Karl Bjarne Kapaasen

Når tiden går i bane

Om samferdselssektorens avhengighet av nøyaktig tid fra GNSS, hvordan dette håndteres i transportetatenes sikkerhetsstyringssystemer og mulige konsekvenser for samfunnssikkerhet

Masteroppgave i organisasjon og ledelse - spesialisering i sikkerhet, pålitelig og vedlikehold

Januar 2021

Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Institutt for sosiologi og statsvitenskap

NTNU
Kunnskap for en bedre verden

Karl Bjarne Kapaasen

Når tiden går i bane

Om samferdselssektorens avhengighet av nøyaktig tid fra GNSS, hvordan dette håndteres i transportetatenes sikkerhetsstyringssystemer og mulige konsekvenser for samfunnssikkerhet

Masteroppgave i organisasjon og ledelse - spesialisering i sikkerhet, pålitelig og vedlikehold
Januar 2021

Norges teknisk-naturvitenskapelige universitet
Institutt for sosiologi og statsvitenskap

NTNU
Kunnskap for en bedre verden

Vi eier tiden, men tiden eier også oss

Henrik Ibsen, de unges forbund, 1869

Og i de dager skal det bli en stor kork. Alle biler skal stanse.

Tor Åge Bringsværd, Probok 1968

Det er bare en måte å bli trygg på: Vi må inngå samliv med fare. Vi må godta at det forferdelige kan skje. Hvis vi forventer null risiko og total beskyttelse, blir vi evig redde. Absolutt trygghet er umulig.

Per Fugelli, kronikk 2015

SAMMENDRAG

I en tid med omfattende digitalisering i samfunnet ser vi at satellittnavigasjonssystemer (GNSS) i stadig større grad brukes som kilde til nøyaktig tid og frekvens for å synkronisere digitale systemer. Dette gjelder også samferdselssektoren og dens betydning for samfunnssikkerhet. Ubevisst systemavhengighet gir potensiale for risiko og sårbarheter. Oppgaven går inn i grensesnittet mellom transport, samfunnssikkerhet og sikkerhetsstyring og setter fokus på avhengighet av GNSS som kilde til nøyaktig tid innen samferdselssektoren.

Innledningsvis forklares hva GNSS er, betydningen av PNT-begrepet og de mest sentrale kildene til forstyrrelse av GNSS-signalene. Videre relateres dette til digitaliseringsprosessen i samferdselssektoren, ITS og hvordan GNSS er en muliggjørende teknologi for denne utviklingen. Begrepene transport, samferdsel, mobilitet og transportsystem drøftes og sentrale aspekter ved sikkerhetsstyring og knytter det til samfunnssikkerhet. I dette ligger også hvordan ulike kunnskapssyn gir ulik tilnærming til risikobegrepet og hvordan svikt i GNSS kan gi kaskadeeffekt på kritiske samfunnsfunksjoner.

I oppgaven gjøres en dokumentstudie av stortingsmeldinger, NOU-er og andre offentlige publikasjoner relatert til samfunnssikkerhet. Fokus er satt på utviklingen i begreper, gjensidige avhengigheter i infrastrukturer, transport, satellittjenester og departementenes hovedansvar. Det er gjort en faktainnsamling vha. intervju av Samferdselsdepartementet (SD) og de største infrastruktureiende etatene/virksomhetene underlagt SD.

Oppgaven viser en omfattende digitalisering i samferdselssektoren. Dette krever kontinuerlig tilgang til nøyaktig tid. Alle informantene opplyser at de har en viktig funksjon for å fylle samferdselssektorens rolle inn mot samfunnssikkerhet og totalforsvar. Alle kritiske samfunnsfunksjoner er på en eller annen måte avhengig av transport. Det resulterer i en GNSS-avhengig samfunnssikkerhet. Dette håndteres ulikt i de ulike etatenes sikkerhetsstyring med ulik grad av bevissthet på tid og kilden til tid. Det skapes et inntrykk av nøyaktig tid som en usynlig ressurs mange er avhengig av, men som ikke får tilstrekkelig fokus fordi det ikke synes. GNSS som en kilde til nøyaktig tid fremstår som et eksempel på hvordan vellykkede teknologiske løsninger får stor anvendelse og derfor kan skape ubevisste avhengigheter og sårbarheter. Sammenhengen mellom IKT-sikkerhet, samfunnssikkerhet og etatenes sikkerhetsstyring kan komme tydeligere fram hos etatene/virksomhetene.

FORORD

«Den som tror han er ferdig utlært er ikke utlært, men ferdig», skal en ha sagt en gang. Verden endrer seg raskt og det er viktig å lære seg nye ting. Det er kanskje særlig viktig når man har innsett at man er inne i andre halvdel av yrkeslivet. Vi kan lære noe hver dag, men det er flott å kunne få gjøre et kunnskapsløft for seg selv som et masterprogram innebærer.

Denne teksten er levert som masteroppgave i NTNU Videres masterprogram i organisasjon og ledelse med spesialisering sikkerhet, pålitelighet og vedlikehold. Oppgaven markerer avslutningen på en fireårsperiode som student på fritiden. Det har vært lærerikt, morsomt, nyttig og tidvis krevende. Det har vært inspirerende å møte medstudenter på samlingene og dele erfaringer fra vidt forskjellige hverdager.

Sist gang jeg leverte et arbeid av dette omfanget ved NTNU var da jeg gikk ut av sivilingeniørstudiet i 1996. Da skulle hovedoppgaven trykkes og leveres fysisk i riktig antall. Denne oppgaven er levert elektronisk og studentbeviset har blitt en app. All dialog mellom universitet og student, og alt som skal deles ut eller leveres inn, skjer digitalt. Veiledning foregår på videokonferanse. Digitaliseringen skjer i hele samfunnet og er også en del av temaet for denne oppgaven.

Jeg vil gjerne takke professor Petter Grytten Almklov ved institutt for sosiologi og statsvitenskap ved NTNU for god veiledning underveis. Han har vært lett tilgjengelig med gode råd om litteratur og metode, gitt rask respons på spørsmål og anbefalt nyttig justering av kurs for å unngå grunnstøting.

Jeg vil også takke min arbeidsgiver Norsk Romsenter, og avdelingsdirektør Steinar Thomsen ved satellittnavigasjonsavdelingen, for velvillighet og støtte slik at det ble mulig for meg å gjennomføre dette masterprogrammet.

Sist, men ikke minst, en stor takk til Barbro som har holdt ut med at arbeidet med oppgaven har kommet høyt på prioriteringslista de siste månedene.

Karl Bjarne Kapaasen
Fjellhamar, 29. januar 2021

INNHOLD

1. INNLEDNING

1.1 Bakgrunn

«We are witnessing nothing less than a revolution in transport». Slik lyder første setning i sammendraget i rapporten The Future of Road Transport fra EUs forskningsinstitutt JRC (JRC, 2019).

Revolusjonen det er snakk om er digitaliseringen av samferdselssektoren. Dette er en spennende og morsom utvikling som påvirker samfunnsutviklingen generelt og byutviklingen spesielt. Det er også en prosess som kan gjøre alle former for transport avhengig av nøyaktig tid. Nøyaktig tid hentes veldig ofte fra satellittnavigasjonssystemer (GNSS). Transport er definert som en kritisk samfunnsfunksjon av Direktoratet for samfunnssikkerhet og beredskap (DSB) og som en grunnleggende nasjonal funksjon (GNF)[1] av Samferdselsdepartementet (SD). Digitaliseringen gjør at hele sektoren kan bli avhengig av GNSS som ligger utenfor transportaktørenes kontroll. Hva skjer da om tilgangen til GNSS reduseres eller faller bort? En slik hendelse vil kunne påvirke hele transportsystemet og ha negativ effekt på samfunnssikkerheten ettersom den er avhengig av fungerende transport.

Utviklingen de senere årene har gjort det mulig å lage kraftige datamaskiner som er små og billige. Miniatyriseringen gjør at stor datakraft kan bygges inn i «alt» vi omgir oss med og som gjør det mulig for tingene å kommunisere gjennom en stadig raskere digital kommunikasjonsinfrastruktur, tingenes internett.

For samferdselssektoren får dette utslag som f.eks. digitale sikkerhetskritiske systemer, autonome skip, selvkjørende biler og at bilen din alltid er «koblet opp». Men kanskje viktigst er hvordan alt kommunisere med alt og danner et digitalt hele for informasjonsutveksling. Gjennom intelligente transportsystemer (ITS) og 4G/5G-nett kan biler kommunisere med veiinfrastrukturen og med hverandre. Informasjon som oppstår ett sted kan raskt utnyttes et annet sted for å gjøre trafikken mer effektiv og sikker. Smarttelefoner er for lengst blitt vanlig og vi kan bruke dem for å finne ut hvor vi er, om toget er i rute, låse opp en el-sparkesykkel,

[1] SD har definert GNF-er for sitt ansvarsområde iht den nye sikkerhetsloven fra januar 2019. Oversikt over departementenes GNF-er pr. høsten 2020 finnes i St. Prop 1 (2020-2021) for Justisdepartementet (tab. 2-9).

finne hvor det er bilkø, bestille en delt bilressurs eller sjekke inn på flyet. I stedet for at den reisende må tilpasse seg transportløsningene blir transportløsningene fleksible for å tilpasse seg den reisende. Transport og IKT forenes for å finne nye, effektive og miljøvennlige løsninger på samferdselsutfordringer samtidig som vi ser en stadig økende elektrifisering av framkomstmidlene.

Baksiden av digitaliseringsmedaljen er sårbarheten som følger med, ikke minst i sammenhenger der digitalisering har grensesnitt mot samfunnssikkerhet. Digitale systemer og enheter i digitale kommunikasjonsnett må synkroniseres for å fungere sammen. Tilgang på tid og frekvens blir avgjørende og dette hentes veldig ofte fra GNSS fordi det er tilgjengelig, pålitelig, nøyaktig og ikke minst, gratis.

I denne oppgaven ønsker jeg å gå inn i problematikken rundt hva denne utviklingen kan bety for måten det jobbes med risiko og sikkerhet innen samferdsel. Mye av det jeg kommer inn på vil være relevant for GNSS relatert til posisjonsbestemmelse og navigasjon, men jeg ønsker i stedet å sette fokuset på bruken av nøyaktig tid. Nøyaktig tid har blitt den usynlige ressursen som mange er helt avhengig av uten å være klar over det, og uten å vite hvor den kommer fra. Jeg ønsker å undersøke hvordan samferdselssektoren har gjort seg avhengig av en tidskilde utenfor sin kontroll og hvordan dette eventuelt fanges opp i aktørenes sikkerhetsstyring i samfunnskritiske sammenhenger. Jeg har derfor valgt følgende problemstilling:

1.2 Problemstilling

I hvilken grad utgjør avhengigheten av nøyaktig tid fra GNSS en sårbarhet for en digitalisert transportsektors betydning for samfunnssikkerheten? Dette blir belyst gjennom å gå inn i spørsmålene:

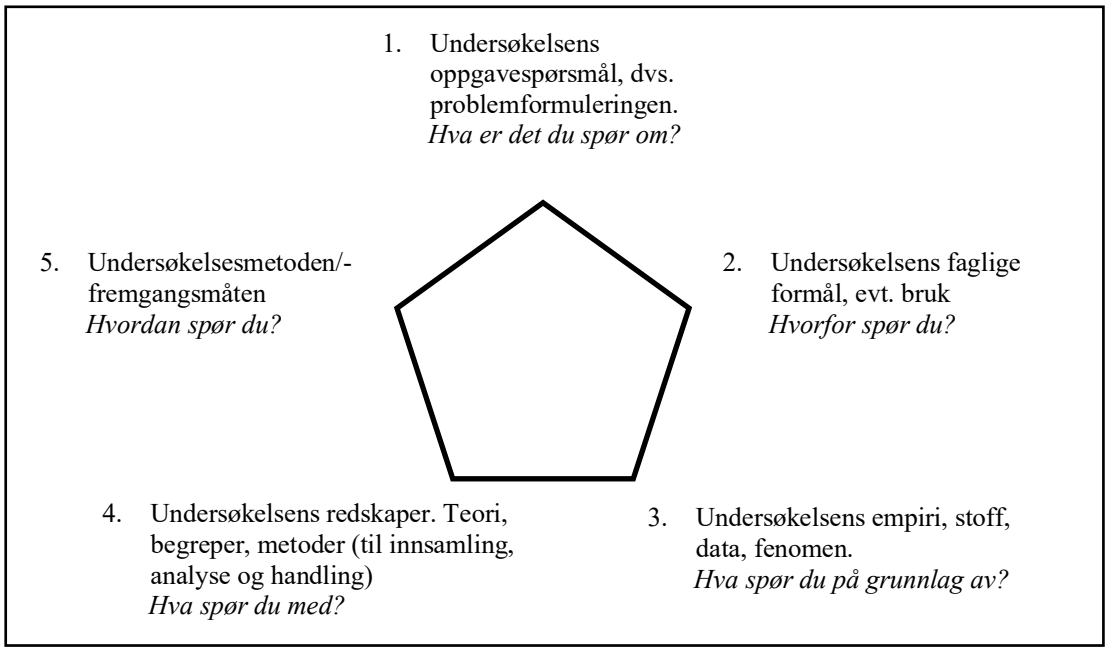
1. *Hva menes med en GNSS-avhengig digitalisert transportsektor*
2. *Hva er transportsektorens rolle inn mot samfunnssikkerhet og hvordan påvirker GNSS-avhengigheten dette?*
3. *Hvordan håndterer transportetatene i sine risiko-/sikkerhetsstyringssystemer at de er avhengig av GNSS som ligger utenfor dere kontroll*
4. *Hva er SDs rolle for å sikre bruken av nøyaktig tid i en digitalisert transportsektor*

2. FORSKNINGSDESIGN OG STRUKTUR PÅ OPPGAVEN

Valg av forskningsdesign innebærer å velge hva og hvem som skal undersøkes og hvordan undersøkelsen skal gjennomføres. Forskningsdesign er «alt» som knytter seg til en undersøkelse (Johannessen et al., 2016). Dette kalles design fordi det er med på å gi oppgaven form. Designet gjøres ved å ta utgangspunkt i problemstillingen og vurdere hvordan det er mulig å gjennomføre undersøkelsen fra start til mål. For å bygge opp en struktur på oppgaven og samtidig komme fram til et relevant forskningsdesign, har jeg valgt å bruke pentagonmodellen. I dette kapittelet besvares modellens tre første spørsmål, mens de to siste besvares i metodekapittelet.

2.1. Pentagonmodellen – spørsmål 1, 2 og 3

Basert på anbefalinger gitt på NTNUs oppstartskurs for masteroppgaveskriving, har jeg valgt å bruke pentagonmodellen (Rienecker et al., 2013) i planleggingen av oppgaven. Den legger opp til at den som skriver må ta stilling til fem spørsmål for å danne den strukturen i oppgaven som en vitenskapelig undersøkelse skal ha. Det er vist på fig. 1:



Figur 1: Pentagonmodellen. (kilde: Rienecker mfl.)

2.1.1. Hva er det du spør om?

Jeg ønsker å lage en undersøkende tekst der temaet ligger i grenseland mellom samfunns-sikkerhet, samferdsel og bruk av satellittnavigasjon (GNSS). GNSS har mange anvendelses-

områder og transportsektoren er største bruker av slike systemer. Dette gir mange fordeler, men også mulige sårbarheter knyttet til systemavhengighet som kan være ubevisst. GNSS brukes av mange som kilde til nøyaktig tid og frekvens for å synkronisere digitale systemer og tidfeste hendelser. Dette gjelder også transport og forhold knyttet til samfunnssikkerhet. Jeg ønsker å gå inn i problematikken rundt hvordan dette håndteres risikostyringsmessig i samferdselssektoren.

2.1.2. Oppgavens formål/Hvorfor spør du?

Oppgavens formål er å forsøke å belyse hvordan en digitalisert samferdselssektor har gjort seg avhengig av satellittjenester som ligger utenfor sektorens kontroll, og deretter undersøke hvordan dette gjenspeiles i risikostyringen hos sentrale aktører i sektoren.

Min forventing til funn er at bevisstheten rundt satellittavhengigheten er varierende og at den til dels er lav. Dette er interessant fordi det fra industriens og myndighetenes side gis uttrykk for at økt grad av digitalisering er en ønsket utvikling. Det forventes økt effektivitet, forbedret sikkerhet og positive miljøeffekter. Jeg håper at funn som gjøres skal gi mulighet for å foreslå tiltak eller skissere muligheter for videre arbeid.

Ønskede effekter av digitalisert samferdsel oppnås gjerne på tvers av transportformene der verdikjeder gjør seg gjeldene. Derfor vil også effekten av risikofaktorer kunne gå på tvers av disse grensene.

2.1.3. Empiri/Hva spør du på grunnlag av?

Temaet og problematikken kommer fram i en rekke offentlig dokumenter de senere årene. For å finne ut mer vil jeg søke i faglitteraturen etter bøker/artikler/teorier som belyser hva som menes med samfunnssikkerhet, digital samferdsel og sikkerhetsstyring. Litteratursøk vil bli gjort gjennom de tilganger som tilbys studentene på NTNU VPN. Det vil være relevant å gi inn i teorier rundt kompleksiteten i moderne samfunn, ulykkesmodeller og hvordan ting henger sammen i verdikjeder. Jeg ønsker å se på relevante stortingsmeldinger, NOU-er, statlige strategier og rapporter som er gitt ut de siste årene. Det kan også være EU-dokumenter som gir verdi.

