktiv i norsk rett og skaper et hjemmelsgrunnlag til å sikre at ITS-applikasjoner skal kunne samarbeide på tvers av landegrensene (D2, D3).

Elektrifisering er en sentral del av det grønne skiftet, men innebærer nye belastningsmønstre på strømmettet og nye installasjoner. Når lys og varme styres trådløst viskes grensene mellom elsikkerhet og ekom ut. Når produksjonen av strøm skjer hos forbrukerne viskes grensen mellom elsikkerhet og energiproduksjon ut (D4). Utviklingen av 5G nettet er sentral for utviklingen av ITS. 5G legger til rette for M2M i større skala, og M2M har mange ulike anvendelser som sensornettverk, energiovervåking, utstyrssporing, smarte hjem, smarte byer, intelligente transporttjenester osv. (D3) Dette gjør også at mange tjenester kobles til nett som gir økt sårbarhet og avhengighet av internett for å betjene lys og varme og fare for hacking av styring og strøm (D4).

Videre argumenterer D2 for å benytte sikkerheten i ny teknologi og at de nye sikkerhetsutfordringene som følger av teknologiutviklingen ikke er et relevant argument for å stoppe utviklingen. D2 viser til at sikkerheten styrkes ved å fase ut gammel teknologi som er sårbar for nye trusler til fordel for ny teknologi med bedre sikkerhetsmekanismer. D2 argumenterer for at myndighetene bør legge til rette for overgang til mer sikker teknologi og kan bruke sin rolle som kjøpermakt til å stille krav om sikre løsninger når de skal anskaffe ekomtjenester.

Selv om digital sikkerhet er avgjørende for å ivareta nasjonal sikkerhet, viser erfaring at den forebyggende digitale sikkerheten er begrenset i mange virksomheter. Alle private og offentlige virksomheter har ansvar for å ivareta egen digital sikkerhet. Justis- og beredskapsdepartementet har et samordnings- og pådriveransvar for digital sikkerhet på sivil side, og utformer regjeringens politikk for digital sikkerhet gjennom nasjonale krav og anbefalinger. Erfaring viser midlertidig at disse blir fulgt opp i varierende grad. (D4).

4.1.3 Flere aktører

På norske veier har man flere aktører, fylkesveinettet utgjør nærmere 45000 km om lag fire ganger lengden på riksveinettet. Antall kjørte kilometer er fordelt med om lag 53 prosent på riksvei og 47 prosent på fylkesvei (D1). Ansvaret for fylkesveinettet ligger hos fylkeskommunen, Fylkeskommunen har ansvar for å planlegge, bygge, drifte og vedlikeholde fylkesveinettet herunder fylkesfergesambandet, samt for utvikling og drift av regional kollektivtransport. Fylkeskommunen har også ansvar for å organisere den regionale sivil transportberedskapen ved større kriser i fred, eller ved beredskap og krig. Dette innebærer å ha kartlagt transportbehovet i fylket, ha oversikt over og kontakt med sentrale transportaktører og ha utarbeidet krise- og beredskapsplaner for håndtering av uønskede hendelse. For riks- og europaveinettet har statens vegvesen ansvar for å planlegge, bygge drifte og vedlikehold, inkludert riksferjesamandene. Statens vegvesen har ansvar for nasjonale oppgaver som gjelder samfunnssikkerhet og beredskap, nasjonalt register for veidata og trafikkinformasjon på offentlig vei. Statens vegvesen har også ansvar for kontroll av tilsyn med kjøretøy og trafikanter. (D5).

Virksomhetene i transportsektoren skal forebygge og være i stand til å møte større uønskede hendelser, både utilsiktede i form av naturhendelser og teknisk- og menneskelig svikt, og tilsiktede i form av kriminalitet, terror, sabotasje og etterretningsvirksomhet (D5). Alle sektorer jobber med IKT-sikkerhet, i sivilsektor har Justis- og beredskapsdepartementet ansvaret IKT-sikkerhet, mens Forsvarsdepartementet har ansvaret på militær side. Samferdselsdepartementet har som sektordepartement ansvar for IKT-sikkerhet knyttet til elektroniske kommunikasjonsnett og -tjenester, herunder internett. Dette reguleres gjennom lov om elektronisk kommunikasjon. Nasjonal kommunikasjonsmyndighet (Nkom) har, som myndighetsorgan under departementet, et særskilt ansvar knyttet til sikkerhet og beredskap i elektroniske kommunikasjonsnett og -tjenester (D2). I tillegg til flere aktører på veinettet har

de mest sentrale infrastrukturforvalterne etablert egne responsenheter for digital hendelseshåndtering. Her er flere av virksomhetene tilknyttet Nasjonal cybersikkerhetssenter og Nasjonal sikkerhetsmyndighet NorCERT (Norwegian Computer Emergency Response Team) sitt sensornettverk gjennom varslingsystem for digital infrastruktur (VDI) (D1).

Samfunnet er svært avhengig av sikre og tilgjengelige ekomtjenester. Ekom og IKT er premissegiver for både kritiske samfunnsfunksjoner og annen kritisk infrastruktur. Arbeidet med ekomsikkerhet og beredskap krever derfor utstrakt samspill mellom ekomyndighetene og aktører både innenfor ekomsektoren og på tvers av andre samfunnssektorer. Avhengigheten mellom ekom og elforsyning gjør at ekomnettene må opprettholde grunnleggende reservestrømløsninger for perioder med bortfall av kraft (D2)

Forsvaret er i dag avhengig av private leverandører og eiere av kritisk infrastruktur og kritiske samfunnsfunksjoner. Sivil side har et ansvar for å legge til rette for at denne støtten kan operasjonaliseres på en tilfredstillende måte, og legge til rette for å kunne dekke både planlagte og uforutsette behov fra norsk og allierte militære (D4).

Mye av teknologiutviklingen som vil påvirke norsk transportsektor og smartbyutviklingen vil skje i privat regi og utenfor Norges grenser, utviklingen vil finne skje uavhengig av hvilke valg norske myndigheter tar (D1). Globalisering er en fellesbetegnelse på samfunnsendringer som bidrar til tettere integrasjon og avhengigheter mellom land gjennom økt flyt av informasjon, varer, tjenester kapital og mennesker (D4). Produksjon av norske ekomtjenester avhenger også i stor grad av fysisk infrastruktur og av innsatsfaktorer fra leverandører utenfor landets grenser. (D2) Utenfor Norges landegrenser ønsker EU bli ledende på utviklingen av intelligente transportsystemer gjennom rammeverk for å tilgang til, og deling av, data fra eksisterende og fremtidige transport- og mobilitetsdatabaser. For norske myndigheter vil noe av dette påvirke gjennom Europa og riksveier som faller under EØS-avtalen. Komplekse digitale systemer og tjenester som intelligente transportsystemer og tjenester kan gjøre sektoren mer effektiv, brukervennlig og sikker, gjennom effektiv styring, bedre kapasitetsutnyttelse og overvåkning av infrastrukturen. (D1).

Siden internett består av mange noder og kompleks infrastruktur finnes det ingen overordnet aktør som styrer infrastrukturen. Nasjoner, organisasjoner og selskaper har forsøkt å skape styringsregler, handlingsnormer, regelverk og andre former for regulering uten hell. (D2).

4.1.4 Samfunnssikkerhet

Dagens risikobilde gjør forebygging stadig viktigere. Den sikkerhetspolitiske situasjonen er forverret, som medfører økt risiko for spionasje, digital kartlegging og sabotasje. Samfunnets økte digitalisering gir statlige og ikke-statlige aktører nye verktøy og arenaer til å forfølge strategiske interesser. Norge har fått stor gevinst av globaliseringen, dette gjør at Norge er avhengig av at verdensmarkedet fungerer. Forholdet mellom globaliseringsprosesser og samfunnssikkerhet er komplekst. D4 peker på særlig fem viktige risikoforhold: 1) Konflikt og ustabilitet i andre deler av verden, 2) Internasjonal handel og ordninger for samhandling kan utnyttes til fiendtlige formål, 3) risiko knyttet til svikt i og manglende kontroll over verdikjeder for kritiske varer og tjenester, 4) Økt sosial ulikhet kan gi risiko for polarisering og 5) økt risiko for rask spredning av alvorlige smittsomme sykdommer.