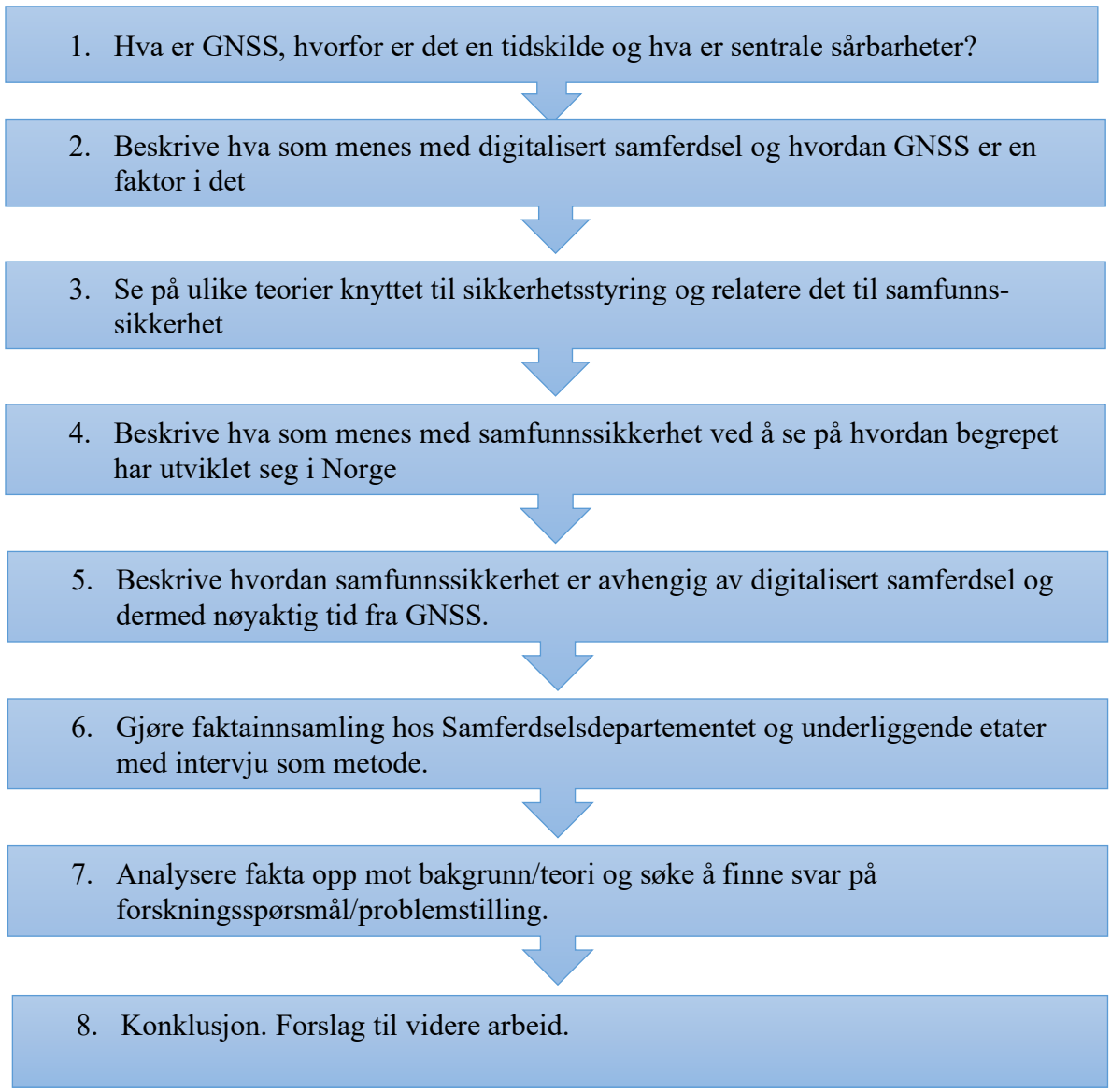
Hensikten med å gå inn i disse dokumentene er å se på hvilke strategier, styringssignaler og føringer som er gitt innenfor området problemstillingen dekker. Disse dokumentene kan også danne et bilde av hvordan synet på samfunnssikkerhet og tilhørende begrepsapparat har utviklet seg. Jeg har også med meg de erfaringer jeg har gjort gjennom å ha jobbet med risiko/sikkerhet innen samferdsel generelt og luftfart spesielt.

2.2. Avgrensning

Oppgaven går inn på begrepet samfunnssikkerhet som er begrep det kan legges ulike ting i. Her vil jeg avgrense betydningen til å relatere det til transport som kritisk samfunnsfunksjon. Jeg avgrenser også faktainnsamlingen til å gjelde Samferdselsdepartementet (SD) og de etatene/virksomhetene som har ansvar for forvaltning av nasjonal infrastruktur. Det gir en aktør for hver transportform pluss SD som har overordnet ansvar.

2.3. Oppgavens struktur

Basert på ovenstående gir jeg oppgaven følgende struktur:



Figur 2: Oppgavens struktur

2.4. Forkortelser og akronymer

Oppgaven inneholder en del forkortelser og akronymer. Disse er forklart første gang de benyttes og er samlet i en oversikt i vedlegg 2.

3. GNSS, NØYAKTIG TID OG SÅRBARHETER

I veldig mange sammenhenger er det GNSS (Global Navigation Satellite Systems) som brukes som kilde til nøyaktig tid og frekvens. Selv om dette ikke er en masteroppgave i et teknisk fag så handler det om samvirke mellom teknologi og samfunn, bevisst og ubevisst. Det er relevant for forståelsen av det jeg skriver lenger ut i oppgaven å innledningsvis gå litt inn på disse systemenes virkemåte. I dette kapitlet vil jeg beskrive hva GNSS er, hvordan GNSS kan gi nøyaktig tid relatert til tidsskalaen UTC (Universal Time Coordinated) og hvilke sårbarheter som er mest sentrale. Jeg vil også forklare begrepet PNT (Posisjonsbestemmelse, Navigasjon og Tidsbestemmelse) som ofte benyttes i sammenheng med GNSS.

3.1. GPS, GLONASS, Galileo og BeiDou

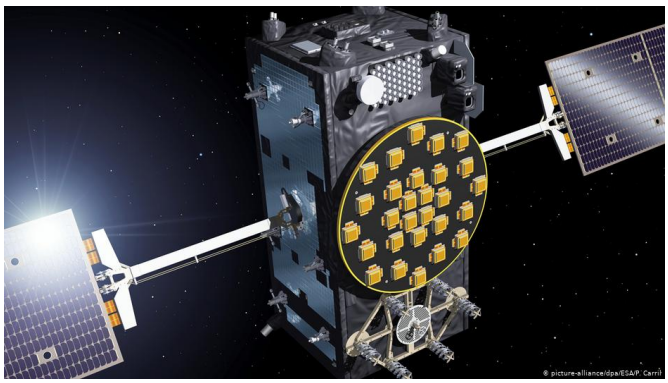
Tidsmåling og navigasjon henger tett sammen. Utviklingen innen urverk har vært drevet av et ønske om stadig bedre nøyaktighet og stabilitet. Etterspørselen etter dette har i stor grad vært drevet av behov innen navigasjon, ikke minst tidligere tiders utfordring ved å bestemme lengdegrad til sjøs uten land i sikte. Løsningen ble etter hvert fjærdrevet kronometer der engelskmannen John Harrison[2] (1693-1776) og franskmannen Pierre Le Roy[3] (1717-1785) har fått sine velfortjente plasser i historien. Teknologien har utviklet seg videre via kvartsur til atomur som i dag er en forutsetning for den nøyaktigheten i posisjonsbestemmelse som kreves innen satellittnavigasjon.

Den tekniske utviklingen innenfor radionavigasjon har brakt oss fra bakkebaserte systemer til satellittbaserte systemer. Det første systemet som ga global dekning hele døgnet, var GPS (Global Positioning System) som ble erklært operativt i 1995. Dette er et amerikansk militært system som driftes av det amerikanske forsvaret. Sivile brukere fikk tilgang til systemet fra starten av, men den gang med en degradering av ytelsen kalt Selective Availiability. Begrensningen på posisjonsbestemmelse ble satt til bedre enn 100m i 95% av tiden. Denne degraderingen ble fjernet allerede for 20 år siden, noe som har bidratt sterkt til den omfattende sivile anvendelsen av GPS vi ser i dag.

[2] https://no.wikipedia.org/wiki/John_Harrison (besøkt 2020-09-13)
[3] https://en.wikipedia.org/wiki/Pierre_Le_Roy (besøkt 2020-09-13)

Omtrent samtidig som USA erklærte GPS for operativt, kom Sovjetunionen med sitt tilsvarende system, GLONASS. I de senere årene har Kina og Europa også bygget sine globale satellittnavigasjonssystemer. Det kinesiske systemet heter BeiDou og ble fullt operativt i 2020. Det europeiske systemet, Galileo, har vært operativt med begrensninger (Initial Services) siden desember 2016 og forventes fullt operativt i løpet av 2020/2021. GNSS er en fellesbetegnelse for disse fire globale satellittnavigasjonssystemene.

Galileo skiller seg ut fra de tre andre GNSS-ene ved at det er et sivilt system under kontroll av sivile myndigheter. Det har ikke tjenester reservert for militær bruk slik de andre har. Systemet er utviklet av ESA[4], eies av EU og er bygget av europeisk industri. Norge, som EØS-medlem, deltar i Galileo-programmet og norsk industri har hatt flere leveranser til satellittene.



Figur 3: Galileosatellitt (kilde: ESA)

Et GNSS deles gjerne inn i tre segmenter. Det første er bakkesegmentet som er infrastruktur på bakken for å kontrollere satellittene og dataene de sender ut. Det andre er romsegmentet som består av alle satellittene. Det tredje er brukersegmentet som er summen av alle mottakerne innen alle anvendelsesområder.

3.2. Vi er alle navigatører

Utviklingen har gjort at navigasjon har endret seg fra å være noe navigatører holder på med på skip eller i fly, til noe som alle holder på med i hverdagen. Det sitter GNSS-mottakere i alle smarttelefoner og etter hvert har også svært mange en eller flere GNSS-mottakere i bilen. Hvis man f.eks. kjøper en ny Iphone vil den ha en multi-GNSS-mottaker innebygget. Det vil si at den benytter satellitter fra flere GNSS samtidig for å regne ut posisjonen. Telefonen bruker GPS, GLONASS og Galileo om hverandre uten at brukeren trenger å tenke på det. Denne allmenngjøringen av satellittbruk har fjernet noe av bevisstheten rundt bruken. Mange er ikke klar over at plasseringen av «den blå prikken» på det digitale kartet er regnet ut ved hjelp av

[4] Den europeiske romfartsorganisasjonen. European Space Agency

satellittsignaler og at de som brukere av mobiltelefoner er avhengig av romteknologi. Ubevisstheten rundt bruk og avhengighet av GNSS kan være en faktor med betydning for sårbarhet. I vaskeseddelen på boken Navigation (Hofmann-Wellenhof et al., 2003) kan vi lese: «Today, everybody is concerned with navigation, even if unaware of this fact».

En konsekvens av dette er at GPS i realiteten har fått utvidet betydning fra å være navnet på et bestemt GNSS til å bli et generelt uttrykk som benyttes synonymt med GNSS. Mange kjenner ikke begrepet GNSS, men «alle» har hørt om GPS. Folk snakker om «GPS-en i bilen» uavhengig av om de mener GPS, et av de andre GNSS-ene, det digitale kartet på skjermen eller algoritmene fra Google som finner raskeste vei fra A til B[5].

3.3. Betydningen av nøyaktig tid

For å bruke GNSS må man ha en mottaker som regner ut sin posisjon når den mottar radiosignaler fra minst fire satellitter. Denne utregningen er basert på nøyaktig tidsmåling. Mottakeren regner ut hvor langt unna den er fra satellitten ved å måle tiden radiosignalet har brukt på sin vei fra satellitten til mottakeren. Basert på disse avstandsmålingene regner mottakeren ut sin posisjon i lengdegrad, breddegrad og høyde. For mange bruksområder vil dette så bli vist i et digitalt kart. For å oppnå tilstrekkelig god tidsmåling er derfor alle GNSS-satellitter utstyrt med atomklokker og satellittnavigasjonssystemet har en systemtid med kjent avvik fra tidsskalaen UTC.

Utbygging av GNSS har altså medført at det er plassert et betydelig antall atomklokker i verdensrommet som sender ut tidsinformasjon med global dekning. Det gjør at GNSS kan betraktes som en klokke i verdensrommet. GNSS er en verdensomspennende kilde til nøyaktig tid og frekvens, med svært god tilgjengelighet og som i tillegg er gratis å bruke. Det medfører at det er mange brukere av GNSS som kun er ute etter tid og frekvens, og som ikke nødvendigvis er interessert i hva GNSS kan tilby innenfor posisjonsbestemmelse og navigasjon. Produsentene av GNSS-mottakere lager egne tidsmottakere for dette formålet.

[5] Et godt eksempel på denne sammenblandingen var å finne på NRKs nyhetsside i januar 2021: https://www.nrk.no/innlandet/gps-villeiar-bilistar-ut-i-skiloypa-1.15291785 (besøkt 2021-01-09)

3.3.1 Tidsskalaer og systemtid

Et tidspunkt må relateres til en tidsskala å for å gi mening. For å samkjøre en stadig «mindre» verden tidsmessig ble det i 1884 besluttet å dele verden inn i 24 tidssoner med bredde tilsvarende 15 lengdegrader (360/24 = 15). Utgangspunktet var nullmeridianen gjennom Greenwich-observatoriet utenfor London. Når solen står på sitt høyeste her er klokken 12:00:00 GMT – Greenwich Mean Time. Klokken skulle så stilles en time tilbake for hver tidssone vestover og en time fram for hver tidssone østover.

GMT som tidsskala, og definisjonen av sekundet[6], ble på dette måten bundet til jordens rotasjon. Med stadig større krav til nøyaktig tid ble dette etter hvert ikke godt nok. I 1967 ble sekundet frikoplet fra jordrotasjonen ved i stedet å relatere det til energinivåene i Cesiumatomet (^{133}Cs). Sekundet er nå definert som varigheten av 9 192 631 770 bølgelengder fra strålingen tilsvarende energiforskjellen mellom to hyperfine nivåer i Cs-atomet. Dette er utgangspunktet for tidsskalaen TAI - International Atomic Time (atomtid). TAI beregnes av det internasjonale byrået for mål og vekt (BIPM) som et vektet gjennomsnitt mellom ca. 400 atomklokker over hele verden. Den største bidragsyteren er amerikanske United States Naval Observatory (USNO). Tidslaboratoriet hos Justervesenet (JV) på Kjeller bidrar også med sine atomklokker.

GMT som tidsskala gikk ut av bruk i 1972 og ble erstattet med skalaen UT1 – Universal Time (universaltid). UT1 er bundet til jordrotasjonen. Ettersom TAI er frikoplet fra jordrotasjonen kan TAI og UT1 over tid avvike en del fra hverandre. TAI og UT1 koordineres derfor til tidsskalaen UTC – Universal Time Coordinated (koordinert universaltid) – hovedsakelig ved bruk av skuddsekunder.

Et GNSS må ha en innebygget tidsskala, en systemtid, for å fungere. Systemtiden i et GNSS holdes innenfor et kjent avvik fra UTC. Nytten ved å relatere systemtiden til UTC ligger i at GNSS da kan brukes som tidskilde for anvendelser utenfor systemet og å relatere systemtidene i de ulike GNSS-ene til en felles tidsskala.

[6] Ett sekund = det gjennomsnittlige tidsrommet mellom to påfølgende ganger der solen står på sitt høyeste over nullmeridianen (et gjennomsnittlig soldøgn) dividert på 86400. (86400 = 24 * 60 * 60)

3.4. PNT

Det er relevant i dette kapitlet å forklare PNT-begrepet ettersom det brukes i mange sammenhenger der GNSS omtales, og brukes i flere norske offentlige publikasjoner relatert til samfunnssikkerhet.

Som omtalt over har utviklingen gått i en retning der radionavigasjon nå er nær synonymt med satellittnavigasjon. Tidligere fantes de langtrekkende bakkebaserte systemene[7], Omega, Decca og Loran-C, men disse er i praksis borte. Det finnes fortsatt en omfattende infrastruktur av bakkebaserte systemer for luftfart, men disse betraktes i stadig større grad som overflødige til fordel for GNSS. GNSS har i tillegg gjort navigasjon på land svært aktuelt. Vi ser f.eks. GNSS-mottakere i treningsklokker, mobiltelefoner, kjøretøy og landbruksmaskiner. Hos nødetatene ser vi flåtestyring av utrykningskjøretøy og det brukes trygghetsalarmer som viser posisjon. Innen veitrafikk ser vi GNSS-basert nødvarsling (eCall[8]), satellittbasert veiprising og intelligente trafikksystemer. Innen elkraft og tele-/data-kommunikasjon ser vi synkronisering av nett og datatrafikk.

Anvendelsen av GNSS dekker nå så mye mer enn bare navigasjon og derfor har begrepet PNT blitt vanlig. Det kommer fra engelsk og står for positioning, navigation and timing. På norsk oversettes det til posisjonsbestemmelse, navigasjon og tidsbestemmelse. PNT-systemer kan fortelle oss hvor vi er og når vi er der og de kan brukes til tidssynkronisering. Dette er ikke nødvendigvis GNSS. Det skilles mellom bakkebaserte og satellittbaserte PNT-systemer. I praksis er det veldig ofte snakk om GNSS, og spesielt GPS.

I november 2018 ga Samferdselsdepartementet (SD) ut en nasjonal PNT-strategi for Norge (SD, 2018b). Den setter fokus på utviklingen innen anvendelse av PNT-systemer og bevisstgjøring rundt avhengigheter og sårbarheter som konsekvens av dette.

[7] Bakkebaserte systemer vil i denne sammenhengen si systemer for radionavigasjon der radiosignalene kommer fra stasjoner på bakken i stedet fra satellitter.
[8] https://www.dsb.no/lover/brannvern-brannvesen-nodnett/artikler/ecall-varsling-av-trafikkulykker/ (besøkt 2021-01-18)

3.5. Feilkilder og sårbarhet

Det er en rekke forhold som kan påvirke nøyaktigheten i, og tilgangen til, GNSS-tjenestene. Det skilles vanligvis mellom utilsiktede og tilsiktede forhold, og mellom naturlige og menneskeskapte forhold.

Avgjørende for satellittenes funksjonalitet er atomklokkene om bord. Disse vil kunne drifte og gi unøyaktigheter over tid. Ettersom satellittene beveger seg svært raskt relativt til jorden, og i et gravitasjonsfelt som er mye svakere enn nede på jorden, vil relativistiske effekter gjøre seg gjeldende. Det betyr at klokkene i satellittene og klokkene ned på jorden ikke går med samme hastighet. Det vil også være differanser mellom satellittenes ideelle og reelle baner.

Satellittene vil kunne skades av romskrot. Dette er utrangerte satellitter, rester fra bæreraketter og andre fragmenter. Problemet er større i lavere baner enn de banene som GNSS-satellittene er plassert i. Dette er menneskeskapt og utilsiktet.

Både satellittene og satellittsignalene vil være utsatt for romvær. Dette er naturlig og utilsiktet og skyldes solaktivitet. Utbrudd på solen slynger ut elektrisk ladede partikler og kraftige elektromagnetiske felt som påvirker radiosignalene, men som i verste fall kan ødelegge satellittene fysisk. Kraftig romvær påvirker ionosfæren og kan gi vakkert nordlys, men har potensiale til å forstyrre satellittsignalet og ødelegge elektronikk og elektriske installasjoner nede på jordoverflaten.

Radiosignalet fra satellitten kan forstyrres av andre signaler fra andre menneskeskapte systemer. Dette kan være utilsiktet ved at det skjer ubevisst eller ved en feil, eller bevisst ved at noen sender ut radiosignaler som er ment å skape forstyrrelser. Det sistnevnte deles gjerne inn i kategoriene støysending (jamming), utsendelse av falske signaler (spoofing) eller retransmisjon av et forsinket signal (meaconing).

De siste par årene har jamming blitt aktualisert i nyhetsbildet her i Norge. Små jammere kjøpes billig på nett og disse kan gjøre mer skade enn brukeren ofte er klar over. Dette har bl.a. skapt store problemer for Luftambulansen (VG, 2019). Kraftige jammesystemer for militært formål er også benyttet mot Norge de siste årene. Nasjonal kommunikasjonsmyndighet (Nkom) skriver i sin årlige rapport EkomROS for 2019 (Nkom, 2019), at det gjennom 2017, 2018 og 2019 er

registrert forstyrrelser av GPS-signalene som har vært en trussel for luftfarten i Nord-Norge generelt og Øst-Finnmark spesielt. Ved hjelp av nye peilestasjoner i Finnmark har Nkom kunnet lokalisere støykilden til områder i Russland i noen av disse tilfellen. Dette er menneskeskapt og tilsiktet.

Satellittsignaler ligger i et frekvensområde som lett lar seg stoppe av fysiske hindringer mellom sender og mottaker. Slik kan bygninger og høyder i terrenget skjerme for signalet. Det er særlig aktuelt når satellittene står lavt på himmelen sett fra mottakeren. For GNSS gjør dette seg mer gjeldende på høye breddegrader, som her i Norge. I urbane strøk med høye hus vil bygningene påvirke slik at satellittsignalene blir reflektert eller skjermet så de ikke når ned til gatenivået der de skal brukes. Dette kalles gjerne «urban canyons» - på norsk byjuv – og er menneskeskapt og utilsiktet.

Et annet menneskeskapt og utilsiktet forhold er feil bruk av mottakeren. Det kan være at det gjøres feil på grunn av manglende kunnskap om utstyret, uforsiktighet, batteriet er oppbrukt, brudd på rutiner eller for liten innsikt i navigasjonsteknologi og hvordan GNSS fungerer.

Bakkesegmentet og driftsorganisasjonen er der for å sikre at systemet leverer den tjeneste-kvaliteten det skal, men feil kan oppstå også her. Det finnes eksempler på at operatørfeil har påvirket systemene negativt. Sommeren 2019 gikk Galileo av lufta en ukes tid på grunn av flere utilsiktede sammenfallende hendelser i bakkesegmentet. Teknisk redundans og driftsorganisasjonens kompetanse, prosedyrer og kvalitetsstyringssystem er viktig for tjenestekvaliteten.

3.5.1 Mulige tiltak

Myndigheter, systemeiere og brukergrupper av GNSS kan arbeide med ulike typer tiltak for å motvirke forhold som nevnt over. Dette følger gjerne PTA-prinsippet – Protect, Toughen, Augment (Theunissen, 2014).

Protect vil si å beskytte systemer og frekvenser gjennom lovverk og lisenser. Et eksempel på dette er den norske ekom-loven som gjør det straffbart å forstyrre radiosignaler for navigasjon.

Toughen vil si å gjøre systemene mer robuste gjennom hensiktsmessige tekniske tiltak. Et eksempel på dette er å bruke mekanismer for autentisering og kryptering.

Augment vil si å redusere brukernes sårbarhet gjennom å ha tilgang på alternative løsninger. Relatert til nøyaktig tid vil det gjerne bety å distribuere tid fra en atomklokke ved hjelp av en

radiosender eller fibernett uavhengig av GNSS. Et slik opplegg er realisert i Sverige (Ebenhag et al., 2019) der flere klokker med geografisk spredning i beskyttede lokaler er kommersielt tilgjengelig gjennom bakkenett. Et tilsvarende opplegg for nasjonal distribusjon av tid er på trappene i UK gjennom National Timing Centre[9].

[9] https://www.npl.co.uk/ntc

4. DIGITALISERING AV SAMFERDSELSSEKTOREN

Problemstillingen i oppgaven går inn i digitalisering av samferdselssektoren. Det er derfor relevant å se på hva som menes med en digitalisert samferdselssektor og hvordan det henger sammen med GNSS. I dette kapittelet vil jeg først drøfte begrepene transport, samferdsel, mobilitet og transportsystem. Disse brukes mye i offentlige dokumenter knyttet til sektoren, men er ikke nødvendigvis klart definert.
Deretter vil jeg beskrive hva som kjennetegner digitaliseringen av hver enkelt transportform. Jeg går inn på transportmidler, infrastruktur og trafikkovervåking/-kontroll. Jeg vil også komme inn på hvordan digitaliseringen muliggjør nye transportformer og hvordan endringene som skjer er med å sette preg på samfunnsutviklingen generelt.

4.1. Sentrale begreper

I en omtale av digitalisering av samferdselssektoren er det nyttig å først se på hva som menes med begreper som transport, samferdsel, mobilitet og transportsystem. Disse brukes mye i tekster, rapporter og planer som omhandler sektoren og de brukes i offentlige dokumenter om samfunnssikkerhet.

4.1.1. Transport

Ordet transport kommer av latin *trans* som betyr «på den andre siden», og *portare*, som betyr å bære. Transport betyr etter dette å bære noe over til den andre siden. I følge Store Norske Leksikon er transport[10] forflytning av gods eller passasjerer fra et sted til et annet. Transport betraktes gjerne som delt i fire ulike transportformer avhengig av infrastruktur og transportmidler: vegtransport, jernbanetransport, lufttransport og maritim transport. Det vil være ulike hensyn som påvirker valget av transportform. For en bedrift som driver etter just-in-time-prinsippet vil transporttid og -pris være viktig. Det er også viktig at leveransen faktisk kommer fram så transportformens, eller transportørens, pålitelighet og sikkerhet vil ha betydning. For den enkelte av oss i hverdagen vil transportbehovet bli dekket gjennom å gå, sykle, bruke bilen eller ta kollektivtransport. Det handler som regel om hva som er tilgjengelig i nærmiljøet, hva som er praktisk i hverdagen og hvor langt vi skal.

[10] https://snl.no/transport (besøkt 2020-08-09)

Hva som er tilgjengelig av transportformer i nærmiljøet har tradisjonelt hatt sammenheng med geografi og topografi. Langs kysten var det naturlig å utnytte vannet og bruke båter for transport, mens det i innlandet var naturlig å velge vei og jernbane. I årene som har gått siden staten opphevet rasjonering av personbiler i 1960, har dette endret seg i betydelig grad. En generell tilretteleggelse for privatbilisme og lastebiltransport gjør at vannet har endret status fra å muliggjøre transport til å bli et hinder for transport. Bilferger som et veisubstiutt ble en nødvendighet. Nå ansees også fergene som et dårlig tilbud og det bygges i stedet broer og tuneller. Dette gjenspeiles f.eks. i alle veiprosjektene som til sammen skal utgjøre fergefri E39. Stortinget besluttet på slutten av 1960-tallet å bruke lufttransport for å knytte landsdelene sammen. Det vi i dag kjenner som kortbanenettet ble til utover 1970- og 1980-tallet. Som et resultat av dette ligger Norge i verdenstoppen i antall lufthavner med rutetrafikk ift. folketallet.

Figur 5: Fjorden som transportmulighet (kilde: https://www.flickr.com/photos/nordnorskfoto/10706270385/)

Figur 4: Fjorden som transporthinder (kilde: https://www.osogfusa.no/nyhende/vegvesenet-vil-prioritera-ferjefri-e39/.

4.1.2. Samferdsel

Den helheten, eller systemet, som dannes av transportformer, transportmidler, transportinfrastruktur, tilbydere av transporttjenester, samt de lover, regler og politiske vedtak som lager rammer og muligheter for systemet, kalles samferdsel. Ifølge Wikipedia[11] omfatter samferdsel «transport av gods, personer og informasjon lokalt, regionalt og internasjonalt. Til samferdselssektoren hører planlegging, forvaltning og drift av anlegg og utvikling, vedlikehold og kontroll av transportmidler». Denne definisjonen legger flytting av informasjon inn i

[11] https://no.wikipedia.org/wiki/Samferdsel (sist besøkt 2020-06-15)

samferdselsbegrepet. I Norge, og en rekke andre land, har det vært tradisjon for dette ved at post- og teletjenester har vært en del av SDs ansvarsområde. Dette ble det gjort en endring på i 2019 som følge av enighet mellom regjeringspartiene i Granavolden-plattformen[12]. Det ble opprettet en digitaliseringsminister i Kommunal- og moderniseringsdepartementet (KMD) og ekom-tjenester ble flyttet fra SD til KMD.

4.1.3 Mobilitet

I tillegg til begrepene transport og samferdsel, som nok brukes en del om hverandre i hverdagen, har det sammen med den pågående utviklingen i sektoren blitt vanlig å bruke begrepet mobilitet. Begrepet brukes i stort omfang i transportrelaterte artikler og offentlige publikasjoner og bærer litt preg av å være et moteord. Hva som legges i begrepet av de som bruker det er ikke alltid like entydig. Store Norske Leksikon[13] sier enkelt at mobilitet er det samme som bevegelighet. Noe som er mobilt er noe som er lett å flytte.

Regjeringen satte i 2018 ned et utvalg kalt Ekspertutvalget for teknologi i fremtidens transportsystem. Utvalgets rapport ble publisert i juni 2019 (SD, 2019). Utvalget bruker mobilitet hyppig i sin rapport, men definerer ikke begrepet. Vi må likevel anta at mobilitet er en sentral del av utvalgets budskap ettersom begrepet brukes i rapportens tittel. Utvalget skriver innledningsvis at bevegelsesfrihet er opplevelsen av høy mobilitet og at denne friheten er grunnleggende positiv og verdiskapende for vårt moderne samfunn. Her kan det se ut til at mobilitet ikke bare handler om at det er lett å flytte på seg i samfunnet, men at begrepet kan knyttes til en opplevelse av, eller følelse av, frihet. Denne frihetsfølelsen bidrar videre til verdiskapning i samfunnet. Ordet mobilitet brukes 140 ganger i løpet av rapportens 100 sider i ulike sammensatte begreper som heller ikke defineres. Det er f.eks. mobiltetsløsninger, mobilitetstjenester og delingsmobilitet.

Nasjonal Transportplan (NTP) er det øverste plandokumentet for norsk samferdselssektor. Det utgis av SD og fyller funksjon som strategidokument og langtidsplan. Det er her de store prioriteringene og rammene for utviklingen i sektoren gis fra politiske myndigheter. Gjeldende versjon (Meld. St. 33 (2016-2017)) dekker en 12-års periode fra 2018-2029. Her brukes også begrepet mobilitet uten at det defineres. Bruken av ordet er til dels sammenfallende med

[12] Politisk avtale fra januar 2019 mellom Høyre, Venstre, Fremskrittspartiet og Kristelig folkeparti (Krf) som grunnlag for at Krf skulle gå inn i regjeringen Solberg.
[13] https://snl.no/mobilitet

Ekspertutvalgets rapport. Blant annet sier NTP at god mobilitet gir mennesker en enklere hverdag og frihet til å bosette seg der man ønsker.

Det skapes en noe mer konkret betydning av begrepet når man ser mer helhetlig på NTP og Ekspertutvalgets rapport. Mobilitet handler om å kunne bevege seg raskt, enkelt og effektivt når man har et transportbehov i hverdagen. For å oppnå dette må det i mindre grad tenkes på den enkelte transportform, men i stedet settes fokus på å forsøke å skape en helhet av alle transportformer der den reisende sømløst kan skifte transportform underveis. Den reisende skal oppleve det som at systemet kan tilby den transporttjenesten som fyller behovet best der og da. Dette kalles mobilitetstjenester eller «Mobility-as-a-Service» (MaaS). Dette kan oppnås gjennom digitalisering av transportsektoren der det samtidig legges vekt på verdiskaping og omstilling til lavutslippssamfunnet. Et eksempel på dette er Vy Tog som tilbyr el-biler (Din Bybil[14]) i Oslo sentrum hvis du har et transportbehov etter du går av toget på Oslo S. Med stadig flere mennesker i byer og tettsteder er det nødvendig at økt transportbehov dekkes gjennom andre løsninger enn bensindrevet privatbil. Dette bidrar staten til økonomisk gjennom å inngå bymiljøavtaler og byvekstavtaler[15] med norsk byer. El-drevne busser, tog og trikk vil være sentralt. El-biler og el-sykler kan leies ved behov. Da går antall kjøretøy ned og arealer kan frigjøres til andre formål enn vei og parkering. Når prinsippene for delingsøkonomi[16] anvendes innenfor mobilitet kalles det noen ganger delingsmobilitet.

Gjeldende versjon av NTP skiller seg fra tidligere utgaver blant annet ved at den har et tydelig fokus på teknologi og digitalisering. Planen har et eget kapittel (kap. 3) om den utviklingen transportsektoren nå gjennomgår. Det fremgår veldig tydelig at den tekniske utviklingen som nå skjer, og de mulighetene det gir for en stadig forbedret mobilitet, er en ønsket utvikling. Regjeringen ønsker å gripe de mulighetene som ny teknologi gir og bruke statlige virkemidler for å fremme teknologisk utvikling som skaper fremtidens mobilitet. Teknologien skal bidra til å nå transportpolitiske målsettinger.

4.1.4. Transportsystem

Begrepet transportsystem er brukt av regjeringen i Ekspertutvalgets mandat og det brukes av utvalget mange steder i rapporten. Det er ikke definert eller forklart og det ser ut til at det kan

[14] https://www.vy.no/bybil?gclid=EAIaIQobChMI_Lrj9IaO6wIVyQJ7Ch2odAzaEAAYASAAEgIYvPD_BwE
[15] https://www.regjeringen.no/no/tema/transport-og-kommunikasjon/kollektivtransport/belonningsordningen-bymiljoavtaler-og-byvekstavtaler/id2571977/ (besøkt 2020-08-26)
[16] https://snl.no/delings%C3%B8konomi

gis ulike betydninger. Der hvor begrepet brukes i entall, f.eks. fremtidens transportsystem eller et transportsystem som fremmer verdiskapning, går det fram at det er en overordnet helhet det tenkes på. Her kan transportsystem forstås som en helhet bestående av transportinfrastruktur, transportmidler og hvordan dette fungerer sammen med brukerne.

Ekspertutvalget skriver at transportsystemet har som sin hovedfunksjon å sikre mobilitet. Med dette knyttes begrepene mobilitet og transportsystem sammen. Transportsystem gis her en betydning av å være infrastrukturen som muliggjør menneskets frihetsfølelse. Transportsystemet gjør det mulig å ferdes dit man vil, når man vil og ved hjelp av de transportmidlene som er mest hensiktsmessig. NTP gjør en tilsvarende sammenkopling ved å si at transportsystemet er i en brytningstid og at dette påvirker fremtidens mobilitet.

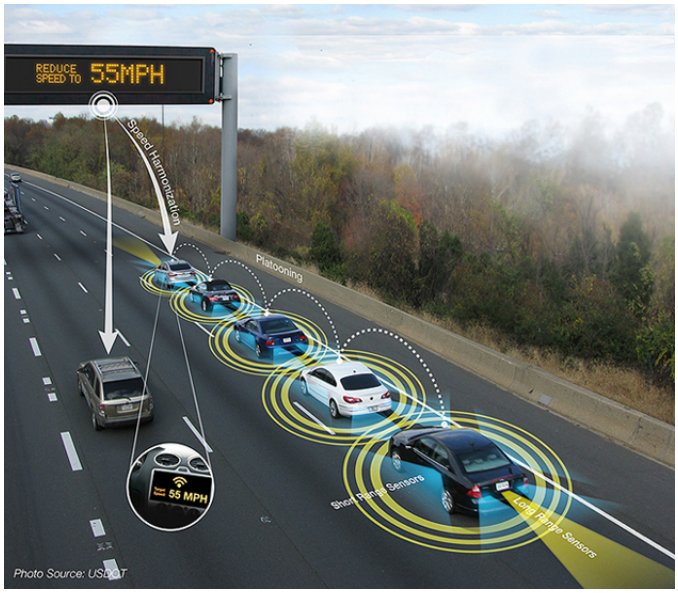
Begrepet transportsystem kan også gis en mer avgrenset betydning. Både NTP og Ekspertutvalget bruker ordet i bestemt og ubestemt form flertall: transportsystemer og transportsystemene. Ved slik bruk kan det være snakk om at det totale transportsystemet betraktes som å være en helhet bestående av de enkelte transportsystemene for hver transportform. F.eks. vil fly, lufthavner, luftromsstruktur og navigasjonssystemer utgjøre transportsystemet for luftfart. Et annet eksempel er at begrepet brukes i omtale av tekniske systemer, og da gjerne digitaliserte transportsystemer. Dette knyttes vanligvis opp mot begrepet ITS, Intelligente Transportsystemer.

4.2. Digitalisering

Det norske samfunnet har de senere årene opplevet store endringer som følge av en stadig økende grad av digitalisering. Dette skjer i både privat og offentlig sektor og gjelder naturlig nok også samferdselssektoren. Det er en politisk målsetting i Norge at samfunnet skal digitaliseres på alle områder der det gir gevinster som forenkling, effektivisering, bedre miljø og bedre sikkerhet (KMD, 2016). Norske samferdselsmyndigheter ønsker å tilrettelegge for denne utviklingen og målsettinger innenfor digitalisering av sektoren kommer særlig til syne i kapittel 3 i gjeldende NTP. I mandatet til Ekspertutvalget sier regjeringen at transportinfrastruktur ikke bare omfatter «klassisk» infrastruktur, men også ny digital infrastruktur som støtter opp under funksjonen til transportsystemet. Det påpekes videre at utviklingen har medført at transportsystemene har blitt mer avhengige av til enhver tid velfungerende og sikre IKT-systemer.

Endringene som bidrar til digitalisering innenfor samferdselssektoren er blitt mulig gjennom den utviklingen som har foregått innen miniatyrisering av elektronikk og datakraft, økt kapasitet i tele-/datanett, trådløse mobilnett med 4G/5G, batteriteknologi, smarttelefoner og gratis tilgang til GNSS. Endringene skjer i transportmidlene, i hvordan disse bindes sammen til en samferdselshelhet og hvordan vi som brukere forholder oss til denne helheten. Der vi før brukte reisebyrå, fysiske penger, rutebok for Norge og papirkart kan vi nå få all informasjon gjennom en digital løsning på smarttelefon.

IKT-systemer som benyttes i samferdselssektoren kalles ofte ITS, Intelligente Transportsystemer (SVV, 2020). Begrepet favner bredt fra automatiserte kjøretøy til billettsystemer og innhenting av sanntidsinformasjon om trafikkforhold ved at biler er koplet sammen gjennom tingenes internett (IoT). ITS brukes i alle transportformer, men vegsektoren har særlig gjort seg gjeldende. Hensikten med ITS er som regel å utnytte transportmidler og infrastruktur bedre slik at det oppnås økt effektivitet, mindre utslipp og økt sikkerhet. ITS som utveksler data mellom kjøretøy, eller mellom kjøretøy og annen infrastruktur gjennom skyløsninger, kalles samvirkende ITS[17]. Det er vanlig å se dette omtalt som Connected-ITS (C-ITS).