D4 nevner forpliktelsene til NATO og et større behov for motstandsdyktighet i kritiske samfunnsfunksjoner og referer til traktatens artikkel 3. Artikkel tre tilsier at alle medlemstater av NATO skal ha resiliensen til å motstå hendelser som naturkatastrofer, sammenbrudd av kritisk infrastruktur og militære angrep. I denne definisjonen av resiliens, ses resiliens som summen av sivilberedskap og militær kapasitet.

I norsk sammenheng er smartby innenfor samfunnssikkerhet først og fremst knyttet å gjøre byene mer robuste mot ekstreme værutslag gjennom å håndtere flom, springflo og lignende. I Strategi for samfunnssikkerhet for transport legger de til rette for tre overnevnte mål i samfunnssikkerhetsarbeidet i transportsektoren: 1. Opprettholde høyt transportsikkerhetsnivå 2. Opprettholde fremkommelighet og funksjonalitet i transportsystemene og 3. opprettholde robust sivil beredskap. En stor andel av Norges kritiske infrastrukturer som IKT eies og driftes av private virksomheter. Dette betyr at viktige beslutninger om utvikling og sikkerhet tas av kommersielle aktører. D3.

Transport er en sentral del av samfunnssikkerheten i Norge, og transport defineres av sikkerhetsloven som både en kritisk samfunnsfunksjon og grunnleggende nasjonal funksjon noe som innebærer at et helt eller delvis bortfall av transportfunksjoner vil få konsekvenser for statens evne til å ivareta våre nasjonale sikkerhetsinteresser.. Både samfunnet og transportsektoren er i rask endring, og sektoren står dermed ovenfor et komplisert og sammensatt risiko-, trussel- og sårbarhetsbilde (D1). Smarte tiltak innenfor transport kan brukes for å gi rask varsling om alvorlige hendelser som får betydning for samfunnssikkerheten, men samtidig er den digitale avhengighet blitt en overordnet sårbarhet for hele transportsystemet.

Transport er også en viktig innsatsfaktor for en rekke sektorer og samfunnskritiske tjenester og er derfor en sentral del av totalforsvaret, og den nasjonale beredskapen. Samferdselsdepartementet har et overordnet ansvar for at en nasjonal sivil transportberedskap ivaretas gjennom tilrettelegging i infrastruktur og regelverk (D1). Det moderniserte totalforsvarskonseptet bygger på gjensidig støtte mellom forsvaret og det sivile samfunnet i hele krisespekteret. Denne understøttelsen av militær aktivitet stiller strenge krav til transportsystemet, og det blir derfor viktig med samordning mellom Forsvaret og relevante aktører på ulike nivåer. Transportberedskapen er bygd opp av samarbeid mellom offentlig myndigheter og private aktører, godt samarbeid mellom disse er avgjørende for å opprettholde tilstrekkelig transportevne under en krise. I kriser der markedet selv ikke klarer å løse transportbehovet har departementet hjemmel til å pålegge transportaktører å utføre visse transportoppgaver (D1)

Som et bidrag til en systematisk tilnærming i samfunnssikkerhet i transportsektoren lagde departementet en strategi for samfunnssikkerhet transport i 2009 som har blitt revidert i 2015 og 2020, etter de store organisatoriske endringene i transportsektoren, endringer i det sikkerhetspolitiske bildet, nye føringer for arbeidet med samfunnssikkerhet og resultater fra risiko- og sårbarhetsanalyser. Denne strategien tilsier at virksomheter innenfor transportsektoren skal rapportere til samferdselsdepartementet for oppfølging av strategien, Departementet fastsetter frister for rapporteringen gjennom bestillinger. Oppfølgingen av strategien for virksomhetene plikter de å 1. ha en egen strategi som konkretiserer hvordan virksomheten skal følge den overordnede strategien for samfunnssikkerhet i transportsektoren og 2. rapportere til departementet på status i oppfølging av egen strategi (D1).

Samtlige transportformer er avhengig av en rekke digitale systemer, og eksterne innsatsfaktorer som strømforsyning og elektrisk kommunikasjon for å levere sikre og effektive transporttjenester. Det digitale systemets evne til å håndtere både utilsiktede og tilsiktede uønskede digitale hendelser vil i økende grad bli en forutsetning for sikkerhet, pålitelighet og fremkommelighet i transportsektoren. Digital sikkerhet skal derfor inngå som en integrert del av transportvirksomhetens arbeid (D1). Norske data strømmer i stor grad gjennom utenlandskontrollerte nettverk, og en betydelig del av Norges kritiske infrastruktur har komponenter som er produsert av utenlandske selskap i utlandet (D4). Der infrastruktur eller innsatsfaktorer i utlandet er underlagt regelverk på tilsvarende sikkerhetsnivå som Norge vil det samlende sikkerhetsnivået kunne opprettholdes på tvers av landegrensene. EUs regulering av sikkerhet i ekomnett- og tjenester er på et svært overordnet nivå og Norge bør være pådriver

for en felles standard. Videre bør norske myndigheter stille krav til sikkerhetsnivået hos tilbyderne som selger ekomtjenester (D2).

I en datadrevet økonomi er kompetanse innenfor digital sikkerhet kritisk, undersøkelser gjort av NSM viser at mange virksomheter har mangler knyttet sikkerhetsbevissthet og sikkerhetskompetanse. God digital sikkerhet er fundamentalt i den dataøkonomien, og samfunnets sårbarhet for digitale trusler blir stadig større. Når det samles inn, lagres og bearbeides mer data øker også eksponeringsflaten for sårbarheter. Sammen med økende datamengder blir den digitale verdikjeden og aktørbildet mer komplisert, oftere er aktørbildet satt sammen av nasjonale og internasjonale aktører. (D3). Den raske utviklingen gjør det krevende å forstå hvilke trusler og sårbarheter som vil prege risikobildet. Feil eller utfall i digitale systemer og tjenester skjer på grunn av menneskelig feil, programvarefeil, utstyrsfeil, naturhendler eller kombinasjon av disse (D4).

At Norge er helt i toppen med IKT bruk gjør Norge mer konkurransedyktige, innovative og produktive, samtidig gjør digitaliseringen at Norge er et av landene hvor endringen i risiko- og sårbarhetsbildet er størst. En av de største utfordringene med å være så langt fremme i den teknologiske utviklingen er at man ikke har land å se til for eksempler. Dette endrer hvordan man forholder seg til sårbarheter i samfunnet og øker usikkerheten. Mange av dagens utfordringer kan bare løses i internasjonalt, og for Norge blir det viktig å delta i de internasjonale arenaene hvor relevante problemer diskuteres (D2).

I dag er nær sagt alle ekomtjenester basert på programvare som kommuniserer over en felles fysisk infrastruktur. Felles plattform for ekomtjenester gir kostnadseffektive løsninger, men løsningene medfører høy grad av kompleksitet og kan øke tilbyderens avhengighet til underleverandører. I tillegg introduseres nye sårbarheter knyttet til både utilsiktede hendelser som programvarefeil, og tilsiktede hendelser som cyberangrep. Økt sentralisering av tjenesteproduksjonen fører dessuten til økt skadepotensiale dersom det først skulle skje noe galt (D1)

Det er en trend i følge D2 at det fysiske utstyret i økende grad blir plassert i eksterne drifts- og datasentre. Dette i kombinasjon med managed services hvor utstyrsleverandører i tillegg til å selge og installere selve utstyret, også står for den daglige driften av nettverket. For å effektivisere driften sentraliserer tilbyderne sin tjenesteproduksjon i ett land og leverer ekomtjenestene på tvers av landegrenser. Fra et sikkerhetsperspektiv kan dette gjøre det

utfordrende for de nasjonale tilbydernes kompetanse, evne til risikostyring av virksomheten og kontroll med trafikkdata og kommunikasjon på tvers av landegrenser. For regulerende myndigheter er det også et problem da aspekter av tilbyderens virksomhet kan ligge utenfor myndighetens jurisdiksjon.