Figur 6: Intelligente transportsystemer muliggjør datautvekslig mellom kjøretøy og mellom kjøretøy og infrastruktur (kilde: www.its.dot.gov)

4.2.1. Veitransport

I veitransport skjer en digitalisering av både kjøretøyet og miljøet kjøretøyet skal være en del av. I en ny bil i dag vil det være mange digitale «nice-to-have»-løsninger som ikke har noe med kjøretøyets framdrift eller styring å gjøre. Disse kan være plassert der av ulike årsaker som f.eks. at det ser bra ut, gjør ting litt enklere eller er ment å skape en følelse av luksus. En rekke andre digitale systemer vil kunne bidra til økt sikkerhet som f.eks. varsling av lavt lufttrykk i et

[17] I forbindelse med C-ITS vil en ofte se forkortelsene V2V (vehicle-to-vehicle) og V2I (vehicle-to-infrastructure), V2C (vehicle-to-cloud) og V2P (vehicle-to-pedestrian). Noen ganger brukes samlebetegnelsen V2X (vehicle-to-everything)

dekk, blindsonevarsling og automatisk oppbremsing hvis det er et hinder i veibanen sjåføren ikke har sett. Flere bilprodusenter tilbyr nå modeller med ulik grad av automatisert kjøring, mange steder prøvekjøres selvkjørende busser og for lastebiltransport har «platooning» blitt demonstrert. Dette vil si at flere lastebiler kjører førerløst tett etter hverandre og automatisk følger bilen foran seg.

Veitrafikksentralene bruker digitale løsninger for overvåking og styring av trafikk på veier og i tuneller, og SVV har etablert digitale løsninger for tjenester rettet mot trafikantene.

Statens vegvesen har stort fokus på ITS med egen ITS-strategi for vegsektoren og en rekke prosjekter for utprøving av teknologi og løsninger. EUs ITS-direktiv (2010/40/EU) er tatt inn i EØS-avtalen og Stortinget vedtok i 2015 en ITS-lov for å gjøre direktivet til norsk lov. Alle løsninger innenfor selvkjøring og digitalisering benytter GNSS for posisjonsbestemmelse eller synkronisering. Andre anvendelser av GNSS er automatisk varsling av ulykker (eCall) som ble påbudt i nye personbiler fra april 2018, og satellittbasert veiprising til erstatning for dagens bompengesystem.

JRC[18] publiserte en rapport i 2019 med tittel The Future of Road Transport (JRC, 2019). Her gjøres en tilsvarende øvelse som Ekspertutvalget gjorde ved at det er sett på den pågående teknologiutviklingen og digitaliseringens betydning for veisektoren i de kommende årene. JRC kaller den utviklingen som foregår nå for en revolusjon og at vi står foran en ny æra innen veitransport. JRC har identifisert fire trender som former utviklingen: automatisering (automation), samvirke (connectivity), alternativer til fossilt drivstoff (decarbonisation) og delingsmobilitet (sharing).

4.2.2. Jernbanetransport

For en sikker togtransport er det viktig å vite hvor togene befinner seg, avstanden mellom dem, om de er i bevegelse, at det ikke har mistet noen vogner og at togsentralen har kommunikasjon med lokføreren. Til dette brukes i dag lyssignaler langs sporet, balliser i sporet, akselltellere, odometer og det digitale kommunikasjonssystemet GSM-R[19].

[18] Joint Research Centre, EUs forskningsbyrå i Roma.

[19] Global System for Mobile Communication – Railway. Digitalt trådløst kommunikasjonssystem for kommunikasjon og dataoverføring mellom tog og kontrollsentralen.

Det pågår innføring av et nytt felleseuropeisk digitalt signalsystem i Norge, ERTMS[20], som vil kunne gi endringer på dette. Via GSM-R vil lokfører motta informasjon om kjøretillatelse (grønt og rødt lys) og hastighet direkte på togets førerpanel. Da vil det ikke lenger være behov for lyssignaler og hastighetsskilt langs sporet. Dette gir mulighet for å tilpasse blokkstrekningene til trafikkmengden og dermed oppnå økt effektivitet gjennom bedre utnyttelse av infrastrukturen. Toget vil automatisk overvåke sin hastighet og kunne melde inn sin posisjon til togsentralen.

Sporveien AS, som eier og drifter trikk og T-bane i Oslo, innfører tilsvarende teknologi, CBTC[21]. Her går alle signaler og datakommunikasjon for trafikkstyring via Telias mobilnett. GNSS er avgjørende for synkronisering av de digitale mobilnettene og dermed sikkerhetskritisk funksjonalitet.

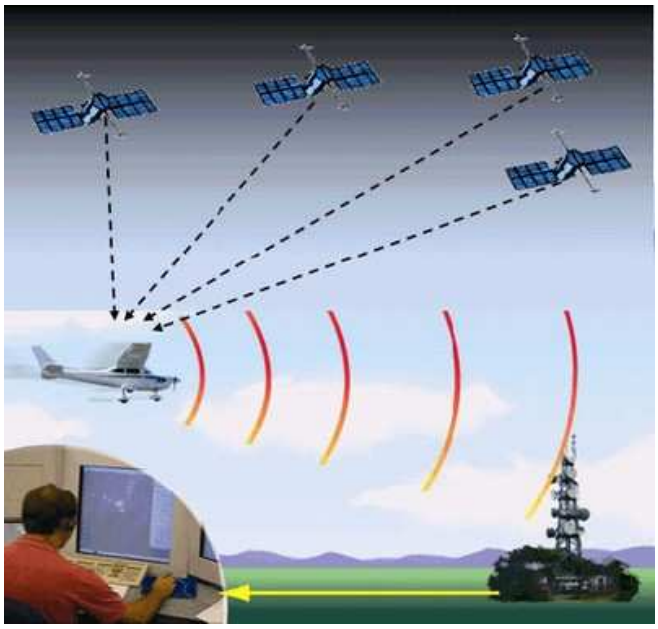
4.2.3. Lufttransport

Lufttransport er den yngste transportformen og har i realiteten alltid vært preget av elektroniske og digitale løsninger både om bord i flyene og i infrastrukturen på bakken. Det finnes en omfattende infrastruktur av radar- og radionavigasjonssystemer, radioinstallasjoner for kommunikasjon mellom fly og bakke, og tele-/datanett for utveksling av operativ og administrativ informasjon mellom enheter i lufttrafikktjenesten og lufthavnene. Utviklingen over de senere årene har gått i retning av økt avhengighet av GNSS generelt og nøyaktig tid fra GNSS spesielt. Flyene bruker i all hovedsak GNSS for navigasjon og innflyging til lufthavnene i stedet for den tradisjonelle radionavigasjonsinfrastrukturen på bakken.

For å overvåke og kontrollerer trafikken i luftrommet har lufttrafikktjenesten tradisjonelt benyttet radar. Denne teknologien er på vikende front til fordel for nye systemer[22]. Disse kan ha både operative og driftsmessige fordeler framfor radar, men de er svært avhengige av GNSS både for posisjon og nøyaktig tid.

[20] European Rail Traffic Management System. Felleseuropeisk standard for digitalt signalanlegg på jernbanen som er under innføring i Norge. GSM-R utgjør det informasjonsbærende elementet i ERTMS.
[21] Communication-based Train Control
[22] Her er særlig relevant WAM og ADS-B. WAM regner ut flyets posisjon ved å måle tidsdifferansen mellom når to eller flere mottakere på bakken mottar et radiosignal («extended twitter» fra Mode-S-transponderen) som er sendt ut fra flyet. Utregnet posisjon overføres til flygelederen. Med ADS-B kringkaster flyet sin identifikasjon og GPS-baserte posisjon. Dette mottas på bakken og overføres til flygelederen.

Alle bakkestasjonene i disse systemene er avhengig av digitale nett for dataoverføring som må synkroniseres. I alle sammenhenger der det er snakk om nøyaktig posisjonsbestemmelse eller nøyaktig tid og frekvens for synkronisering, benyttes GNSS alene eller sammen med atomklokker. Det betyr at GNSS er avgjørende både for flyenes navigasjon og lufttrafikktjenestens kontroll av trafikken.



Figur 7: Luftfart har gjort seg helt avhengig av GNSS

Et annet aspekt innenfor digitalisering av luftfart er fremveksten av dronebransjen. Fra å være små leketøy har dette utviklet seg til en bransje som tilbyr tjenester utført med relativt store droner der myndighetene stiller krav til opplæring og sertifikater. Droner kan utføre ulike inspeksjons- og datafangstoppgaver eller transport av varer og mennesker. Dronene bruker i stor grad GNSS for navigasjon.

I 2018 publiserte regjeringen en nasjonal dronestrategi (SD, 2018a). Strategien setter fokus på hvordan regulering av flysikkerhet, samfunnssikkerhet, miljøvern og personvern kan gjøres og samtidig legge til rette for en markedsrettet og samfunnstjenlig utvikling av dronevirksomhet i Norge.

4.2.4. Maritim transport

Innen maritim transport har GNSS for lengst etablert seg som primærsystemet for navigasjon selv om radar, lykter og merker fortsatt spiller en rolle for kystnær navigasjon. Tidligere fantes bakkebaserte radionavigasjonssystemer som Loran-C og Decca, men disse er utfaset. Papirkart er i stor grad erstattet av digitale kartplottere og ECDIS[23]-installasjoner som viser egen og andre fartøys posisjon i et digitalt kart. Anti-kollisjonssystemet AIS[24] ble innført for en del år tilbake. Båter som er innenfor dekning av hverandres AIS-signaler vil bli synlig på skjerm hos hverandre med informasjon om posisjon, kurs og fart. Systemet er digitalt og synkroniseringen

[23] Electronic Chart Display and Information System. («kartmaskin»).
[24] Automatic Identification System

er basert på tid fra fartøyets GPS. AIS-signalene fanges også opp av Kystverkets basestasjoner på land og satellitter i polar lavbane[25] (AISSat og NorSat). Mottatte signaler brukes til trafikkovervåking og kontroll ved Kystverkets sjøtrafikksentraler.

Den internasjonale sjøfartsorganisasjonen IMO har utviklet en global strategi kalt eNav[26]. eNav har til hensikt å legge til rette for digitalisering og automatisert utveksling av informasjon mellom skip og mellom skip og land. Målsettingen er forenkling av arbeidsprosesser som derav gir økt sikkerhet. Kystverket har en rekke prosjekter knyttet til nye løsninger som er i tråd med strategien. Et eksempel er rapporteringssystemet SafeSeaNet.

Figur 8: Yara Birkeland (kilde: https://www.tu.no/artikler/yara-birkeland-autonomiprosjekt-pa-land-ble-for-komplisert/502268)

Utviklingen av fjernstyrte og autonome skip har stort fokus og har kommet relativt langt i Norge. Skip uten mannskap vil være svært avhengig av GNSS for å kunne seile autonomt, men også satellittkommunikasjon blir viktig for overvåking og fjernstyring fra land. En ser for seg en mulig fremtid der autonome lasteskip legger til ved automatiserte havner der automatikken sørger for å losse containerne og sette dem på selvkjørende lastebiler for videre landtransport. Det klassiske eksemplet i Norge har blitt Yara Birkeland-prosjektet som bygger en autonom, elektrifisert lastebåt. I 2019 ble losloven opphevet til fordel for ny havne- og farvannslov. Hovedhensikten med endringen var å åpne for autonom seilas uten bruk av los. Det finnes etter hvert flere aktører som tilbyr droner for undervannsoppgaver.

[25] Polar lavbane vil si at satellittbanen går over polområdene og at satellittene er lavere enn 1000 km over bakken.
[26] http://www.imo.org/en/OurWork/safety/navigation/pages/enavigation.aspx (Besøkt 2020-08-26)

4.2.5. Nye transportformer

I tillegg til de fire klassiske transportformene har utviklingen innen digitalisering og elektrifisering gitt oss nye transportformer. Et eksempel på dette er mikromobilitet (TØI-rapport 1721/2019). Begrepet omfatter transportmidler med eller uten elektrisk motor og som ikke veier mer enn 500kg. Transportmidlene brukes som regel i urban sammenheng og kan gjerne være en delt ressurs. El-sparkesykkel, bysykler og varesykler er eksempler på dette. Slike sykler har GNSS-mottaker innebygd. Utleie og informasjon om hvor det er ledige sykler foregår gjennom app på smarttelefon. Transportformen stanser raskt uten GNSS. Et annet eksempel er Urban Air Mobility (UAM). Dette handler om persontransport med førerløse droner som et drosjetilbud. Dette er teknologisk avansert og bilindustrien og flyprodusentene går sammen i utviklingsprosjekter. Eksempler på dette er samarbeid mellom Airbus og Audi og mellom Boeing og Porsche. Slike «flygende biler» vil være avhengig av GNSS både for egen navigasjon og for å kunne sende egen posisjon inn til lufttrafikktjenesten og operatørens flåtestyringssystem.

Figur 9: Drone for persontransport (kilde: https://www.cnet.com/roadshow/news/audi-flying-taxi-airbus-drone/)

4.3. Smart mobilitet og smarte samfunn

Samferdsel og organiseringen av samfunnet henger tett sammen. Muligheten for å flytte oss dit vi vil når vi vil, mobilitet, har stor betydning for at samfunnet skal fungere effektivt på en god måte. Tilgang på transportmidler og transportinfrastruktur påvirker reisetid og dermed hvor vi bor i forhold til skole og jobb, og hva vi synes er grei avstand til butikker og andre nødvendige tjenester.

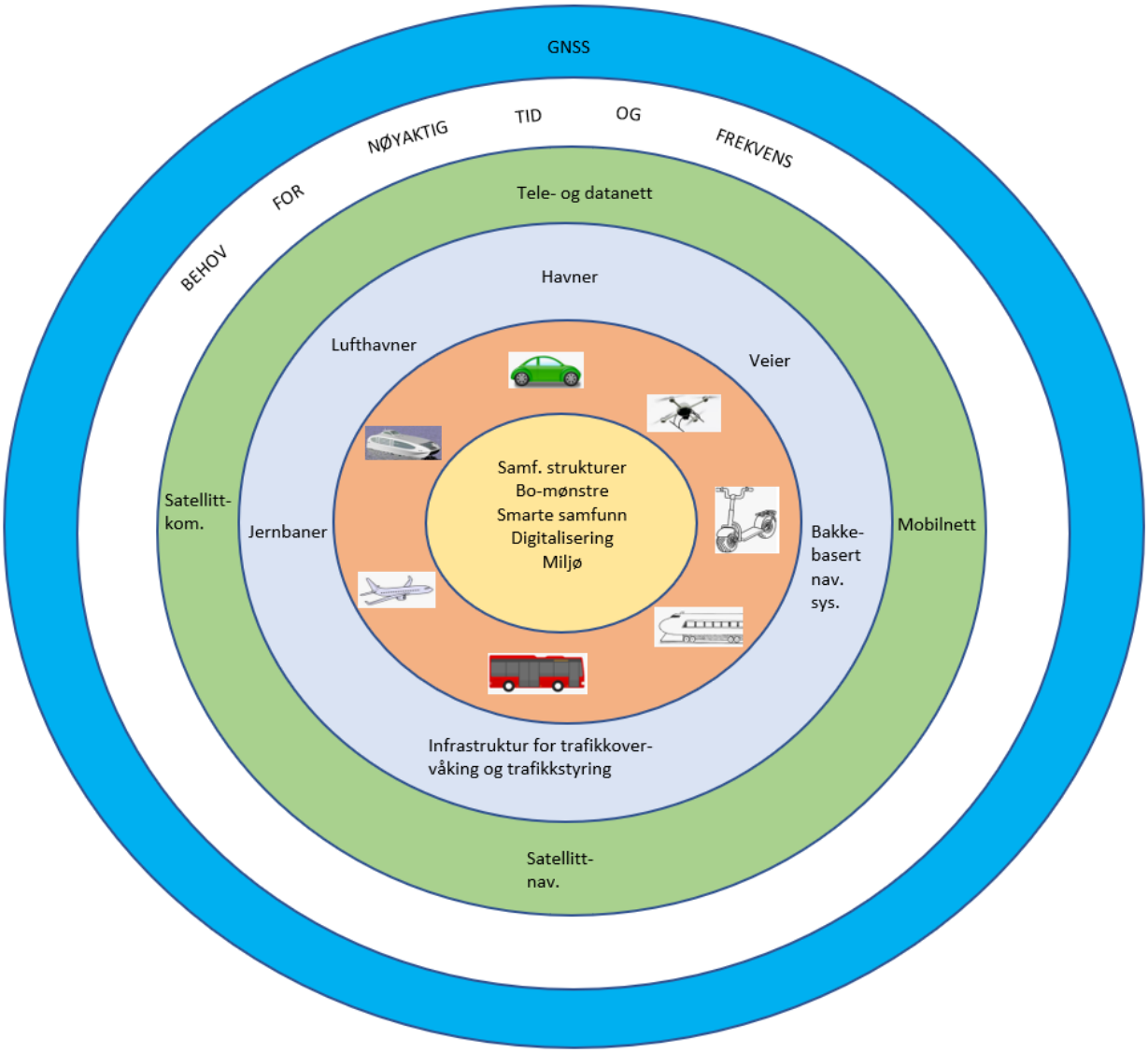
Med det grønne skiftet settes også fokus på hvordan byer og tettsteder skal utvikles til å bli bærekraftige og moderne samfunn fundamentert på miljømessige verdier. Dette kalles ofte smarte samfunn. Hvordan beboerne ferdes i slike samfunn er viktig for den helheten som ønskes skapt.

Figur 10: Illustrasjon av prinsippene for smarte byer (kilde: https://www.researchgate.net/figure/Smart-Mobility-in-a-Smart-City_fig1_286613340)

Ved å legge smarte mobilitetsløsninger, delingsøkonomi, digitalisering, elektrifisering og ITS til grunn for samfunnsplanleggingen kan det skapes moderne samfunn med reduserte transportbehov, men som samtidig kan tilby effektiv mobilitet i hverdagen. Smart mobilitet forklares gjerne som det å transportere mennesker og gods fra et punkt til et annet på nye, innovative og bærekraftige måter.

4.4. Betydningen av GNSS for digitaliseringen

I kapittelet om GNSS gikk jeg inn på hvordan GNSS virker og hvorfor det er en populær kilde til nøyaktig tid og frekvens. Enkelt sagt så er alle digitale IKT-løsninger avhengig av synkronisering, og nødvendig tid og takt hentes veldig ofte fra GNSS. Det betyr at den digitaliseringen vi ser foregår skaper en stadig større avhengighet av GNSS. Ettersom samferdsel er viktig for samfunnssikkerheten følger det av dette at også samfunnssikkerheten blir stadig mer avhengig av GNSS. Innenfor de ulike grenene av samferdselssektoren ser vi at GNSS er viktig for utviklingen av transportmidler som automatiserte fartøy, selvkjørende biler og droner. Det gjelder både posisjonsbestemmelse, navigasjon og tidsbestemmelse. Samtidig har GNSS blitt en viktig faktor for å synkronisere den digitale infrastrukturen som knytter alt dette sammen og som knytter de reisende til mobilitetsløsningene. Når dette til slutt legges til grunn for å skape smarte samfunn ser vi at i realiteten har samfunnet som helhet blitt GNSS-avhengig med tilhørende mulige sårbarheter. I fig. 11. har jeg illustrert hvordan dette kan betraktes som et GNSS-basert sosioteknisk system.



Figur 11: Et digitalisert samfunn som et GNSS-basert sosioteknisk system

5. SIKKERHETSSTYRING

I dette kapitlet går jeg inn på begreper og teorier knyttet til sikkerhetsstyring og relaterer det til samfunnssikkerhet. Dette er relevant som grunnlag for faktainnsamlingen senere i oppgaven som bl.a. vil rette seg mot sikkerhetsstyring hos samferdselsaktører. Sikkerhetsstyring kan defineres som alle tiltak som iverksettes for å oppnå, opprettholde og videreutvikle et sikkerhetsnivå i overensstemmelse med definerte mål. Definisjonen gjelder for samfunnssikkerhet hvis ordet sikkerhetsnivå erstattes med samfunnssikkerhetsnivå. (Njå et al., 2020).

Jeg ser først på enkelte sentrale begreper som sikkerhet, risiko, sårbarhet og barriere. Videre går jeg inn på forskjellen mellom naturvitenskapelig og samfunnsvitenskapelig kunnskapssyn relatert til sikkerhetsstyring, og deretter ulykkesmodeller og kaskadeeffekter.

5.1. Sikkerhetsbegrepet

Hva menes med sikkerhet? NTNU-professorene Rausand og Utne skriver i boka Risikoanalyse – teori og metoder (Rausand & Utne, 2009), at sikkerhet som begrep er vanskelig å definere. Bortsett fra i innarbeidede ordsammenstillinger som f.eks. IKT-sikkerhet og samfunnssikkerhet, unngår de derfor å bruke ordet. I Store Norske Leksikon[27] (SNL) er sikkerhet definert som en tilstand med fravær av uønskede hendelser eller frihet fra fare og frykt. En slik tilstand er ikke statisk, men vil bli påvirket av endringer i faktorer som trussel, farer, sårbarhet og verdi.

I stedet for sikkerhet tar Njå mfl. for seg usikkerhet. Med utgangspunkt i det latinske ordet certanitatem[28], som betyr noe som er gitt eller ikke kan betviles, kan usikkerhet betraktes som noe som *kan* betviles og diskuteres. Beslutninger under usikkerhet er sentralt i risikovurderinger ettersom usikkerhet er en karakteristikk ved fremtiden. Likevel har ingen klart å gi en entydig definisjon på usikkerhet. Betydningen av usikkerhet kan knyttes til hvor vi er på tidslinjen. I nåtid handler usikkerhet om hva vi kan vite om våre systemer eller samfunnsviktige funksjoner. I fortid vil usikkerhet være knyttet til graden av korrekt observasjon av ting som har skjedd, og

[27] https://snl.no/sikkerhet (besøkt 2020-08-06)
[28] Certanitatem er latinsk utgangspunkt for det engelske «certainty» som betyr sikkerhet

dermed våre metoder. I fremtid handler usikkerhet om hva som vil skje. Usikkerhet om fremtiden er knyttet til risiko.

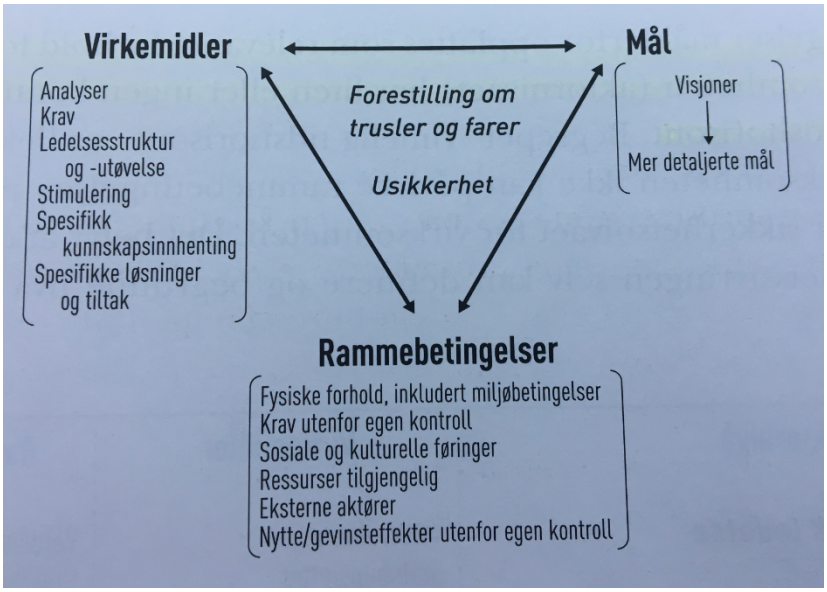
SNLs definisjon knytter sikkerhet sammen med fravær av uønskede hendelser. Begrepet uønsket hendelse er i terminologilisten hos Rausand/Utne gitt to ulike forklaringer. Den første er «hendelse som kan medføre tap av verdier». Den andre er «en irreversibel, fysisk hendelse som kan føre til skade på mennesker, miljø eller materielle verdier». Hvis vi ser dette i sammenheng med SNLs definisjon ser vi at en tilstand av sikkerhet handler om fravær av hendelser som påfører skade på oss selv eller våre omgivelser på en måte som ikke kan gjøres om.

Denne måten å betrakte sikkerhet på er en av flere. Sikkerhetsbegrepet kan ha flere dimensjoner (Antonsen et al., 2017). Sikkerhet kan betraktes som en subjektiv størrelse der spørsmålet om noe er sikkert avgjøres av hvordan det oppleves. Hvordan sikkerheten oppleves – sikkerhets-persepsjon – henger ofte sammen med i hvilken grad vi føler å ha kontroll over situasjonen vi befinner oss i. Et annet aspekt ved sikkerhet handler om hvorfor ting går bra. Ting går ikke nødvendigvis bra av seg selv. Det kan være et grundig og systematisk risikostyringsarbeid der det er gjort gode tiltak som er grunnen til at det ikke skjedde en ulykke. Det viser at organisatorisk praksis har betydning for oppnådd sikkerhetsnivå.

Fravær av ulykker alene er ikke i seg selv noe bevis på god sikkerhetstilstand. Granskninger av større ulykker har vist at det før ulykken var en lengre periode med høy risiko (Kongsvik et al., 2018). Sikkerhet kan betraktes ut fra to ulike perspektiver. Det ene er sikkerhet som fravær av risiko. Det kan oppnås gjennom å etablere barrierer for å hindre at hendelser oppstår eller for å hindre at konsekvenser oppstår som følge av en hendelse. Det andre er sikkerhet som nærvær av spesielle organisatoriske egenskaper. Det er egenskaper ved organisasjonen som gjør at den kan håndtere uventede situasjoner.

Njå et al. presenterer en generell modell for sikkerhetsstyring (fig. 11). Den tar utgangspunkt i at det er ønskelig å få kontroll over en situasjon med usikkerhet relatert til definerte trusler og farer. Denne prosessen skjer så gjennom å definere mål utledet fra en visjon, og deretter utarbeide relevante virkemidler for å nå disse målene. Alt skjer innenfor et sett av

rammebetingelser som vil være forhold av betydning for sikkerhetsstyringen, men som virksomheten har liten eller ingen kontroll over innenfor en rimelig tidshorisont.



Figur 12: Modell for sikkerhetsstyring (kilde: Njå mfl. fig. 3.1)

5.1.1. Resilience engineering, safety-I og safety-II

Erik Hollnagel er sentral innen teori om resilience engineering (RE). Resiliens er en fornorsking av resilience og brukes som faguttrykk på norsk. Denne teorien handler om hvordan organisasjoner kan utvikles slik at de får evne til å opprettholde tilstrekkelig sikkerhet når de utsettes for potensielt farlige påvirkninger (Kongsvik et al.). Resiliens skal her forstås som evne til å tilpasse seg forstyrrelser uten at normale funksjoner stopper opp. Dette forutsetter at sikkerhet ikke bare knyttes til hva som kan gå galt, men at det settes fokus på det som er normalt i daglig drift og hvordan dette kan videreutvikles slik at organisasjonen blir i stand til å håndtere uventede situasjoner. En resilient organisasjon må være i stand til å improvisere. Hollnagel sier en resilient organisasjon kjennetegnes ved:

- Evne til å lære
- Evne til å forutse
- Evne til å overvåke
- Evne til å respondere

Hollnagel snakker om safety-I og safety-II der RE er særlig knyttet til det siste. Safety-I er det vi kan kalle et tradisjonelt syn på sikkerhet. Her er fokuset på sikkerhet som fravær av uønskede hendelser og ulykker. Hvis noe går galt er det fordi mennesker, teknologi eller organisatoriske

forhold har sviktet. Safety-I-tankegang ligger bl.a. til grunn for virksomheten til Statens Havarikommisjon[29]. Innenfor safety-II-tankegang settes fokuset på hvorfor det nesten alltid går bra. Her er ikke mennesker en mulig kilde til feil, men en ressurs som er nødvendig for at systemet skal være fleksibelt og resilient. Et viktig poeng i safety-II er å studere situasjoner der sikkerheten er god nok, ikke der hvor ulykker skjedde.

5.1.2. Safety og security

Det norske ordet sikkerhet blir på engelsk til både safety og security. I engelsk-språklig faglitteratur differensieres det derfor mellom ulike betydninger av det vi bare har ett ord for på norsk. Innen lufttransport brukes safety om flysikkerhet i betydning gjennomføre flyturen fra start til slutt på en sikker måte, mens security brukes om vakthold og adgangskontroll ved flyplassen i betydning å hindre uvedkommende å true sikkerheten. Mer generelt er det etablert en forståelse på norsk der safety peker på hendelser som ikke er planlagt, som uhell og ulykker, mens security relateres til bevisste, målrettede handlinger (Kongsvik et al., 2018).

I vedlegg 5 til NOU 2006:6 (JD, 2006), drøfter professor Finn Erik Vinje begrepene safety og security rent språklig. Han hevder at denne forskjellen som er etablert i Norge ikke er så tydelig i engelsk språk og gir eksempler på at både safety og security brukes uavhengig av villede/ikke-villede handlinger. Vinjes forslag er at safety oversettes til trygghet og security til sikring. Safety kan ha to betydninger som er viktig innenfor samfunnssikkerhet. (Engen et al., 2016) Det ene er sikkerhet som tilstand, det vil si sikkerhet som noe faktisk. Det andre er sikkerhet som følelse, det vil si i hvilken grad man føler seg trygg.

Forskjellene i syn på sikkerhet slik begrepene safety og security representerer, har hver sine fagmiljø og sett av teorier. Innenfor samfunnssikkerhet brukes både societal safety og societal security. Societal safety skal forstås som det norske begrepet samfunnssikkerhet. Begrepet favner vidt og tar opp i seg forhold som dekker både security og safety (Almklov, Antonsen, Bye, et al., 2018). Societal security er et begrep som knyttes til den såkalte Københavnerskolen (Engen et al., 2016). Det omhandler samfunnets evne til å opprettholde sin karakter under endrede forhold og trusler. I artikkelen safer societies (Almklov, Antonsen, Størkersen, et al., 2018) argumenterer forfatterne for at digitaliseringen av samfunnet har medført at det har blitt et kunstig skille mellom security og safety. Sikkerhetstiltak relatert til security forutsetter ofte

[29] https://www.havarikommisjonen.no/

infrastruktur med fokus på safety gjennom teknisk sikkerhet, pålitelighet og oppetid. IKT-feil kan bli utløst både med og uten hensikt. Det er derfor viktig at fagmiljøene for safety og security samhandler ved risikoanalyser og sikringstiltak.

5.2. Risiko, barrierer og ulykker

Hensikten med å utøve sikkerhetsstyring er å oppnå et ønsket sikkerhetsnivå. Det gjøres gjennom et systematisk arbeid med å kontrollere faktorer som kan tenkes å påvirke sikkerheten. Sentralt i dette arbeidet er risikostyringen. Hvis vi legger til grunn definisjonen som sier at sikkerhet er fravær av uakseptabel risiko, så ser vi at ønsket sikkerhetsnivå kan oppnås ved å jobbe med risikofaktorer. Risikostyring er derfor en sentral del av sikkerhetsstyringen.

Risikostyring er en kontinuerlig ledelsesprosess. Når vi snakker om en risiko for et eller annet snakker vi alltid om framtidig usikkerhet. Når noe har skjedd forsvinner usikkerheten knyttet til det og risiko for at noe vil skje blir erstattet av faktisk kunnskap om hvordan det gikk. Risiko handler derfor om hva vi velger av de mulighetene vi har. På samme måte som for sikkerhet, er også risiko et begrep som brukes på ulike måter og har flere definisjoner. I følge Store Norske Leksikon[30] innebærer risiko hendelser som kan inntreffe og som har konsekvenser for noe som er av verdi for oss mennesker. Konsekvensene kan være knyttet til f.eks. liv og helse, miljø eller økonomiske verdier og det er alltid minst ett utfall som oppfattes som negativt eller uønsket. I dagligtale brukes ofte risiko og sannsynlighet om hverandre.

5.2.1. Realistisk/naturvitenskapelig kunnskapssyn

Risiko betraktes ulikt ut ifra valg av kunnskapssyn (Engen et al., 2016). Innenfor et realistisk kunnskapssyn tas det gjerne i bruk matematikk og statistikk for å prøve å forutsi muligheten for at en hendelse kan inntreff og hva som i så fall vil være konsekvensen. Definisjonen av risiko som produktet av sannsynligheten for at en hendelse inntreffer og konsekvensen hvis den inntreffer, hører til dette kunnskapssynet. Risiko blir her betraktet som en kalkulerbar størrelse.

Med referanse til standarden IEC60300-3-9, Risk Analysis of Technical Systems, oppgir Rausand/Utne at risikostyring kan brytes ned i tre hovedaktiviteter:

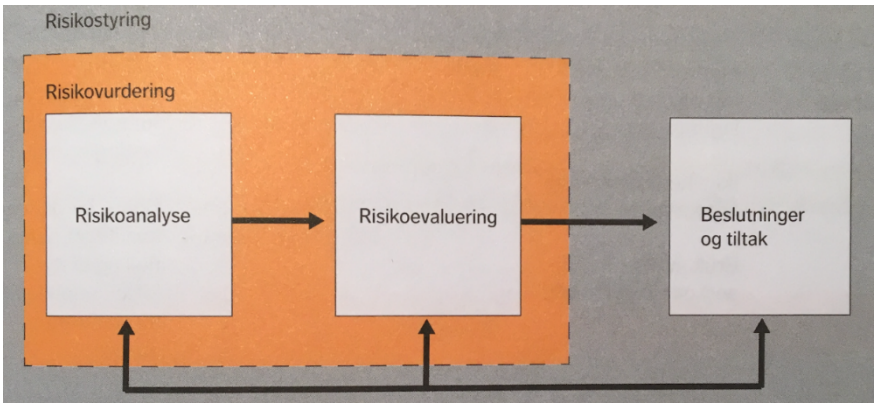
- Risikoanalyse
- Risikoevaluering

[30] https://snl.no/risiko (besøkt 2020-08-06)

- Risikokontroll og risikoreduksjon

Kongsvik et al. angir de samme tre hovedaktivitetene med referanse til standarden ISO 31000 Risikostyring. Ordlyden i det siste kulepunktet er litt annerledes i 31000 og kalles beslutninger og tiltak, men formålet med aktiviteten er den samme i begge standarder.

Risikovurdering brukes som et samlebegrep for de to første aktivitetene, mens risikostyring bruks som et samlebegrep for alle tre. Dette er illustrert i fig. 13.

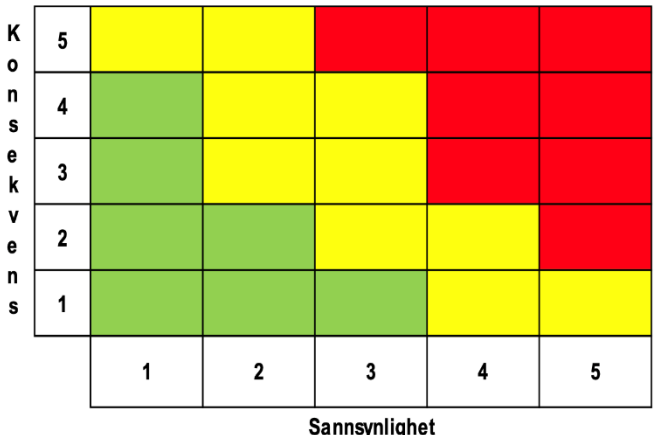


Figur 13: Risikostyring (kilde: Kongsvik et al. figur 7.1)

En risikoanalyse kan enkelt sies å bestå i å svare på følgende spørsmål (Kaplan 1997) relatert til den situasjonen som skal analyseres:

- Spm. 1: Hva kan gå galt?
- Spm. 2: Hvorfor går det galt, og hva er sannsynligheten for at det går galt
- Spm. 3: Hva kan bli konsekvensen hvis det går galt?

Utfallet av risikoanalysen kan så vurderes opp mot satte kriterier for hva som kan aksepteres for den aktiviteten/situasjonen/systemet som har blitt risikovurdert. Utfallet av dette vil være risikoevalueringen. Slike kriterier vil variere mellom ulike virksomheter og aktiviteter. Når en bedrift eller etat lager et sikkerhetsstyringssystem for sin



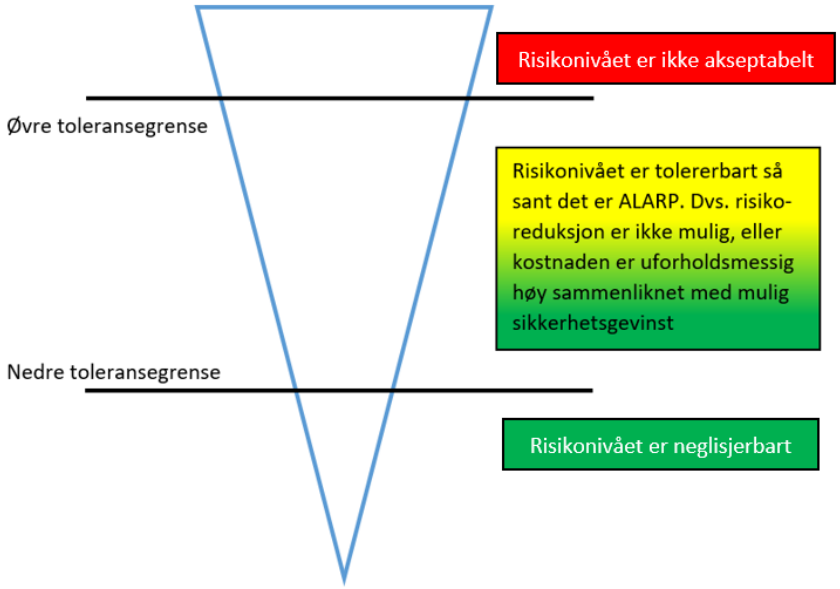
Figur 14: Prinsippskisse risikomatrise

virksomhet er det å utarbeide en riskomatrise som inneholder slike akseptkriterier en viktig aktivitet. De ulike feltene i matrisene gis vanligvis fargene grønn, gul eller rød etter følgende inndeling:

- Grønn – risikoen er akseptabel
- Gul – risikoen er innenfor hva som kan tåles, men kan med fordel reduseres
- Rød – risikoen er uakseptabel. Tiltak må iverksettes.