Sammen med at den økende outsourcingen av ekomtjenester så har ekomsektoren vært regulert av overordnede metodekrav og bruk av standarder gjennom blant annet ekomloven. Dette innebærer at tilbyderne av ekomtjenester har stor fleksibilitet i valg av løsning. Samtidig som det stiller store krav til hvilke vurderinger tilbyderne selv gjør. Myndighetene pålegger kun krav der tilbyderne ikke når kravene i ekomregelverket til sikkerhet og beredskap. D2.

Telenors transportnett bærer en majoritet av den totale elektroniske kommunikasjonen i Norge. D2 beskriver det som en sårbarhet som må håndteres at Norge anghenger av en enkeltaktørs transportnett, og for å ivareta sikkerheten i en tid med økt internasjonalisering av nett og tjenester, vil det være økende kommersielt behov for uavhengige robuste sambandsoverføringer mellom Norge og utlandet. Økt kapasitet og flere føringsveier ut av landet vil også være nødvendig for å møte et økende kommunikasjonsbehov til utlandet.

For å redusere sårbarheten er det viktig at forvaltningen og næringslivet stiller relevante krav til sikkerhet og robusthet. Dette gjør at tilbyderne i større grad ser seg tjent med å investere i sikkerhet i sine tjenester. Samfunnets avhengighet av tjenester som benytter eldre teknologiske løsninger gjør det vanskeligere å få til en rask overgang til nyere, tryggere og mer fremtidsrettede løsninger. Eldre teknologi er typisk utviklet for et annet trusselbilde og for andre tjenester. Dette fordi eldre teknologi blir eksponert for trusler som ikke var forutsett da teknologien ble utviklet. Dette akkumulerer til et unødvendig høyt risikonivå. D2.

4.1.5 Klima

D4 legger til grunn at klimaendringer er en av vår tids aller største utfordringer. Videre at som følge av klimaendringene vil natur hendelsene bli mer alvorlige. Den enkelte sektor og forvaltningsnivå har et selvstendig ansvar for å redusere konsekvensene av klimaendringer innenfor eget område. Selv om klimatilpasning er et arbeid som går på tvers av alle sektorer.

I D1 handler klimatilpasning handler om å forebygge uønskede hendelse og risikoreduserende tiltak for å redusere skadeomfang når hendelsen inntreffer. En stor andel av de uønskede hendelsene i transportsektoren med store samfunnsmessige konsekvenser er naturhendelser. D1

tar hensyn til klimaframskrivingene som viser til at hele landet vil oppleve et endret klima, med ulike effekter i ulike geografiske områder. De venter at uønskede naturhendelser vil øke i både frekvens og styrke frem mot år 2100. Hendelsene de forventer er hyppigere og sterkere nedbør, i tillegg til havnivåstigning og økende fare for større stormflohendelser. I D2 er også klimaendringene nevnt som en av de største utfordringene verden står ovenfor i dag, men legger vekt på at det finnes betydelige muligheter innen IKT for å bidra til mindre klimagassutslipp og bedre miljø. Det legges vekt på at smart anvendelse av digital teknologi blant annet kan muliggjøre bedre ressursutnyttelse og mer effektiv energibruk.

4.1.6 Smart by i Norge

IKT har etter hvert blitt synonymt med «smart», definisjonen av smarte byer kan variere ettersom begrepet har forandret seg i takt med den teknologiske og samfunnsmessige utviklingen. Smartbyinitiativer har som mål å forbedre offentlige tjenester og innbyggernes livskvalitet, utnytte felles ressurser optimalt, øke byenes produktivitet, samt redusere klima- og miljøproblemene i byene. 90 prosent av Norges befolkning bor i byer og byområder. I Norge legges det opp til at 5G-teknologi skal være en bærebjelke for tingenes internett. (D2). D7 bruker følgende definisjon for å forstå smart by i Norge «En smart by bruker digital teknologi til å gjøre byene til bedre steder å leve, bo og arbeide i. Smartby-initiativer har som mål å forbedre offentlige tjenester og innbyggernes livskvalitet, utnytte felles ressurser optimalt, øke byenes produktivitet, og å redusere klima- og miljøproblemer i byene.».

Videre beskriver D7 smartbyprosjekter som: Prosjekter som tar utgangspunkt i innbyggernes og brukernes behov, og involverer disse i utviklingen av løsninger. Hvor løsningene tar i bruk moderne teknologi for å forenkle og forbedre. Det kan for eksempel handle om å benytte mulighetene som ligger i automatisering, bruk av «Big Data», deling av åpne data, og bruk av digitale sensorer IoT. Hvor prosjektene innebærer ulike samarbeidskonstellasjoner på tvers av kommune, eller med næringsliv, organisasjoner og akademia

D7 fant at et sted mellom 30-50 kommuner arbeider med smartby i Norge. Videre fant de at flere kommuner ikke benytter Smartby-begrepet selv, selv om de har prosjekter som passer inn i definisjonen. Smartby som begrep er ganske nytt i Norge og satsingen faller på regionalt nivå. D7 fant at De fleste smartbyinitiativer ligger innenfor smart transport og infrastruktur, sammen med smart drift av bygg og smart energi. Smartby prosjekter kommer ofte fra linjen, fra ildsjeler eller medarbeidere med særskilt interesse eller kompetanse.

Kommunene er selvstending forvaltningsnivå noe som innebærer at kommunene selv er ansvarlig for iverksetting av digitalisering og ivaretagelse av egen digital sikkerhet (D4 & D7). De fleste norske byer er for små til å investere i smartbykompetanse og teknologi på samme nivå som store byer i utlandet. I mange tilfeller er norske smartbyprosjekter finansiert av forskings og utviklingsmidler (D2). D2 ser det som viktig for norske smartbyprosjekter at man ser internasjonalt etter velprøvde løsninger fra byer i tilsvarende posisjon. Samtidig legger de vekt på at for å realisere smarte samfunn vil det være nødvendig med stor grad av samhandling mellom ulike etater og aktører innenfor ekom-, energi-, helse-, finans- og transportsektoren. De opplevde barrierer mot smart by i Norge er manglende digitale standarder for deilig av data, organisatoriske siloer og tilgang til kompetanse og kunnskap i kommunene (D7).

Tidligere var ekomtjenester dominert av informasjonsutveksling mellom personer (tale, meldinger osv.), eller ved interaktiv kommunikasjon mellom person og tjenesteserver (internetturfing, nettbank, film osv. Dette er i dag i endring, og i senere tid har smarte løsninger hvor objektene kommuniserer hverandre fått større fokus. Dette er løsninger som mindre skala som smarthus og smarte bedrifter eller større som smarte byer, intelligente trafikksystem og smart miljø. (D2). Smarte byer vil gi en enorm

D2 viser til at mange digitaliseringsprosjekter både offentlige og private er krevende, har høyt ambisjonsnivå og stor kompleksitet. Dette gir høy risiko. En av regjerings hovedprioriteringer i IKT-politikken er å profesjonalisere planleggingen og gjennomføring av slike prosjekter, slik at kompleksitet og risiko reduseres og man får realisert de planlagte gevinstene. Videre har de identifisert på at tre grunner til at digitaliseringsprosjektene ikke lykkes er: 1) Enkelte prosjekter har feil resultatmål i forhold til virksomhetens reelle behov. 2) Virksomhetene mangler tilstrekkelig erfaring og kompetanse til anskaffelse og gjennomføring. 3) Anskaffelsesprosessen gjør ofte at den mest optimistiske, og ikke nødvendigvis den beste leverandøren vinner. 4) Prosjektet går over flere år, med risiko for at valgt teknologi allerede er utdatert før lansering. 5) Urealistiske gevinstberegninger og manglende evne til å realisere gevinster etter endt prosjektperiode (D2).