Den oversikten man sitter med etter å ha utført risikoanalyse og risikoevaluering kalles et risikobilde. Risikobildet er et beslutningsunderlag for ledelsen som skal iverksette aktiviteter som reduserer risikoen for hendelsene som er røde og gule, samtidig som ingen av de grønne hendelsene skal få mulighet til å utvikle seg til å bli gul eller rød. Dette er risikokontroll/reduksjon.

Et mye brukt prinsipp for å jobbe med risikoreduksjon er ALARP. ALARP er akronym for As Low As Reasonably Practicable og er et prinsipp som har sitt utspring i britisk HMS-lovgivning på 1970-tallet og er knyttet til verdier for individuell risiko, IRPA[31]. Det er senere tatt inn som prinsipp i flere EU-direktiv og i standard for spesifikasjon for RAMS[32] i jernbanedrift (EN 50126).

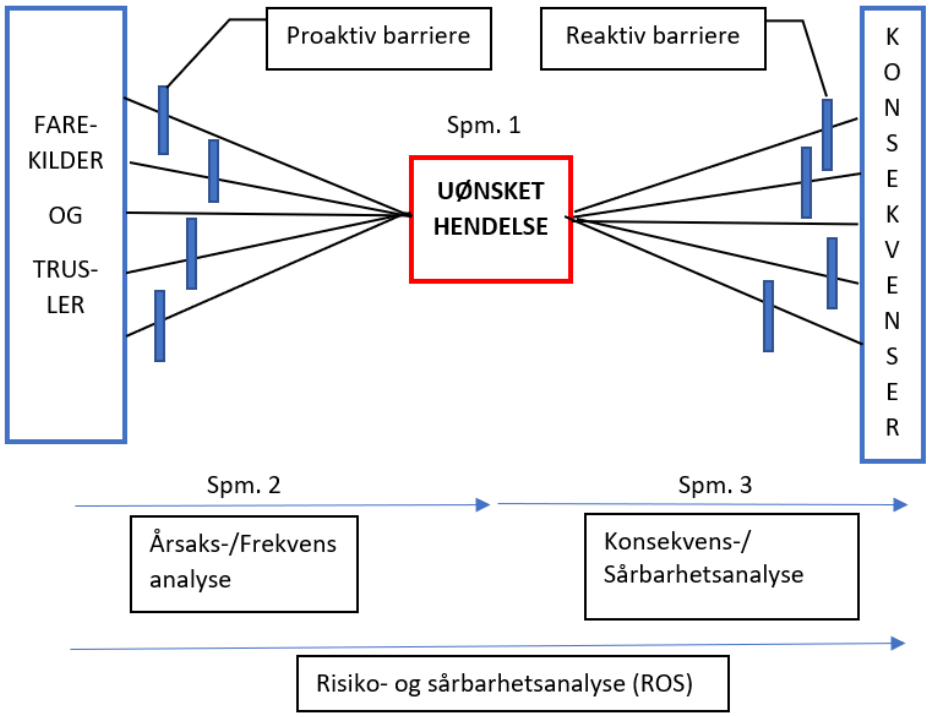


Figur 15: ALARP (basert på fig. 4.4 hos Rausand/Utne)

[31] IRPA = Sannsynligheten for at en person blir drept i en ulykke i løpet av et år (Rausand/Utne s. 55)
[32] Reliability (pålitelighet), Availability (tilgjengelighet), Maintainability (vedlikeholdbarhet), Safety (sikkerhet)

Ved bruk av ALARP defineres det en øvre og nedre grenseverdi. Risikoverdier som havner over øvre grense er uakseptable og tiltak må iverksettes. Risikoverdier som havner under nedre grense er akseptable. Risikoverdier som ligger mellom disse grensene sies å være i ALARP-området. Det skal forstås som at risikoverdien er akseptabel hvis kostnaden for å redusere den ytterligere overstiger nytteverdien av aktiviteten som medfører risikoen. Det skal jobbes med å finne risikoreduserende tiltak, men det vil være kost/nytte-analyser som avgjør om slike tiltak skal gjennomføres. Risikoen blir derfor «så lav som rimelig mulig».

En måte å visualisere sammenhengen i de ulike delene av en ROS-analyse og plassering av barrierer, er å bruke «bow-tie»-modellen (fig. 16). Her plasseres svaret på «hva kan gå galt» i boksen i midten på figuren. På venstre side plasseres farekilder og trusler som kan tenkes å bli årsak til den uønskede hendelsen. Linjene fra disse og inn til den uønskede hendelsen symboliserer årsakskjeder. På tilsvarende måte kan vi på høyre side av figuren plassere mulige konsekvenser av at den uønskede hendelsen inntraff. Linjene på denne siden symboliserer konsekvenskjeder. Gjennom risikostyringsarbeidet ønsker vi å oppnå at disse kjedene brytes ved å sette inn barrierer eller at linjene fjernes helt.



Figur 16: Bow-Tie-diagram (basert på fig. 5.4 hos Rausand/Utne)

Barrierene er et verktøy for å få kontroll med farekildene. En barriere skal hindre noe og må derfor ha en funksjon som er tilpasset det den skal hindre. Barrierefunksjoner kan være menneskelige, tekniske og/eller organisatoriske elementer som kan hindre eller gripe inn i en hendelsessekvens (Kongsvik et al.). Barrierefunksjoner kan bygges opp ved å sette sammen barriereelementer. I «bow-tie» skal barrierene i årsakskjedene hindre at den uønskede hendelsen inntreffer. Dette kalles proaktive barrierer. Hvis hendelsen inntreffer er det fordi barrieren ikke var riktig tilpasset farekilden eller at farekilden ikke var fanget opp i risikoanalysen slik at det ikke fantes noen barriere. Feiltreanalyse kan være et nyttig verktøy for å forstå årsaker hvis en proaktiv barriere ikke holder. Barrierene på høyre side av hendelsen kalles reaktive barrierer og skal hindre konsekvenser hvis den uønskede hendelsen skjer. For å finne mulige konsekvenser og egnede barrierer må det gjøres en sårbarhetsanalyse. En eventuell barrierebrist her kan analyseres ved hjelp av hendelsestre-metodikk.

Behovet for barrierer skal fremkomme gjennom risiko- og sårbarhetsanalyse (ROS). Risikobildet vil være dynamisk og derfor må barrierene også stadig vurderes og tilpasses slik at riktig barrierefunksjon er etablert. Dette kalles barrierestyring og er en del av sikkerhetsstyringen.

5.2.2. Konstruktivistisk/samfunnsvitenskapelig kunnskapssyn

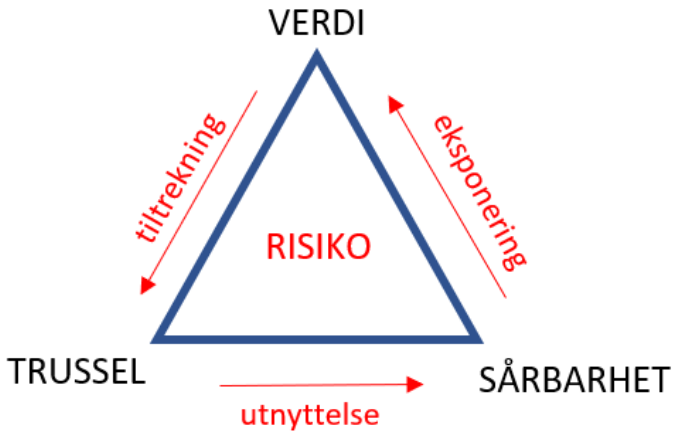
En annen måte å beskrive risiko på finnes i det konstruktivistisk/samfunnsvitenskapelige kunnskapssynet. Dette handler om hvordan framtiden forstås og tolkes av individer. I stedet for at risiko regnes ut blir den forstått og konstruert i samspillet mellom enkeltindivider, grupper og organisasjoner.

Det er ikke alltid hensiktsmessig å benytte bow-tie-modellen til å vurdere risiko og sårbarhet relatert til en uønsket hendelse. F.eks. ved hendelser som har et aspekt av tilsiktet uønsket handling vil det ofte være utfordrende å tallfeste risiko og konsekvens.

Innenfor samfunnsfaglig tilnærming til risiko finnes begrepet sikringsrisikostyring. Dette handler om hva som kan lede til villede/tilsiktede uønskede handlinger og hva vi kan gjøre for å forhindre dem eller redusere konsekvensen av dem. Mens vi ifm. bow-tie snakket om hendelser snakker vi nå om handlinger. Relevante teorier her er rutineaktivitetsteorien (Cohen & Felson, 1979) og APT-teorien (Manunta, 1999). Cohen/Felson sier at for at en uønsket

tilsiktet handling skal skje må tre forhold være oppfylt. Det må være et passende mål, en motivert gjerningsperson og fravær av beskyttelse. Hvis en av disse endres vil ikke handlingen skje. Manunta bygger på Cohen/Felson og sier at sikring er en funksjon av, dvs. samspillet mellom, A, P og T. Her er A = verdien som skal beskyttes (asset). P = den som beskytter verdien (protector). T = trusselaktøren (threat). Dette samspillet foregår innenfor en sammenheng som kalles sikringskonteksten, og tiltakene beskytteren iverksetter for å beskytte verdien kalles sikringsprosessen. Hvis en av faktorene (A, P, T) mangler bortfaller sikringskonteksten og sikringsprosessen blir med det unødvendig.

Disse teoriene er med å danne grunnlaget for trefaktormodellen som vi finner i NS 5832. Her fremstilles risiko som en kvalitativ vurdering basert på de tre faktorene verdi (V), trussel (T) og sårbarhet (S). Dette fremstilles gjerne som en trekant som vist i fig. 17.



Figur 17: Risiko basert på vurdering av verdi, trussel og sårbarhet

Risiko beskrives her gjennom å gjøre en verdivurdering, en trusselvurdering og en sårbarhetsvurdering. De røde pilene illustrerer at en trusselaktør utnytter sårbarhetene, verdiene eksponeres gjennom sårbarhetene, og eksponerte verdier tiltrekker seg trusselaktører.

Vi finner denne tilnærmingen til risiko hos flere statlige aktører med oppdrag relatert til samfunnssikkerhet. PST[33], NSM[34] og POD[35] ga i 2015 ut en felles veileder til terrorsikring som

[33] Politiets Sikkerhetstjenesten
[34] Nasjonal Sikkerhetsmyndighet
[35] Politidirektoratet

er basert på trefaktormodellen. NSMs egen veileder, risikovurdering for sikring fra 2016, er også basert denne modellen.

I FFI-rapport 2015/00923 gjør forfatterne en sammenlikning av de to tilnærmingene til risiko. FFI tar utgangspunkt i de to standardene NS 5814 og NS 5832, samt hvordan Forsvarsbygg har omsatt disse til praksis i sin virksomhet. FFIs konklusjon er at disse i bunn og grunn er veldig like, men at de er forskjellige i hvordan risiko presenteres. NS 5814 er konkret på hva risiko er (sannsynlighet x konsekvens), mens NS 5832 ikke sier noe om hvordan man kommer seg fra vurderingene av V, S og T til beskrivelse av risikoen.

5.3. Sårbarhet

Sårbarhet handler om mulige negative konsekvenser av inntrufne uønskede hendelser. Spissformulert kan vi si at det gjør ingenting å være sårbar så lenge det ikke skjer noe uønsket, men så lenge det ikke skjer noe vil også bevisstheten om egen sårbarhet lett svinne hen. Skulle derimot en uønsket hendelse eller handling inntreffe, vil omfanget av konsekvensene som regel være en funksjon av graden av sårbarhet. Sårbarhetsutvalget definerte sårbarhet som et uttrykk for 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. System skal her forstås i et videre perspektiv en rent teknisk. Det kan godt være et helhetlig MTO-perspektiv[36]. Etter dette kan sårbarhet knyttets til problemer med å gjenoppta normal virksomhet og med det være et uttrykk for tap av verdi. Sårbarhet henger derfor sammen med uønsket hendelse slik dette begrepet er definert hos Rausand/Utne. Ofte brukes begrepet robust for å beskrive det motsatte av sårbart.

Relatert til «bow-tie» er vi nå på høyre side av figuren, altså det som utvikler seg til konsekvenser når den uønskede hendelsen har skjedd. Konsekvensene forsøkes unngått ved å sette inn reaktive barrierer. Barrierefunksjonene identifiseres gjennom sårbarhetsanalyser. Hvor godt vi lykkes med barrierestyringen bestemmer derfor grad av konsekvenser og hvor sårbare vi er for den aktuelle uønskede hendelsen. Sårbarhetsutvalget sier derfor at sårbarhet i stor grad er selvforskyldt. Innenfor samfunnssikkerhet vil gjerne de reaktive barrierene ta form av beredskapstiltak. Beredskap kan defineres som alle tiltak som skal bidra til å hindre at farlige

[36] Menneske – Teknologi – Organisasjon

situasjoner får utvikle seg til ulykker, eller tiltak som skal redusere konsekvensene av inntrufne ulykkeshendelser (Njå et al., 2020).

En sårbarhetsanalyse innebærer å identifisere, tallfeste og prioritere sårbarhetene i et system (FFI 2015/00923). Virksomheten må kartlegge ulike forhold ved sin organisasjon, sine systemer, bygg og anlegg og deretter vurdere i hvilken grad dette kan skades ved en hendelse eller være interessant å ødelegge for en angriper. Barrierefunksjonene må styrke systemene eller kunne stanse en angriper.

5.4. Ulykkesmodeller og kaskadeeffekter

Sikkerhetsstyringens hensikt er å etablere et sikkerhetsnivå som er godt nok til at sannsynligheten for at uønskede hendelser og ulykker inntreffer er innenfor akseptkriteriene virksomheten har definert. Så lenge det foregår en aktivitet vil risikonivået imidlertid aldri være null og derfor vil sannsynligheten for at det skal skje en ulykke heller ikke være null. Det finnes en rekke teorier/modeller rundt hvordan ulykker kan forstås. Ulykkesmodeller kan deles inn i tre kategorier (Hovden et al., 2010) som også representerer en utvikling over tid fra enkelt til mer komplekst og sammenkoblet:

- Enkle, lineære årsaks-virkningsmodeller med fokus på tekniske feil og feilhandlinger som årsaker til ulykker.
- Komplekse, lineære modeller som vektlegger sammenfall mellom aktive feil og latente svakheter som gjør at mange barrierer svikter samtidig.
- Ikke-lineære, systemiske modeller der ulike faktorer samvirker på uforutsette eller uforutsigbare måter i tett sammenkoblede systemer der det kan oppstå forsterkende effekter.

Et eksempel på teori i den første gruppen er energi/barriere-perspektivet. Teorien sier at ulykker oppstår når energi kommer på avveie og slik kan påføre sårbare objekter skade. Energi med potensial til å forårsake skade kalles en farekilde. Ulykker unngås ved å bygge barrierer som kontrollerer farekildene. Haddons ti strategier for å kontrollere farekilder er knyttet til dette perspektivet (Haddon, 1973).

Et eksempel på teori i den midterste gruppen er James Reasons «sveitserostmodell» (Reason, 2000). Modellen sier at barrierer ikke er perfekte. De kan betraktes som skiver av sveitserost

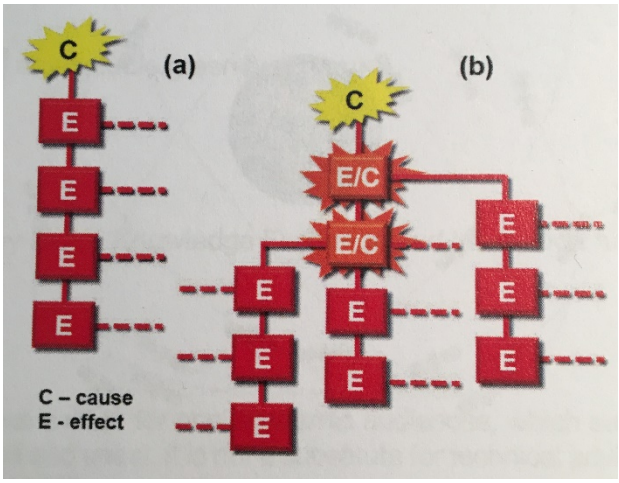
med hull. En ulykke inntreffer når disse hullene havner rett overfor hverandre slik at de etablerte barrierene svikter samtidig. Reason mener det ikke er hensiktsmessig å «skylde på» menneskelige feilhandlinger når noe skjer. I stedet bør feilhandlinger betraktes som en konsekvens av et sosioteknisk system.

Et eksempel på teori i den siste gruppen er Charles Perrows teori om uunngåelige, eller normale, ulykker (Perrow, 1999). Perrow mener enkelte systemer har utviklet seg på en slik måte at det ikke er til å unngå at en ulykke før eller siden vil skje. Dette er gjerne komplekse systemer med det Perrow kaller tette koblinger. Med tette koblinger kan små feil resultere i store ulykker. Hvis flere feil oppstår kan disse virke sammen og skape en uforutsett effekt med større skadepotensial enn hva hver enkelt feil alene ville forårsaket. Hvis det inntreffer en feil et sted i systemet kan feilen forplante seg raskt og ukontrollert gjennom systemet og føre til større ulykker.

Slik samfunnet har utviklet seg med økt kompleksitet, mange grensesnitt mellom aktører og uoversiktlige digitale verdikjeder, er Perrows teori sentral for samfunnssikkerhet. Teorien beskriver begrensninger i organisasjoners og samfunnets evne til å forutse og organisere arbeidet med risiko og sikkerhet. Perrow påpeker at det ikke er slik at teknologier tvinges på samfunnet. Det er vi mennesker som bestemmer om teknologier skal finansieres, utvikles og organiseres (Engen et al., 2016).

5.4.1. Kaskadeeffekter

Når en hendelse eller ulykke inntreffer kan det utløse en kjede av nye hendelser som kan være av en mer alvorlig art enn den utløsende hendelsen. Kaskadeeffekt kan defineres som den dynamikken som finnes i ulykker som gjør at en fysisk hendelse, en teknisk eller menneskelig feil generer en serie av hendelser i menneskeskapte sub-systemer som resulterer i fysisk, sosial eller økonomisk ødeleggelse (Pescaroli & Alexander, 2015). Kjeder av hendelser kan være lineære eller komplekse. I en lineær kjede følger hendelsene etter hverandre som årsak og



Figur 18: Lineær og kompleks kaskade (kilde: Pescaroli et al. 2019, fig.2)

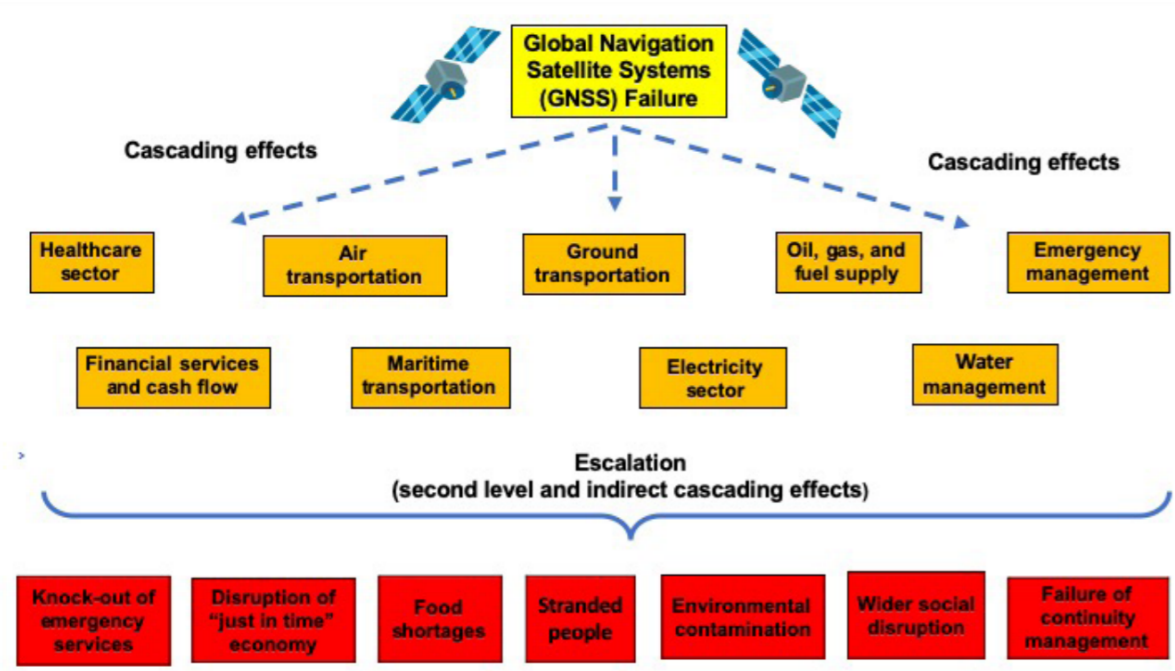
en serie av konsekvenser. Det kan også være en kompleks kjede der en konsekvens av den første årsaken blir å betrakte som årsak til at en ny kjede starter. Kaskadeeffekter er i større grad relatert til teknisk og samfunnsmessig sårbarhet enn til omfanget av den utløsende hendelsen.

Kjeder av hendelser som utløses ved en potensiell svikt ved GNSS er høyst relevant for samfunnssikkerhet. I en rapport fra britiske Institute of Risk and Disaster Reduction ved UCL[37] gjør forfatterne en overordnet analyse av dette (Pescaroli et al., 2019). Forfatterne tar utgangspunkt i en rapport fra MSD («Sveriges DSB») som slår fast at nøyaktig tid og posisjon er de to essensielle funksjonene fra GNSS, og går gjennom kilder til mulig svikt i GNSS. Den viktigste utfordringen ved svikt i GNSS er at bruk av GNSS er knyttet opp mot moderne tekniske løsninger, samtidig som organisatorisk resiliens vil bety å ha evne til å bruke reserveløsninger som ofte oppfattes som «low-tech». Det er komplisert å innarbeide slik kontinuitet og resiliens på grunn av tre forhold:

- Just-in-time-økonomi har ikke rom for redusert hastighet i verdikjedene
- På grunn av kostnadskutt blir ikke gamle løsninger videreført som «back-up»
- Kompetanse på å bruke reserveløsningene forsvinner fra organisasjonen

GNSS-avhengigheter, som avhengighet av nøyaktig tid, er vanskelige å få satt på dagsorden fordi de er ukjente for de som faktisk har gjort seg avhengig. Det gjør at mulige konsekvenser av svikt i GNSS er krevende å kommunisere fordi de fremstår som «skjulte». Kaskadekjeder som starter med GNSS-feil og får effekt på samfunnet kan illustreres slik:

[37] UCL = University College London



Figur 19: Mulige kaskadeeffekter på samfunnsfunksjoner ved svikt i GNSS (kilde: Pescaroli et al. 2019, fig. 3)

For transportområdet identifiseres kaskadeeffekter som redusert transportkapasitet, lavere tilgjengelighet på varer, økt belastning på redningstjenesten pga. fly og båter i nød, isolasjon av øysamfunn, feil i tidsangivelser, svikt i telekom, osv.

6. SAMFUNNSSIKKERHET

Utover 2000-tallet har det kommet en rekke NOU[38]-er, stortingsmeldinger, statlige strategier og veiledere som omhandler ulike sider av samfunnssikkerhet. Dokumentene gjenspeiler en utvikling fra kald krig til et digitalisert, sivilt samfunn. De har i stor grad preget det offentlige Norges fokus på samfunnssikkerhet og bidratt til utviklingen av begreper, offentlige instansers roller og ansvar, og identifisering av hva som regnes som kritisk infrastruktur og kritiske samfunnsfunksjoner.

I dette kapitlet ser jeg først kort på historisk utvikling av samfunnssikkerhetsbegrepet og går deretter gjennom de publikasjonene som jeg har vurdert som mest sentrale for oppgavens problemstilling. Jeg har satt fokus på utvikling av begreper, ansvarsforhold og hva som sies om sammenheng mellom samfunnssikkerhet, digitalisering, transport og satellittbaserte tjenester. Hensikten er å få en dypere forståelse av hva som egentlig menes når det hevdes at samfunnssikkerhet er avhengig av transport og satellittbruk. Dette vil jeg bruke som fundament for utarbeidelse av intervjuguide og gjennomføring av faktainnsamling.

6.1. Betydning av begrepet – de lange linjer

Samfunnssikkerhet som begrep har vært under utvikling i mange år og er heller ikke i vår tid et klart definert faguttrykk. Likevel er det et mye brukt begrep som er med å styre politiske prioriteringer. Bruk av sikkerhetsbegrepet i politisk sammenheng kan dokumenteres tilbake til Romerriket og Pax Romana (Engen et al., 2016) med betydning statens sikkerhet mot ytre fiender og statens evne til å skape sikkerhet for sine innbyggere. Med statsdannelser i Europa på 1600- og 1700-tallet oppsto begrepet securitas publicas – offentlig sikkerhet. I dette lå krav og forventning om at fyrsten hadde ansvar for folkets sikkerhet. Krav på sikkerhet flyttes gradvis fra det kollektive til individet.

I 1775 ble hovedstaden i Portugal, Lisboa, utsatt for et kraftig jordskjelv som antas å ha tatt nær 100 000 menneskeliv. Franskmannen Voltaire skal ha stilt spørsmål ved hvorfor det ble bygget så høye hus i et jordskjelvutsatt område. Ulykken i Lisboa, og Voltaires spørsmål, betraktes som opphavet til sikkerhetsvitenskapelig tenkning (Engen et al., 2016). Hendelsen inntraff på

[38] Norsk Offentlig Utredning

høyden av opplysningstiden og det ble søkt etter vitenskapelige forklaringer i stedet for å slå fast at ulykken var en straff fra Gud. Portugals statsminister iverksatte omfattende kartlegging av forløp og skader for å lage en faktabasert forståelse av hva som hadde foregått.

Naturkatastrofer ødelegger og tar fra oss ting som er med på å skape trygghet i hverdagen. Med dette kan sikkerhet sees på som en forventning om å beholde det man har. Hendelsen i Lisboa var med på å danne utgangspunktet for en gryende forsikringsbransje basert på ny lærdom om at folk er villige til å betale for å kunne få tilbake det som skaper sikkerhet og trygget.

Fremveksten av selvstendige stater på 1700- og 1800-tallet påvirket forståelsen av sikkerhetsbegrepet. Begrepet «statens interesser» ble knyttet til samfunnssikkerhet gjennom totalforsvarskonseptet. En stats sikkerhet handlet i all hovedsak om å trygge seg selv mot angrep fra en ytre fiende. Et sterkt militært forsvar ble sett på som en forsikring. Etter første verdenskrig og opprettelse av Folkeforbundet ble denne problemstillingen snudd på hodet: Hvordan kan en stat trygge egen sikkerhet uten å øke andres risiko eller usikkerhet?

Folkeforbundet (1920-1946) lyktes ikke i å forhindre annen verdenskrig. Etter krigen, i 1948, ble FN opprettet med målsetting om å forhindre krig og sikre fred gjennom politisk press eller direkte intervensjon. Gjennom en kald krig og stormaktenes vetorett i sikkerhetsrådet, ble FNs handlingsrom på dette området begrenset. I stedet engasjerte FN seg innenfor en rekke andre områder som også bidrar til å stabilisere samfunn og gjøre dem trygge. Et eksempel er å skape sikkerhet gjennom utvikling og deling av kunnskap mellom landene og anerkjenne viktigheten av å beskytte nasjonenes egenverdi og kulturelle uttrykk (Engen et al., 2016).

I Norge, som ellers i Europa, satte den kalde krigen sitt preg på de første 40-50 årene etter annen verdenskrig. Nasjonal sikkerhet ble et begrep i denne tiden. Samfunnets sikkerhet ble knyttet til å beskytte landet mot militær aggresjon fra Warszawapakten og ble preget av allmenn verneplikt, NATO-medlemskap og et norsk forsvar som øvde på å motstå angrep fra Sovjetunionen. Forsvarskommisjonen av 1946 slo fast at det var viktig for sikkerheten at det ble etablert et fungerende samspill mellom militære og sivile funksjoner, det såkalte totalforsvaret. Mange forhold relatert til sivil samfunnsplanlegging ble av denne grunn integrert i beredskapshensyn utover etterkrigstiden. Det sivile samfunnets ressurser skulle være en støtte for det militæret forsvaret. Statens ansvar for å beskytte sivilbefolkningen kom til uttrykk ved sivilforsvarets oppgaver og myndighetskrav til tilfluktsrom.

Lund-kommisjonen (Stortinget, 1996) dokumenterte i 1996 at statens sikkerhet i disse årene hadde blitt brukt som argument av de hemmelige tjenestene til å registrere og overvåke norske sivile borgere som hadde plassert seg på venstresiden i det politiske landskapet. Den kalde krigen var en periode der statens sikkerhet godt kunne bli satt foran individets personvern. Statens fokus var rettet mot ytre fiender, men også mot norske borgere som kunne tenkes å utgjøre støttespillere for trusselen utenfra.

Rundt århundreskiftet endret dette seg med Berlin-murens fall i 1989, Sovjetunionens oppløsning i 1991 og terroren i USA 11. september 2001. Den tradisjonelle ytre fienden forsvant. I den nye situasjonen var det andre typer krefter som kunne utgjøre en fare for samfunnet. Terror fundamentert i religion, men også naturkreftenes ødeleggelser av samfunnsinfrastruktur, fikk mer fokus. Den såkalte nyttårsorkanen[39] i 1992 og flommen på Østlandet[40] i 1995, bidro til dette. Disse forholdene hadde mer karakter av å være indre, egenproduserte farer og trusler mot samfunnets sikkerhet. At uvær, flom og skred fikk fokus relatert til samfunnssikkerhet var samtidig en konsekvens av økt kompleksitet i samfunnet og økt forståelse av hvorfor ulykker oppstår (Engen et al., 2016).

Samfunnssikkerhet ble både et fagfelt og et politisk begrep. Der hvor ingeniørene hadde fått råde grunnen nærmest alene, fikk de nå selskap av samfunnsvitere og psykologer. Disse bidro med teorier som knyttet mennesker, teknologi og organisasjon til samfunnssikkerhetsbegrepet. Samfunnssikkerhet har blitt et flerfaglig emne og ulike fagdisipliner vil kunne legge ulike ting i begrepet. Samfunnssikkerhet som begrep ble første gang definert i St. meld. 17 (2001-2002) som den evne samfunnet har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjennelser (JD, 2002).

6.2. Utvikling av begrepet – nyere tid i Norge

6.2.1. Et sårbart samfunn

Bondevik-I-regjeringen satte i september 1999 ned et utvalg som skulle utrede samfunnets sårbarhet med sikte på å styrke samfunnets sikkerhet og beredskap. Utvalget ble ledet av tidligere statsminister Kåre Willoch, og det omtales som Willoch-utvalget eller Sårbarhetsutvalget. Utvalgets rapport ble publisert 4. juli 2000 som NOU 2000:24, *Et sårbart*

[39] https://no.wikipedia.org/wiki/Nytt%C3%A5rsorkanen_i_Norge_i_1992 (besøkt 2020-08-29)
[40] https://no.wikipedia.org/wiki/Flommen_p%C3%A5_%C3%98stlandet_1995_(Vesleofsen) (besøkt 2020-08-29)

samfunn. (JD, 2000). Utvalget fikk i oppdrag å gjøre «…vurderinger knyttet til den økende sårbarheten i samfunnet for avbrudd i viktige forsyninger av varer og tjenester som følge av menneskelige feil, tekniske sammenbrudd, naturkatastrofer, terror, sabotasje eller krigshandlinger».

Utvalget bruker hyppig begrepet samfunnssikkerhet i rapporten, men definerer det ikke. Utvalget har lagt disse definisjonene til grunn for en rekke sentrale begreper:

- *Risiko*: en funksjon av sannsynligheten for mulige uønskede hendelser og konsekvensene av disse. Risiko uttrykker fare for tap av viktige verdier som følge av uønskede hendelser.
- *Trussel*: et hvert forhold eller enhver enhet med potensiale til å forårsake en uønsket hendelse
- *Sårbarhet*: et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet år med å gjenoppta sin virksomhet etter at hendelsen har inntruffet.
- *Krise*: en hendelse som har potensiale til å true viktige verdier og svekke organisasjonens evne til å utføre viktige funksjoner.
- *Kritisk infrastruktur*: systemer, som når de ikke fungerer, vil ha en sterkt negativ effekt på samfunnet.

I definisjonen av risiko kan det se ut til at utvalget legger et realistisk kunnskapssyn til grunn. Det kommer imidlertid fram i rapporten at utvalget er bevisst på at det i flere sammenhenger vil være nær umulig å foreta matematiske beregninger fordi det ikke finnes noe relevant statistikk å ta utgangspunkt i. Utvalgets syn på sårbarhet er at det i de fleste tilfeller er selvforskyldt og representere et mulig tap av verdi.

I utredningen presenteres de tre prinsippene for sikkerhets- og beredskapsarbeidet i Norge. De forklares slik:

- *Ansvarsprinsippet*: Den virksomhet som har ansvaret for en sektor, har også ansvaret for nødvendig skadeforebyggende tiltak, beredskapsforberedelser og iverksettelse av tiltak i kriser og krig.

- *Likhetsprinsippet*: Det skal være størst mulig likhet mellom organisering i fred, krise og krig. Begrunnelsen for dette er at den som utfører samfunnsoppgaven i fred, også har de beste forutsetninger for å håndtere oppgavene i kriser og krig.
- *Nærhetsprinsippet*: Kriser skal håndteres på lavets mulig nivå.

Sårbarhetsutvalget mener at endringen i trusselbildet må få følger for hvilke prioriteringer som legges til grunn for beredskapen i det sivile samfunnet. Her tar utvalget i bruk begrepet *samfunnsverdier* og sier at samfunnet skal sikres mot det som kan utgjøre utfordringer mot sentrale samfunnsverdier. Samfunnsverdier er ifølge utvalget: liv, folkehelse og velferd, livsmiljøet, det demokratiske systemet, nasjonal styringsevne og suverenitet, landets territoriale integritet, materiell og økonomisk trygget og kulturelle verdier.

Utvalget har gjort en kvalitativ vurdering av hvilke temaer som har betydning for samfunnet og som kan være relevante som trusler mot samfunnsverdiene. Fra en liste på 13 temaer er det her relevant å fremheve IKT, transport av mennesker, varedistribusjon og transport av farlig gods.

Utvalget slår fast at sikkerhets- og beredskapsarbeidet i Norge er preget av sterkt fragmentert ansvar og organisering og at det tilsynelatende er liten politisk interesse for den sivile beredskapen. For å få til gode helhetlige løsninger i samfunnet og etablere en aktør som kan samordne samfunnssikkerhets- og beredskapsarbeidet, foreslår utvalget å etablere et nytt departement som skal ha ansvar for alt ikke-militært arbeid for sikkerhet og beredskap. Utvalget foreslår også å opprette en nasjonal sikkerhetsmyndighet ved å dele opp Forsvarets sikkerhetstjeneste og legge den nye etaten under dette departementet. Dette er bakgrunnen for dagens NSM.

Utvalgets vurderinger for transportsektoren er at trusselbildet er knyttet til stengte veier, ulykker med farlig gods, tunellbranner og flyulykker på kortbanenettet. Svikt i telesystemer antas å ha liten effekt for vegtransporten, men betydelig større effekt for flytransport og jernbane. Vurderingen bør nok sees i lys av at det på 1990-tallet var flere store flyulykker som Namsos[41],

[41] Widerøe havarerte under innflyging til Namsos lufthavn 27. oktober 1993. Seks personer omkom.

Operafjellet[42] og Norne[43], samt at jernbaneulykkene på Åsta[44] og Lillestrøm[45] inntraff mens utvalget var i arbeid.

En mindre regulert sektor som utsettes for åpen konkurranse og kostnadspress, antar utvalget vil kunne ha en negativ utvikling på sikkerhetsnivået. Utvalget slår fast at ordningen med transportberedskapsorganisasjonen, som var basert på totalforsvarstankegangen der myndighetene kan kontrollere nasjonale transportaktører, er utgått på dato og derfor bør avvikles. Da denne NOU-en ble utgitt hadde GPS vært operativt i 5 år og var nok mest kjent blant navigatører og ingeniører. Ordet satellittnavigasjon er nevnt ett sted i rapporten i omtalen av Sleipner-ulykken[46] i 1999.

6.2.2. Når ulykken er ute

Stoltenberg-I-regjeringen nedsatte et utvalg som skulle vurdere organiseringen av de operative rednings- og beredskapsressursene. Utvalgets rapport ble publisert som NOU 2001:31, *Når ulykken er ute* (JD, 2001). Utvalgets hovedkonklusjon ble at det ikke ville anbefale noe omstrukturering av betydning. Utvalget hadde også vurdert om det burde opprettes en sentral krisehåndteringsmyndighet, men ville heller ikke anbefale dette.