D1 legger de rette for at tiltak skal gjennomføres nasjonalt. Investeringene skal komme alle veieiere til gode, og utvikling og gjennomføring av piloter vil ha nasjonal karakter slik at alle deler av Norge for mulighet til å bli involvert. I Norge har man valgt flere norske veistrekninger

som skal være pilotprosjekter for å teste intelligente transportsystemer. Et av disse strekningene er fra Skibotn til Kilpisjärvi, denne strekning har blant annet blitt utstyrt med teknologi som akustiske fiberkabler, kameraer, blåtannlesere, reisetidsantennener og værstasjoner. Dette pilotprosjektet har vært et samarbeid mellom private og offentlige aktører i Norge, Sverige, Danmark og Finland. Prosjektet har vært delfinansiert gjennom EU. Et annet tiltak gjennomført er Augment City som bygger digitale tvillinger av byer, i Norge var Ålesund valgt ut som testby men gjennom testperioden har Augment City blitt solgt inn til 17 byer og tatt i bruk i flere prosjekter. I dette prosjektet har partnerne vært Statens Vegvesen, Trondheim Kommune, Telenor, Easy Park og VY.

4.1.7 Stordata

De potensielle samfunnsmessige gevinstene for stordata i Norge er store. Generelt har offentlige virksomheter kommet kort i bruke av stordata (D6). Stordata kan bidra til å forutse atferd og hendelser, i offentlig sektor testes nå stordatateknologi. Vegdirektoratet tester ut stordatateknologi til planlegging av vedlikehold, trafikkavvikling og kapasitetsplanlegging i veinettet (D1 & D6). Databaserte analyser kan gi mer effektiv ressursbruk gjennom vedlikeholdsplanlegging, og bedre datagrunnlag for å vurdere hvilke investeringsprosjekter som gir positiv samfunnsøkonomisk effekt. I D1 viser de til at statens vegvesen planlegger å utvikle en digital tvilling for riksveinettet, som er egnet for overordene analyser. Dette prosjektet skal sikre en helhetlig utforming av veinettet, som blant annet tar hensyn til kjøretøy med avansert teknologi og automatiserte løsninger.

Utviklingen i sensorteknologi har gjort at sensorteknologi har gitt bedre, mindre og billigere sensor. Dette sammen med at kommunikasjonsteknologien har blitt bedre og fortsetter å bli bedre gjennom utviklingen av 5G. Bruk av data har skala fordeler, sammenslåing av to komplementære datasett kan gi mer innsikt enn datasettene hver for seg. Store datamengder er i utgangspunktet ikke nok for å skape verdier. Det er først når data settes i en sammenheng, analyseres og bearbeides, at det skapes verdier. En måte å gjøre dette på er gjennom datadeling. Datadeling må balanseres mot eventuelle ulemper for personvern, konkurranse og nasjonale interesser. Her finnes det utfordringer knyttet det å finne løsninger for datadeling som ikke strider mot egne forskningsinteresser som kan være både komplisert og ressurskrevende. I tillegg mangler det insentivstrukturer og bærekraftige delingsmodeller som reduserer usikkerhet knyttet dataeierskap og rettigheter. D3.

Det offentlig har to roller knyttet stordata, myndighetene påvirker rammebetingelser ved å legge til rette for stordata bruk, og for å sikre at teknologien ikke blir misbrukt. Deres andre rolle er stordata i egen offentlig tjenesteproduksjon. Utviklingen av teknologier som stordata, automatisering og kunstig intelligens antas å være en viktig for tjenesteproduksjonen i fremtiden (D2). D6 finner at introduksjonskostnader er et av de største hindrene for introduksjon av stordata teknologi, men at mange virksomheter er nysgjerrige på teknologien.

Markedet for stordatatjenester domineres av noen få store aktører. Aktører som IBM, HP, EMC og Amazon er ledende på markedet, markedet totalt sett kan fortsatt sies å være umodent. Markedets umodenhet er enda et hinder for bruk av stordata (D6).

4.1.8 Oppsummering funn dokumentanalyse

Smartbyen er avhengig av mange ulike systemer som skal snakke sammen. Stordata, IoT og IKT-løsninger er grunnpilarer i smart by arbeidet. Samtidig viser det at fokuset i samfunnsikkerhetsarbeidet handler om å håndtere klimaendringer. Dette viser at smart by konseptet i stor grad handler om klimatilpasning. Samtidig viser funnene at Smart by konseptet er i sin spede begynnelse i Norge, men at det er store muligheter for Norge i denne typen arbeid både økonomisk og samfunnsnyttig. Videre viser funnene at Norge i stor grad vil bli påvirket av eksterne aktører både i form av andre nasjoner, men også teknologisk utvikling gjort av private aktører.

5 Diskusjon

Formålet med denne studien har vært å se hvordan det arbeides med smart by i Norge og hvordan dette påvirker sikkerheten i norske byer og generelt i landet. Resultatene skal forsøke å vise retningen i arbeidet i Norge gjennom offentlige dokumenter, og se hvordan dette påvirker sårbarhet og resiliens basert på den teorien oppgaven legger til grunn. Dette kapittel skal diskutere funnene av dokumentanalysen. Diskusjonskapittelet er systematisert etter forskningsspørsmålene.

5.1 FS1: Hva er spesielt for Norge når man skal iverksette smart by initiativer?

Empirien viser at Norge bruker penger mer enn andre tilsvarende land som andel av BNP (D1). Norges gode økonomi legger til rette for å kunne gjennomføre investeringer innenfor smart by prosjekter. Urbanisering og byvekst er store drivere for Norges økonomiske utvikling (D2), dette sammen med utviklingen innenfor dataøkonomi gjør at smarte byer vil bli mer attraktivt fremover. Samtidig som Norge ikke har noen overordnet strategi for norske smart byer viser D7 at smart by arbeider foregår i mange ulike norske byer og at det i stor grad handler om hvordan byene definerer det selv. Vi kan se at det er mange ulike aktører på det norske veinettet. Veiene har forskjellig eier etter om de er satt som riksvei, fylkesvei eller europavei, hver av disse bringer egne aktører og vil stille store krav til samhandling.

Selv om ikke alle byer definerer seg sitt digitaliseringsarbeid som smartby arbeid kan vi se paralleller mellom definisjonen av digitaliseringsprosjekter og smartby arbeid. «*Et digitaliseringsprosjekt er et utviklingsprosjekt eller endringsprosjekt hvor IKT-utgjør en sentral del, og som endrer arbeidsprosesser, organisering, regelverk eller teknologi*» (D3). Ser vi denne i lys av den norske definisjonen av smart by fra D7: «*En smart by bruker digital teknologi til å gjøre byene til bedre steder å leve, bo og arbeide i. Smartby-initiativer har som mål å forbedre offentlige tjenester og innbyggernes livskvalitet, utnytte felles ressurser optimalt, øke byenes produktivitet, og å redusere klima- og miljøproblemer i byene.*». Med dette kan det se ut til at smart by arbeid kan forekomme selv om byer selv ikke blir definerer det som smart by arbeid. Dette gjør at denne oppgaven handler i like stor grad om hvordan fremtidsutviklingen innenfor digitalisering i Norge påvirker sårbarheten og resiliensen, som den handler om smart by. Alle byer vil bli påvirket av den teknologiske utviklingen og det vil bli naturlig utvikling at byer investere i IKT-teknologier. Å bygge infrastruktur krever langtids forpliktelser, når de først er bygget kan infrastruktur være svært kostbart og modifisere eller fjerne.

Vi kan også se likhetstrekk mellom den norske definisjonen av smart by og de internasjonale, særlig de mer moderne definisjonene til Caragliu et al (2011) og EU (2022). Dette kan være et resultat av at det norske smart by arbeidet fremdeles er ganske nytt fenomen. Dette kommer også frem i D7. Det at Norges definisjon ikke skiller seg fra internasjonale kan være fordelaktig i Norges smart by arbeid. Dette åpner for samarbeid mellom andre land som har egne smart by satsninger, og kan gjøre at det kan samarbeides rundt utviklingen av smarte prosjekter. Definisjonen er samtidig viktig da den sier noe om hva teknologi skal brukes til. Dette gir rammer for arbeidet og viser til et problem som skal løses. Samtidig kan det kritiseres at det å «gjøre byene til bedre steder å leve, bo og arbeide i» er for abstrakt og kan nærmest åpne for hvilke som helst bruk av teknologi i byene. Det at Norge ikke har noen felles smart by strategi, kan gjøre at byer og kommuner ukritisk innfører teknologiske tiltak i et ønske å om å fremstå som ledende innenfor smart by. Dette kan medføre problemer hvor man innfører teknologiske tiltak for teknologien skyld og ikke vurderer om det faktisk løser noen av byens problemer. Dette kan samtidig medføre økt sårbarhet som vil bli diskutert videre i neste delkapittel.

Samtidig som Norge har en sterk økonomi og er i en god finansiell posisjon for å kunne innføre smarte tiltak beskriver D1 og D2 at topografien i Norge gjør det utfordrende og dyrt å bygge infrastruktur i Norge. Dette i kombinasjon med at D5 viser at i fremtiden vil det bli større grad av omprioriteringer og kutt i budsjettene som kan gjøre det mer utfordrende å få gjennomført smart by prosjekter. New public management (NPM) kan også være hinder for implementering av smart by arbeidet i Norge. Fokuset på kostnadsbesparelser og effektivisering kan gjøre det utfordrende å få gjennomført tiltak innenfor Smart by. Ved NPM påvirkningen er det også fare for at konkurranseutsettingen kan føre til at ikke de mest kvalifiserte får mulighet til å delta i prosjektene, og heller de som er billigst eller mest optimistisk som har vært en utfordring blant annet i digitaliseringsarbeidet. Dersom flere smart by prosjekter skulle feile vil antakelig tilliten til konseptet svekkes og det vil bli vanskeligere å kunne innføre større tiltak som mulig kunne hatt enda større påvirkning på samfunnsproblemer som klimaendringer eller forurensing.

Funnene viser at Norge er i en god posisjon med tanke på ekomtjenester og digitalisering. I tillegg til velutviklede Ekom infrastruktur, bor allerede hele 90 prosent av befolkningen i byer og byregioner i Norge (D2). Dette i kombinasjon til nordmenns sterke IKT-ferdigheter gjør at

byene er i god posisjon for smarte tiltak. I tillegg til dette er Norge i verdenstoppen av elektrifisering av nybilsalget (D1), elektriske kjøretøy og deres teknologi vil være med på å utvikle byen videre gjennom sensor og kommunikasjonsteknologi i bilene. Dette kan gjøre at man er bedre rustet til å møte noen av de slemme problemene som smart byen medbringer. Spesielt legger det til rette for deltakelse i smart byen, ved at de aller fleste har tilgang på høy kvalitets internettilgang og kompetanse om bruk av IKT. Ved at man allerede har så stor tilknytning til byene vil man få større nytte av de smarte tiltakene da byene vil dra nytte av stordriftsfordeler som igjen vil gi større samfunnsøkonomisk nytte samtidig som kostnadene blir lavere. Funnene viser videre at Norge i stor grad påvirkes av eksterne aktører i smart by utviklingen. Norges nærmeste handelspartner EU har flere tiltak som vil påvirke norsk transportsektor i årene fremover, og EØS-samarbeidet vil gi flere retningslinjer for norsk transportsektor og innføringen av ITS (D1).

Smart byer i Norge er fortsatt i sin begynnende fase (D7), byene som har best utgangspunkt for å innføre tiltak er kanskje de større byene i Norge. Store byer kan dra fordel av stordriftsfordeler med større markeder, flere leverandører og større tjenestetilbud (D2). Dessuten er det storbyene som har størst nytte av å forbedre transportløsninger for å redusere forurensning, bedre trafikkavvikling og sikkerhet. Store byer kan også stille større krav til tilbyderne av løsninger, som kan fremtvinge fokus på robuste løsninger. Store byer kan om de utnytter stordatateknologi få stor kunnskap billigere takket være stordriftsfordeler (dette kan også oppnås gjennom smartby klynger). Allikevel ser man i D7 at det er svært ulik størrelse på kommunene som arbeider med smart by. Det kan se ut til at smart by kan være en måte å gjøre byer eller kommuner mer attraktive, og at dette er motivasjonen for implementeringen. Smart by kan virke for noen byer i Norge å være en merkelapp som brukes politisk for å gjennomslag for sine prosjekter.

På nasjonalt nivå står det i D1 at tiltak skal gjennomføres nasjonalt og at investeringene skal komme alle veieiere til gode. Dette kan åpne for at enda fler kommuner og byer får kjennskap til smart by konseptet og kan drive frem utvikling og kunnskap på feltet. De fleste norske byer er for små til å investere i smart by på samme nivå som store byer i utlandet. Samarbeid mellom flere byer i smart by klynger kan være en løsning på denne utfordringen

Etttersom teknologien alltid utvikler seg, vil antakelig arbeidet med smart by vil aldri bli ansett som ferdig. Gammel teknologi utskiftes med ny over tid og man vil finne ny teknologi og løsninger i fremtiden. Benyttelsen av stordata kan bidra positivt i igangsettingen av

infrastruktur prosjekter, da de kan benytte for samling av stordata som kan bidra til økonomisk gevinst gjennom dataøkonomien. Et av problemene identifisert av Seidu (2018) var at infrastruktur var kronisk underfinansiert og at private aktører generelt er skeptiske til å investere i infrastrukturprosjekter etter som det historisk har gitt lav avkastning. Stordata kan bidra til å gjøre infrastrukturprosjekter mer økonomisk attraktive.

5.2 FS2: Hvordan påvirker smartby initiativer innenfor transport egenskapen resiliens hos Norske byer?

5.2.1 Evnen til å forutse

Ved å benytte teori på resiliens kan vi se hvordan resiliens i norske smarte byer blir tilrettelagt. Sett til Westrum (2006) sine tre aspekter av resiliens: Forutse, håndtere og gjenopprette kan vi undersøke hvor smarte byer er resiliente og hvor de har mangler. Den første delen av resiliens som handler om å forutse hvilke farer og trusler som kan treffe byen handler om evnen til å unngå at en hendelse inntreffer. Arbeidet med å identifisere hvilke trusler som kan inntreffe vil skje hos mange ulike aktører involvert i smart by arbeidet. I utgangspunktet er kommunene selvstendig forvaltningsnivå som innebærer at kommunene selv har ansvaret for ivaretagelse av egen digitalisering, digital sikkerhet og sikkerheten til innbyggerne innenfor fylkeskommunen (D4, D5). Denne oppgaven blir stadig mer komplisert, smart byen bringer mange utfordringer for å kunne forutse hendelsene.

Det at risikobildet blir mer komplisert bringer også utfordringer knyttet akseptabel risiko. Med utvikling av smart by og digitalisering kan det være utfordrende å få fullstendig oversikt over risikoen man faktisk tar. Smart by, IoT og IKT bringer store og kompliserte verdikjeder. Dette kan gjøre det utfordrende for beslutningstakere å kunne fatte informerte beslutninger. Dette gjelder også innbyggerne av byen som blir påvirket av valgene.

Når man implementer ny teknologi som smart by i prosjekter kan det være mer utfordrende å forutse hvilke trusler som kan inntreffe. Dette kan spesielt være utfordrende dersom man er tidlig ute med ny teknologi som ikke er særlig utprøvd fra før, da kan det tenkes at det oppstår hendelser som ikke var mulig forutse ettersom de aldri har inntruffet før. Her kan en løsning være å se til andre land som har kommet lengre i arbeidet for å unngå prosjekter som gir unødig høy risiko. Samtidig kan det å ikke gjøre noe påvirke risikoen negativt, samtidig som

teknologien utvikler seg får ondsinnede aktører nye virkemidler å utnytte. Eldre teknologi og infrastruktur er ofte mer sårbare enn ny ettersom de ble bygget i henhold til et annet trusselsituasjon og verdensbilde (D2).

For å forutse hvilke hendelser som kan inntreffe i smart by arbeid kan vi gjennom å se hvor mange ulike aktører som opererer i transportsektoren alene. I en storby som ønsker å investere i smarte initiativer innenfor transport vil fylkeskommunen ha ansvaret for fylkesveiene, som innebærer arbeidet med å planlegge, bygge, drifte og vedlikeholde fylkesveinettet samt har fylkeskommunen ansvaret for å organisere den regionale sivil transportberedskapen. Samtidig har statens vegvesen ansvaret for Europa- og riksveinettet. Gjennom EØS-samarbeidet får i tillegg statens vegvesen føringer fra EU sin side. (D4). Dette gjør at evnen til å forutse hendelser går på tvers av mange ulike nivåer. Det som gjøres på et nivå kan få betydning for de andre. Forebyggende tiltak og interesser kan se ulikt ut på de forskjellige nivåene, det kan derfor oppstå konflikt mellom tiltakene og hva som prioriteres som kan gjøre evnen til å forutse og forebygge hendelser lider.

Selv om det er mange ulike aktører som befinner seg i transportsektoren behøver ikke dette å hindre dem fra å skape en resilient sektor. Dersom det er enighet og samarbeid mellom aktørene involvert kan de dra nytte av hverandre for å sammen kunne identifisere de nødvendige tiltak for å sikre seg. Et problem særlig når det gjelder digital sikkerhet er at erfaringen har vist at den forebyggende digitale sikkerheten er begrenset i mange virksomheter. Alle private og offentlig virksomheter har ansvar for å vareta egen digital sikkerhet. Evnen til å forutse kan bli spesielt utfordrende for mindre byer og kommuner som har mindre tilgang på ressurser og kompetanse. Dette blir videre komplisert at tilbydere av Norges data strømmer gjennom utenlandskontrollerte nettverk, med infrastruktur som kan finne seg utenfor landegrensene med egne jurisdiksjon (D4).

Fokus på kostnadsbesparelse og effektivisering kan føre til at sårbarheten øker dersom det går på bekostning av sikkerheten. Ingen av prosjektene listet i D1 nevner samfunnssikkerhet eksplisitt. Tiltakene ser ut til å være til for å redusere kostnader, som i Augment city som er beskrivelsen en teknologi som gjøre det mulig for byplanleggere å erstatte tidkrevende papirbaserte prosesser. I dag er en utfordring at den tradisjonelle infrastrukturen i form av veinettet, vann og avløp er eid av det offentlige, mens de digitale infrastruktur er eid av det private. Det er en utfordring at Telenors transportnett bærer største delen av den totale elektroniske kommunikasjonen i Norge (D2). Outsourcing av digital infrastruktur gjør

prosjektene billigere, men samtidig blir det vanskeligere å holde oversikt over egne data, samtidig som man mister kompetansen om drifting av IKT systemer i Norge. Dette kan særlig være problem dersom man flytter driftingen av IKT systemer til land som kan ha mer slepphendt forhold til personvern eller har interesse av etterretning, eller er tett knyttet andre land som kan utgjøre en sikkerhetsrisiko.

Med alt dette tatt i betraktning kan det virke som Norske byer som ønsker å bli smarte vil møte store utfordringer med det å forutse hvilke hendelser som kan oppstå. Dette vil være på grunn av den store kompleksiteten og usikkerheten i risikobildet. Her bør norske smart byer legge til rette for stor grad av samordning og nøye utredning av verdikjedene i smart byen. Man bør sørge for at man finner måter å bevare kompetansen rundt IKT i landet for å kunne ha oversikt over prosessene. Dersom man benytter velprøvde teknologier kan det tenkes at evnen til å forutse styrkes.

5.2.2 Evnen til å håndtere

Evnen til å håndtere at en hendelse går fra vondt til verre er den neste evnen av resiliens som er viktig for smart byen. Selv om smart by ikke er utviklet for å forbedre samfunnssikkerheten så kan tiltak man iverksetter positivt bidra til å kunne håndtere hendelser. Siden smart by inneholder flere systemer kan den være resilient i en del av systemet, og mindre resilient i et annet. Det kan tenkes at i transportsektoren at evnen til å håndtere trusler knyttet fysisk resiliens vil kunne styrkes. Dette kan være i form av sensornettverk som gir informasjon om hendelser på veinettet, f.eks. ved informasjon ved trafikkulykker eller overvåking av infrastruktur som trenger vedlikehold.

I transportsektoren får man stadig flere kjøretøy som kan kommunisere med andre kjøretøy og infrastruktur rundt gjennom IoT. Dette kan benyttes til å gi informasjon om hendelser, eller strekninger som er spesielt utsatt. Her er det store muligheter for å utvinne stordata, men det oppstår også en utfordring knyttet personvern, hvem som eier dataen og om dette kan utnyttes av utenlands etterretning eller andre trussel aktører. Dette bringer også spørsmålet om cyber resiliens i transportsektoren. I fremtiden legges det opp til autonome selvkjørende kjøretøy, dette har fremdeles ikke blitt utbredt i stor grad, noe som kan gi fordel for hvor resilient trafikksektoren er i cyberdomenet. Ettersom kjøretøy fremdeles styres av mennesker, trenger ikke cyberangrep å få stor betydning for veinettet. Dersom internett blir slått ut av et cyberangrep fungerer fortsatt veinettet takket være redundans i systemet. Denne redundansen kan tenkes å forvitte f.eks. dersom autonome kjøretøy blir den dominerende transportmetoden

i fremtiden uten mulighet for overstyring og manuell kontrollering av kjøretøyet, her har vi et tydelig eksempel av de slemme problemene som følger med i smart byen. En annen utfordring kanskje nærmere i tid kan være overgangen til elektrifiserte kjøretøy. Samtidig som dette er positivt for å redusere klimagassutslippene, ender man med en større avhengighet på strømforsyningen. I dag er man både avhengig av fossile drivstoff og strømforsyning for å få transportsektoren til å gå rundt, dette skaper redundans i systemet og gjør at effektene av strømbrudd eller manglende tilgang på fossile drivstoff ikke gjør at hele transportsektoren stopper opp.

I dag kan det se ut til at smart by tiltak kan være med å styrke evnen til å håndtere hendelser og ikke gjøre de verre. Transportsektoren i dag har fordelene av redundans i systemene som gjør de resilient mot hendelser. Det kan se ut til at man møter på et av de slemme problemene over tid hvor elektrifiserte og autonome kjøretøy kan øke avhengigheten på tilgang på strømforsyning og internetttilgang. For å unngå at dette blir et problem bør beslutningstakerne legge til rette for andre måter å skape redundans på f.eks. ved andre typer drivstoff som hydrogenkjøretøy, eller gjennom å skape redundans i strømmettet og transportnettet for ekom.

5.2.3 Evnen til å gjenopprette

Hvordan evnen til å gjenopprette etter en hendelse blir i en smart by vil kunne avhenge av hvor hendelsen treffer, noen deler av smart byen kan antakelig være rask til å gjenopprette dersom det er slik man legger opp byen. Ansvar for å gjenopprette vil havne der hendelsen har skjedd. Dersom man legger opp smart byen med tette koblinger vil sannsynligheten være større for at evnen til å gjenopprette lider. Det er viktig når man innfører prosjekter at det gjøres vurderinger om hvor tett koblet sammen de ulike enhetene skal være. Dersom de kobles for nære øker risikoen for kaskade feil som kan føre til at systemet ikke klarer å gjenopprette normal funksjon innenfor en tilfredsstillende tidsramme.

Evnen til å gjenopprette i smarte byer virker nokså god i dag. Av samme grunner som evnen til å håndtere er transportsystemet nokså resilient mot hendelser i dag på grunn av at utviklingen av smart by innenfor transport ikke har kommet langt nok til å gi noen store avhengigheter. Smarte tiltak som sensornettverk for overvåking av veinettet kan antakelig bidra til å forbedre evnen til å gjenopprette. Med dette kan veieiere holde oversikt over hvilke strekninger som trenger vedlikehold, eller muligheten til å innhente mer informasjon om en trafikk-kollisjon eller andre hendelser som skaper forstyrrelse i transportsektoren.

6 Konklusjon

Studien viser at Norge er i en god posisjon for å kunne lykkes i innføringen av Smart by basert på Nordmenns kunnskap og kompetanse angående IKT-bruk, Norges økonomiske situasjon og befolkningens tillit til myndighetene. Smart by prosjekter kan derfor ses som en stor mulighet både økonomisk og samfunnsnyttig i Norge dersom den gjennomføres på en fornuftig måte.

Det første forskningsspørsmålet «*FS1: Hva er spesielt for Norge når man skal iverksette smart by initiativer?*» var ment til å utforske om det var spesielle forhold som la til rette for utvikling av smart prosjekter i Norge, og for å finne hvor aktuelt temaet var i Norge. Ut fra empirien og diskusjonen har jeg funnet at det norske smart by arbeidet er veldig i en oppstartsfase. De byer og kommuner som jobber med smart by gjør det veldig mye på eget initiativ, med unntak av byer som deltar i større forskningsprosjekter i regi av Norge selv, eller gjennom EU. Det norske smart by arbeidet ser ikke ut til å skille seg fra andre lands smart by arbeid og miljø og klimautfordringer er sentral motivasjon for å bli en smart by. Det er også funnet at Norge i stor grad vil bli påvirket av valg tatt av eksterne aktører både i form av andre nasjoner og organisasjoner.

Studien har funnet at det er sterke sammenhenger mellom digitaliseringsprosjekter og smart by prosjekter. Noe som understøtter det at mye arbeid går under smart by paraplyen uten at byen benytter definisjonen selv. Norge har ingen overordnet smart by strategi, dersom de ønsker denne utviklingen i flere norske byer bør det utvikles en felles strategi som angir retning og mål med tiltakene. Alle byer vil måtte ta valg knyttet når det kommer til utviklingen av egen by, og ingen kommer unna at de blir påvirket av den teknologiske utviklingen. Dersom Norge ønsker en samlet innsats mot et smartere samfunn blir de nødt til å ta stilling om det skal utvikles en felles strategi på nasjonalt nivå, dette kan bidra til at flere byer kan dra nytte av hverandres kunnskap og erfaringer, samtidig som man unngår at byer tar valg som kan få betydning for samfunnssikkerheten.

Det andre forskningsspørsmålet «*FS2: Hvordan påvirker smartby initiativer innenfor transport egenskapen resiliens i Norske byer?*» for å svare på dette forskningsspørsmålet benyttet jeg tre forskjellige aspekter ved resiliens for å se hvordan smart by arbeidet kunne påvirke dem. Her er det vanskelig å komme frem til noe konkret svar. En utfordring her er at det er få eksempler å se til og svaret er at det er avhengig av hvordan man iverksetter tiltakene. I denne oppgaven fant jeg at slik det har blitt arbeidet med smart by i dag hvor fokuset for mange tiltak virker å

være å effektivisere og gjøre prosesser mer kostnadseffektive kan man øke sårbarheten ved at man gjør det vanskeligere å forutse hvilke trusler som kan ramme byen. Dersom byer ønsker å kunne forsterke evnen til å kunne forutse hvilke trusler som kan ramme er de nødt til å kunne forstå hvordan tiltakene deres påvirker. Dette blir utfordrende når smarte tiltak bringer store og kompliserte verdikjeder som svekker beslutningstakernes evne til å fatte informerte beslutninger.

Evnen til å håndtere hendelser og gjenopprette etter en hendelse virker per i dag å være styrket gjennom smart by arbeid. Her må allikevel beslutningstakere være varsomme ettersom utviklingen av teknologi kan fjerne redundanser iboende i systemet i dag. For fremtiden gjelder det å finne andre måter å oppnå redundans for å kunne bevare den resiliente evnen.

For å besvare problemstilling «*Er fremtiden mer resilient eller mer sårbar med smarte byer i Norge?*» kan jeg ut ifra mine funn konkludere med at fremtiden kan bli mer resilient med smart byer i Norge dersom det blir lagt føringer og krav til byene. Det bør bli inkludert i smart by arbeidet krav og regulering som sørger for at de smarte byene ikke bytter bort sine resiliente evner mot kortvarig gevinst innenfor effektivisering og kostnadsbesparelser.

7 Litteraturliste

Al Nuaimi, E., Al Neyadi, H., Mohamed, N., & Al-Jaroodi, J. (2015). Applications of big data to smart cities. *Journal of Internet Services and Applications*, 6(1), 1-15. DOI 10.1186/s13174-015-0041-5

Asdal, K. & Reinertsen, H. (2021) *Hvordan gjøre dokumentanalyse – En praksisorientert metode*, Cappelen Damm Akademisk

Aven, T. (2015) *Risikostyring* (2. utg.). Universitetsforlaget

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

Aven, T. (2021). On Some Foundational Issues Concerning the Relationship Between Risk and Resilience. *Risk Analysis*.

Bjelle, S. L., & Sydnes, A. K. (2019). Auditing Industrial Safety Management: A Case Study. *International Journal of Management, Knowledge and Learning*, 8(1), 43-59.

Boin, A., Comfort, L. K., & Demchak C.C (2010) The rise of resilience. I A., Boin, , L. K., Comfort & C. C., Demchak (Red.) *Designing Resilience: Preparing for Extreme Events*. University of Pittsburgh Press

Bodø Kommune (2021 11. mai) *Smart-prosjektene vi jobber med* <https://nybybodo.no/smart-bodo/smart-prosjektene/> hentet 31.januar 2022

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*.

Caragliu, a., Del Bo, C. & Nijkamp, P. (2011) Smart Cities in Europe, *Journal of Urban Technology*, 18:2, 65-82, DOI: 10.1080/10630732.2011.601117

Carvalho, L. (2015). *Smart cities from scratch? A socio-technical perspective*. *Cambridge Journal of Regions, Economy and Society*, 8(1), 43-60.

Cedergren, A., Johansson, J., & Hassel, H. (2018). Challenges to critical infrastructure resilience in an institutionally fragmented setting. *Safety science*, 110, 51-58.

Cocchia, A. (2014). Smart and Digital City: A Systematic Literature Review. I Dameri, R. P & Rosenthal-Sabroux, C. (Red.), *Smart City – How to Create Public and Economic Value with High Technology in Urban Space*. Springer

Colding, J., Barthel, S., & Sörqvist, P. (2019). Wicked problems of smart cities. *Smart Cities*, 2(4), 512-521.

Dobbs, R., Smit, S., Remes, J., Manyika, J., Roxburgh, C., & Restrepo, A. (2011). Urban world: Mapping the economic power of cities. *McKinsey Global Institute*, 62.

Elzen, B., Geels, F. W., & Green, K. (Eds.). (2004). *System innovation and the transition to sustainability: theory, evidence and policy*. Edward Elgar Publishing.

Ejaz W. & Anpalagan A. (2019) Internet of Things for Smart Cities: Overview and Key Challenges. In: Internet of Things for Smart Cities. SpringerBriefs in Electrical and Computer Engineering. Springer, Cham. https://doi.org/10.1007/978-3-319-95037-2_1

Engen, O. A. H, Kruke, B. I, Lindøe, P. H., Olsen, K. H, Olsen, E. O, Pettersen, K. A (2016). *Perspektiver på samfunnssikkerhet*. Cappelen akademisk.

European Commission. (2020). 100 Climate-Neutral Cities by 2030 – by and for the Citizens: Interim Report of the Mission Board for Climate-Neutral and Smart Cities. Brussels, Belgium: General for Research and Innovation. doi:10.2777/62649

EU (2022) EU Mission: Climate-Neutral and Smart Cities

Fiksel, J. (2003). Designing resilient, sustainable systems. *Environmental science & technology*, 37(23), 5330-5339.

Giacometti, A., Teräs, J., Perjo, L., Wøien, M., Sigurjonsdottir, H., Rinne, T., ... & Rinne, T. (2018). *Regional economic and social resilience: Conceptual debate and implications for nordic regions*. Discussion paper prepared for Nordic thematic group for innovative and resilient regions.

Hafting, T. (2017) *Krisehåndtering: Planlegging og handling*. I T. Hafting (Red.), *Krisehåndtering: Planlegging og handling*. (s. 17-56)

Hall, J. (2019). A simulation tool to guide infrastructure decisions: system-of-systems modeling aids prioritization and uncertainty planning. *IEEE Systems, Man, and Cybernetics Magazine*, 5(3), 10-20.

Hall, R. E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H., & Von Wimmersperg, U. (2000). *The vision of a smart city* (No. BNL-67902; 04042). Brookhaven National Lab.(BNL), Upton, NY (United States).

Halvorsen, K. (2008) *Å forske på samfunnet: En innføring i samfunnsvitenskapelig metode* (5. utg.). Cappelen akademisk forlag

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J., & Williams, P. (2010). Foundations for smarter cities. *IBM Journal of research and development*, 54(4), 1-16

Hollnagel, E., Pariès, J., Wreathall, J (Red.). *Resilience Engineering in Practice A Guidebook*. Ashgate

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). *A review of definitions and measures of system resilience*. *Reliability Engineering & System Safety*, 145, 47-61.

Justis- og beredskapsdepartementet (2019) *Veileder til samfunnssikkerhetsinstruksen*

Lunde, I. K. (2014) *Praktisk krise- og beredskapsledelse*. Universitetsforlaget

Lynggaard, K. (2012) Dokumentanalyse. I S. Brinkmann & L. Tanggaard (Red.), *Kvalitative metoder – Empiri og teoriutvikling* (s. 153-170). Gyldendal

Johannessen, A., Tufte, P. A. & Kristoffersen, L. (2006) *Introduksjon til samfunnsvitenskapelig metode*. Abstrakt forlag

Julsrud, T. E., & Krogstad, J. R. (2020). Is there enough trust for the smart city? exploring acceptance for use of mobile phone data in oslo and tallinn. *Technological Forecasting and Social Change*, 161, 120314.

Kommunal- og moderniseringsdepartementet (2016). Kartlegging og vurdering av stordata i offentlig sektor. Kommunal- og moderniseringsdepartementet.

<https://www.regjeringen.no/no/dokumenter/kartlegging-og-vurdering-av-stordata-i-offentlig-sektor/id2478539/>

Kommunal- og moderniseringsdepartementet (2019). Smarte byer og kommuner i Norge – en kartlegging (R1020566) Kommunal- og moderniseringsdepartementet. https://www.regjeringen.no/contentassets/d6fa05005d5d4ea3a45f62286c2ba2fe/kartlegging_a_v_smarte_byer.pdf

Kopackova, H. & Libalova, P. "Smart city concept as socio-technical system," *2017 International Conference on Information and Digital Technologies (IDT)*, 2017, pp. 198-205, doi: 10.1109/DT.2017.8024297.

Kruke, B. I. (2017) Styre den som syre skal, eller kan: befolkningens rolle i beredskapsarbeid og i krisehåndtering. I T. Hafting (Red.). *Krisehåndtering: Planlegging og handling*. Fagbokforlaget

IoT-Analytics. The Top 10 IoT Segments in 2018—Based on 1600 Real IoT Projects; Technical Report; IoT-Analytics: Hamburg, Germany, 2018. Available online: <https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects> (accessed on 27. Januar 2022).

Iversen, A. B. (2011). 'Kvalitative og kvantitative metoder—et kontinuum?'. *Sosiologisk tidsskrift*, 19(02), 175-183.

Meld. St. 27 (2015-2016) *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet* Kommunal- og moderniseringsdepartementet.

Melt. St. 20 (2020-2021) *Nasjonal transportplan 2022-2033* Samferdselsdepartementet

Meld. St. 22 (2020-2021) *Data som ressurs – Datadrevet økonomi og innovasjon*

<https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/>

Monzon, A. (2015, May). Smart cities concept and challenges: Bases for the assessment of smart city projects. In 2015 international conference on smart cities and green, *ICT systems (SMARTGREENS)* (pp. 1-11). IEEE.

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

NOU 2000: 24. (2000). *Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Justis- og politidepartementet. <https://www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/>

Norris, F.H., Stevens, S.P., Pfefferbaum, B., Wyche, K.F. and Pfefferbaum, R.L. (2008), Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness. *American Journal of Community Psychology*, 41: 127-150. <https://doi.org/10.1007/s10464-007-9156-6>

SN-ISO Guide 73 (2009) *Risikostyring - Terminologi*

Parris (2020) Smart cities: locations for environmental entrepreneurship. I W J. Nuttall, D V. Gibson, D. Trzmielak & A. Ibarra-Yunez *Energy and mobility in Smart Cities* (31-59). ICE publishing

PST (2021) *Nasjonal trusselvurdering 2021*, Politiets sikkerhetstjeneste <https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/>

Rambøll (2018) *IT-i-praksis: Smarte og bærekraftige byer*. <https://www.ikt-norge.no/wp-content/uploads/2018/09/it-i-praksis-2018-smarte-og-brekraftige-byer.pdf> Rambøll

Richter, C., Kraus, S., & Syrjä, P. (2015). The Smart City as an opportunity for entrepreneurship. *International Journal of Entrepreneurial Venturing*, 7(3), 211-226.

Rose, A. and Liao, S.-Y. (2005), Modeling Regional Economic Resilience to Disasters: A Computable General Equilibrium Analysis of Water Service Disruptions. *Journal of Regional Science*, 45: 75-112. <https://doi.org/10.1111/j.0022-4146.2005.00365.x>

Rød, B., Lange, D., Theocharidou, M., & Pursiainen, C. (2020). From risk management to resilience management in critical infrastructure. *Journal of Management in Engineering*, 36(4), 04020039.

Sagiroglu, S., & Sinanc, D. (2013, May). Big data: A review. In 2013 *international conference on collaboration technologies and systems* (CTS) (pp. 42-47). IEEE.

Samih, H. (2019) Smart cities and internet of things, *Journal of Information Technology Case and Application Research*, 21:1, 3-12, DOI: 10.1080/15228053.2019.1587572

Silverman, D. (2013) *Doing Qualitative Research* (4.utg.). Sage

Smart Innovation Norway (2022, 31. januar) <https://www.smartinnovationnorway.com/>

Thagaard, T. (2013) *Systematikk og innlevelse – En innføring i kvalitativ metode* (4. utg.). Fagbokforlaget

Trondheim Kommune (2021, 8. april) *Trondheim blir smartby* <https://www.trondheim.kommune.no/trondheim-blir-smartby/> Hentet 31.januar 2022

UNEP (2018). *The Weight of Cities–Resource Requirements of Future Urbanization*. Paris: International Resource Panel Secretariat.

Van der Merwe, S. E., R. Biggs, and R. Preiser. 2018. A framework for conceptualizing and assessing the resilience of essential services produced by socio-technical systems. *Ecology and Society* 23(2):12. <https://doi.org/10.5751/ES-09623-230212>

Weick, K. E. & Sutcliffe, K. M. (2015). *Managing the unexpected – Sustained performance in a complex world* Wiley

Westrum, R. (2006) A Typology of Resilience Situations I E. H. Hollnagel, D. D. Woods & N. Leveson (Red.), *Resilience Engineering: Concepts and Precepts* Ashgate

Wood, L. Global Smart Cities Market Report 2020–2025: Analysis & Forecasts of Smart Transportation, Smart Buildings, Smart Utilities, Smart Citizen Services. 2020. Available online: <https://www.businesswire.com/news/home/20201008005413/en/Global-Smart-Cities-Market-Report-2020-2025-Analysis-Forecasts-of-Smart-Transportation-Smart-Buildings-Smart-UtilitiesSmart-Citizen-Services---ResearchAndMarkets.com> (accessed on 27. Jan 2021).

Wreathall (2006) Properties of Resilient Organizations: An Initial View I E. H. Hollnagel, D. D. Woods & N. Leveson (Red.), *Resilience Engineering: Concepts and Precepts* Ashgate

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine*, 55(1), 122-129.