6.2.3. Veien til et mindre sårbart samfunn

For å følge opp Sårbarhetsutvalgets utredning kom Bondevik-II-regjeringen med St.meld. nr. 17 (2001-2002), *Samfunnssikkerhet – veien til et mindre sårbart samfunn*, i april 2002 (JD, 2002). I tiden mellom Sårbarhetsutvalgets rapport og denne stortingsmeldingen hadde terroren i USA 11. september 2001 skjedd. Dette setter sitt preg på meldingen og innledningsvis skriver regjeringen at terrorhendelsen viser at utviklingen i et moderne samfunn krever en sterkere oppmerksomhet om hvilke trusler vi kan tenkes å stå overfor. Videre fremkommer det at regjeringen har tre hovedmål for samfunnssikkerhetsarbeidet i Norge:

1. Effektiv forebygging av kriser og alvorlig svikt i samfunnskritiske funksjoner
2. Effektiv håndtering av kriser
3. God organisering av samfunnets beredskapsapparat

[42] Vnukovo Airlines havarerte under innflyging til Svalbard lufthavn 29. august 1996. 141 personer omkom
[43] Helikopter Service AS havarerte på Nornefeltet 8. september 1997. 12 personer omkom.
[44] To tog kolliderte ved Åsta i Østerdalen 4. januar 2000. 19 personer omkom.
[45] To godstog kolliderte på Lillestrøm stasjon 5. april 2000. Stor eksplosjonsfare. 2000 personer evakuert.
[46] Ulykke med hurtigbåten «MS Sleipner» ved Store Bloksen i november 1999. 16 mennesker omkom.

Samfunnskritiske funksjoner defineres her som funksjoner samfunnet er svært avhengig av for å kunne opprettholde ordinær drift. For å oppnå disse målene vil regjeringen sette fokus på kontinuitet i dette arbeidet slik at tiltak for å sikre samfunnet ikke skal være styrt av inntrufne hendelser, men bygge på vurderinger av farer samfunnet kan stå overfor. Terrorhendelsen i USA tas til inntekt for at samfunnssikkerhetsarbeidet i større grad må ta hensyn til at andre enn statlige aktører kan være i stand til å påføre samfunnet stor skade. Det blir satt fokus på terrorisme og organisert kriminalitet.

Regjeringen velger her en bred tilnærming til sikkerhetsbegrepet. Den skriver at begrepet omfatter alle relevante kategorier av tiltak som har til hensikt å unngå uønskede hendelser eller tilstander og begrense konsekvensene om disse skulle inntreffe. Sikkerhet er derfor ikke bare en tilstand, men også tiltakene for å oppnå denne tilstanden. I denne stortingsmeldingen defineres samfunnssikkerhetsbegrepet som en evne samfunnet har:

- *Samfunnssikkerhet*: et begrep som beskriver den evne samfunnet som sådan har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger.

Sammenliknet med Sårbarhetsutvalget ser vi at ordet krig nå er borte og det snakkes kun om kriser. Regjeringen slår fast at de tre prinsippene for sikkerhet-/beredskapsarbeid gjelder for både årsaksreduksjon og konsekvensreduksjon. Relatert til «bow-tie»-modellen betyr dette at samfunnssikkerhetsarbeidet i Norge skal omhandle arbeidet på begge sider av den uønskede hendelsen og omfatte både proaktive og reaktive barrierer.

Stortingsmeldingen har et eget kapittel om transportsikkerhet. I begrepet transportsikkerhet legges det her to ting: hindre storulykker og sikre transportberedskap ved krise og krig. Det refereres til FFIs pågående arbeid med BAS[47]-4 (utgitt juni 2003 som FFI-rapport 2003/00929) som omhandler sårbarhetsreduserende tiltak innen transport. Fokuset i meldingen er på organisering av tilsyn i samferdselssektoren og reservedelslager for transportberedskap.

6.2.4. Sivilt-militært samarbeid

Bondevik-II-regjeringen kom med St.meld. nr. 39 (2003-2004), *Samfunnssikkerhet og sivilt-militært samarbeid,* i mai 2004 (JD, 2004). Hensikten med denne meldingen er hovedsakelig

[47] Beskyttelse av Samfunnet. En serie av prosjekter hos Forsvarets Forskningsinstitutt

oppfølging av resultatet av Stortingets behandling av den forrige meldingen (Innst. S. nr. 9 (2002-2003)). Stortinget ønsket blant annet å ha en ordning med parallell behandling av langtidsplaner for Forsvaret og sivilt beredskap og det påla også regjeringen å utrede en sentral krishåndteringsenhet. Stortinget valgte her annerledes enn anbefalingen i NOU 2001:31.

Regjeringen ønsket med denne meldingen å si hva den mente skulle være *totalforsvarets rolle* i en ny tid med et nytt trusselbilde, og hvilken form sivilt-militært samarbeid skulle ha. Det fremgår at det er seks forhold som skal vektlegges i samfunnssikkerhetsarbeidet:

1. Forebyggende virksomhet, herunder HMS
2. Sikring av nød- og beredskapsetatenes evne til å håndtere større hendelser, herunder terror
3. Målrettet og samordnet arbeid for å sikre samfunnskritisk infrastruktur
4. Økt samarbeid, herunder planverk og øvelser, mellom sivile og militære myndigheter
5. Styrking av etterretnings- og sikkerhetstjenestens evne til å analysere, varsle og forebygge ulike former for terror i Norge
6. Helhetlig og samordnet krisehåndtering sentralt, regionalt og lokalt.

Fokuset er på håndtering av terror og sikring av infrastruktur. Det er interessant å se hva regjeringen skriver her om totalforsvaret sammenliknet med forsvarskommisjonen av 1946. Den gang skulle det sivile samfunnets ressurser støtte det militære forsvaret. Det var snakk om bistand kun én vei. Nå omtales totalforsvaret som et samarbeid og en toveis gjensidig støtte. Forsvaret skal bidra til samfunnets sikkerhet også i situasjoner der rikets sikkerhet ikke er truet[48]. Når det gjelder motsatt vei, det sivile samfunns støtte til Forsvaret, skriver regjeringen at det handler om leveranse av varer og tjenester.

På grunn av de store kuttene i Forsvaret har ikke etaten lenger behov for at det finnes store kvanta på sivile lager. Det sivile samfunns leveranser skal dekkes gjennom et normalt fungerende marked. Dette siste er særlig interessant for det legger til grunn at samfunnets markedsdrevne forsyningslinjer fungerer normalt i en krisesituasjon. At det ikke nødvendigvis er sånn har vi nylig sett et eksempel på relatert til beredskapslagre av smittevernutstyr under corona-pandemien.

[48] Eksempel på dette er Forsvarets bistand ifm. kvikkleireraset i Gjerdrum i desember 2020. Forsvaret bisto med søk- og redningskapasitet, vaktmannskaper og broleggingssystemer.

Meldingens kapittel 10 omhandler sikkerhets- og beredskapsarbeid innen enkelte sektorer. Regjeringen skriver at transportsektoren står overfor store utfordringer relatert til transportberedskap. Det pågår arbeid for å modernisere beredskapsordningene med tanke på større kriser i fred og internasjonale regler mot terrorisme. Regjeringen vil blant annet prioritere fredskriseberedskapen innen alle transportgrener, videreutvikle planverk og ROS-analyser og sikre en helhetlig oppfølging av sikkerhet og beredskap på tvers av transportgrener.

6.2.5. Når sikkerheten er viktigst

Infrastrukturutvalgets rapport ble publisert i april 2006 som NOU 2006:6, *Når sikkerheten er viktigst* (JD, 2006). Utvalget skriver at truslene mot samfunnet har endret karakter og har et potensial for å true samfunnets sikkerhet ved at samfunnets sårbarhet er endret. Potensielle trusler har blitt mer uoversiktlig og har potensial til å ramme kritisk infrastruktur og kritiske samfunnsfunksjoner. På grunn av økt avhengighet av teknologiske løsninger, ny teknologi og nye måter å organisere virksomheter på, har samfunnets sårbarhet endret seg. Virksomhetenes sikkerhets- og beredskapsarbeid må baseres på trussel- og ROS-informasjon og utgjøre en integrert del av virksomhetens risikostyring. Utvalget er på linje med Sårbarhetsutvalget når det sier det er en fordel at det offentlige eier samfunnets kritiske infrastruktur.

Kritiske infrastrukturer kan være gjensidig avhengig av hverandre og svikt kan dermed få en sektorovergripende karakter. Ved svikt er ikke samfunnet i stand til å opprettholde de leveranser av varer og tjenester som befolkningen er avhengig av. Utvalget har gått grundig inn i begrepet kritisk infrastruktur og har utarbeidet sin egen definisjon der det knytter infrastruktur og samfunnssikkerhet sammen med det å føle trygghet:

- *Kritisk infrastruktur*: de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse.

I rapporten skilles det tydelig mellom kritisk infrastruktur og *kritiske samfunnsfunksjoner*[49]. Forskjellen kommer fram i den trinnvise metoden utvalget har laget for å identifisere kritisk infrastruktur. Det skal først identifiseres hva som er samfunnets grunnleggende behov. Kritiske samfunnsfunksjoner vil være de samfunnsfunksjonene som må til for å dekke disse behovene.

[49] Kritiske samfunnsfunksjoner skal forstås som synonymt med samfunnskritiske funksjoner

Kritisk infrastruktur vil være infrastrukturer som må være på plass for at disse funksjonene skal fungere under forutsetning av at det ikke finnes alternativer til dem, at de er tett koplet, og at store grupper er avhengig av dem. «Tett koplet» skal her forstås i henhold til teorien til Perrow. Ved bruk av denne metoden har utvalget identifisert følgende kritiske samfunnsfunksjoner: bank og finans, matforsyning, helse- sosial- og trygdetjenester, politi, nød- og redningstjeneste og kriseledelse.

For å realisere disse funksjonene mener utvalget det trengs følgende kritiske infrastrukturer: elektrisk kraft, elektronisk kommunikasjon, vann og avløp, *transport*, olje og gass og *satellittbasert infrastruktur*.

Her er det interessante forskjeller mellom Infrastrukturutvalget og Sårbarhetsutvalget. Det Sårbarhetsutvalget kaller samfunnsverdier ser ut til å ligge på et høyere abstraksjonsnivå enn det Infrastrukturutvalget kaller samfunnsfunksjoner. Noe av det som dette utvalget kalles kritisk infrastruktur faller sammen med det Sårbarhetsutvalget har kalt tema, men disse temaene er i større grad preget av å være tjenester/funksjoner.

Utvalget mener begrepet samfunnssikkerhet kan ha en bred og en snever tilnærming. Bred tilnærming omhandler forebygging og håndtering av ekstraordinære hendelser samt å ha ressurser til å forebygge og håndtere dagligdagse hendelser. Det omfatter også å forhindre at mindre hendelser blir mange nok til å gå ut over samfunnet. Den snevre tilnærmingen av begrepet omhandler å forebygge og håndtere ekstraordinære hendelser som krever ressurser ut over det vanlige.

Blant de seks kritisk infrastrukturene som utvalget har identifisert, finnes både transport og satellittbasert infrastruktur. Utvalget skriver at hele samfunnets funksjonsdyktighet er avhengig av transport. Det settes fokus på at naturkatastrofer og terrorangrep utgjør en trussel mot infrastrukturen i de ulike transportformene og at det skaper en sårbarhet for et samfunn som i stadig større grad baserer seg på just-in-time-prinsippet.

Mange tjenester i et moderne samfunn baserer seg på bruk av data og tjenester fra satellitter. Utvalget påpeker at disse systemenes internasjonale karakter er en utfordring ettersom sikkerhetsmessige virkemidler på nasjonalt plan vil ha begrenset effekt. Funksjonssvikt i navigasjonssystemene vil kunne ha betydning for samfunnssikkerheten og den nasjonale

sikkerheten ettersom slike systemer utgjør en understøttende infrastruktur til en rekke andre infrastrukturer.

Rapportens vedlegg 11 har tittel navigasjonssystemer og samfunnssikkerhet. Det er utarbeidet av NSM og peker på tre kategorier av sårbarheter: feilkilder i systemet, feilkilder som resultat av villede handlinger og sårbarheter i bakkeinfrastrukturen. NSM skriver at mange kritiske samfunnsfunksjoner har gjort seg avhengig av GPS og at dette utgjør en sårbarhet. Det forventes at sårbarheten vil kunne bli redusert når det europeiske Galileo-systemet blir operativt.

6.2.6. Samvirke og samordning

Stoltenberg-II-regjeringen ga ut St. Meld. 22 (2007-2008), *Samfunnssikkerhet – samvirke og samordning* i mai 2008 (JD, 2008). Meldingen oppgis å ha følgende hensikter:

1. Følge opp regjeringens målsetninger i Soria-Moria-erklæringen[50] om helhetlig sikkerhetspolitikk og styrket samfunnssikkerhet
2. Følge opp Stortingets behandling av St. Meld. 39 (Innst. S. nr. 9 (2004-2005))
3. Følge opp forslag fra Infrastrukturutvalget
4. Opprettholde praksis om parallell stortingsbehandling av langtidsplaner for militært forsvar og sivilt beredskap.

I Soria-Moria-erklæringen uttaler regjeringspartiene at sikkerhetsutfordringen i mindre grad enn før er knyttet til militære trusler. Det er miljøkatastrofer, storulykker og terroranslag som utgjør mulige farer og trusler.

Stortingsmeldingen legger Infrastrukturutvalgets definisjon av kritisk infrastruktur til grunn. Som meldingens tittel tilsier er hovedbudskapet viktigheten av samarbeid og regjeringen skriver at ingen sektor alene kan forebygge, redusere, hindre eller håndtere fremtidens utfordringer innen samfunnssikkerhet. Kriseplanlegging skal være basert på best mulig kunnskapsgrunnlag, blant annet om teknologiske endringer. Regjeringen appellerer til frivillige organisasjoner og dugnadsinnsats for å lykkes med samfunnssikkerhetsarbeidet.

[50] En politisk avtale fra 2005 mellom Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti som lå til grunn for Jens Stoltenbergs andre regjering.

Ved å trekke inn dugnadsinnsats kan det se ut til at regjeringen vil relatere samfunnssikkerhetsarbeidet til sosial kapital. Sosial kapital[51] handler om hvordan borgerne i et samfunn utvikler tillitsfulle relasjoner som styrker fellesskapets evne til å løse kollektive utfordringer. Nilsen et al. har gjort en litteraturstudie og funnet at sosial kapital har potensial til å være en bidragsyter før, under og etter en katastrofehendelse (Nilsen et al., 2019).

Meldingens kap. 5 omhandler sikkerhet i kritisk infrastruktur og har et avsnitt om satellittbasert infrastruktur. Her er første gang i denne dokumentserien om samfunnssikkerhet at GNSS som kilde til *nøyaktig tid* omtales, og at dette brukes til synkronisering av data- og kommunikasjons-systemer. Det virker ikke som regjeringen er helt enig med Infrastrukturutvalget om at Galileo vil redusere sårbarheten relatert til GPS-avhengighet, og trekker i stedet fram systemet Loran-C. Det hevdes at dette er mer robust mot forstyrrelser og kan i modernisert utgave (eLoran) utgjøre en reserveløsning til satellittnavigasjonssystemene. Mastene på de norske stasjonene ble demontert vinteren 2018 etter beslutning i SD.

For transportinfrastrukturen sier meldingen at SD vil vektlegge ulykker og uønskede hendelser som kan føre til store samfunnsmessige konsekvenser. Samferdselssektorens beredskap og krisehåndteringsevne skal styrkes gjennom ROS-analyser, videreutvikling av krise-organisasjonen, planverk og øvelser.

JDs samordningsrolle trekkes frem i denne meldingen også og det er laget en 10-punktsliste over tiltak som skal styrke denne rollen. Det fremgår at Krisestøtteenheten ble etablert 1. januar 2006 og underlagt JD. Regjeringen fremhever også forskning på samfunnssikkerhet.

6.2.7. Samfunnssikkerhet grunnlag

Meld. St. 29 (2011-2012), *Samfunnssikkerhet* (JD, 2012) ble publisert sommeren 2012. Dette er første stortingsmelding relatert til samfunnssikkerhet etter terrorangrepet på regjeringskvartalet og Utøya 22. juli 2011. Regjeringen understreker at samfunnssikkerhet handler om at befolkningen skal oppleve *stor grad av trygghet*. Det skal skje gjennom:

1. Effektivt forebygge og om mulig forhindre uønskede hendelser
2. Sikre en effektiv beredskap og operativ evne og kapasitet til å håndtere alvorlig kriminalitet, kriser og ulykker

[51] https://snl.no/sosial_kapital

3. Sikre god evne til raskt å gjenopprette samfunnskritiske funksjoner dersom uønskede hendelser ikke har latt seg forebygge
4. Sikre en god læring på av inntrufne hendelser og øvelser

Meldingen har fokus på store tverrsektorielle hendelser med gjensidige avhengigheter, inkludert IKT-sikkerhet. I dette ligger utfordringen med at flere infrastrukturer er koblet sammen på tvers av landegrenser og at arbeidet med å sikre kritisk infrastruktur dermed har en grenseoverskridende faktor. Meldingen har et eget kapittel om IKT, men sier svært lite om samferdsel og satellittbruk.

Flere av de foregående utredningene/meldingene har listet de tre prinsippene for samfunns-sikkerhets- og beredskapsarbeidet. Disse tre omhandler ansvar, nærhet og likhet. I denne meldingen innfører regjeringen et nytt, fjerde prinsipp om samvirke:

- *Samvirkeprinsippet*: Myndighet, virksomheter eller etater har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeid med forebygging, beredskap og krisehåndtering.

Det nye prinsippet innføres fordi erfaring viser at de tre andre prinsippene i for liten grad kommuniserer nødvendigheten av godt samvirke mellom ulike ansvarlige aktører. Samvirkeprinsippet skal tydeliggjøre regjeringens samlede ansvar på tvers av sektorgrenser.

6.2.8. KIKS-1

I januar 2012 ga DSB ut rapporten Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner (KIKS). DSB legger til grunn St. Meld 22 og Infrastrukturutvalgets definisjon av kritisk infrastruktur og kritisk samfunnsfunksjoner. Her utredes en modell for overordnet risikostyring. Rapporten ble presentert som første delrapport fra KIKS-prosjektet og kalles følgelig «KIKS-1-rapporten». I rapporten presenteres KIKS-modellen som skal være et verktøy for å etablere en overbygning for den sektorvise risikostyringen av kritisk infrastruktur og kritiske samfunnsfunksjoner. DSB sier at hensikten med infrastrukturen er å realisere funksjonene og at det derfor er samfunnsfunksjoner som er det sentrale begrepet. Samfunnsfunksjonene brytes ned i basiskapabiliteter[52] og videre i basisleveranser. DSBs utredning ender opp med 12 kritiske samfunnsfunksjoner med til sammen 21 basiskapabiliteter.

[52] Kapabilitet er en fornorsking av engelsk capability som kan oversettes med ha evne/egenskap til å utføre noe. Store norske leksikon (https://snl.no/kapabilitet) forklarer kapabilitet som dyktighet eller yteevne. Jeg synes det

Hverken samferdsel eller satellittbaserte tjenester er nevnt i denne oversikten.

6.2.9. Digital sårbarhet – sikkert samfunn

Resultatet av Lysne-utvalgets arbeid ble publisert i november 2015 som NOU 2015:13, *Digital sårbarhet – sikkert samfunn* (JD, 2015). Utvalgets oppdrag var å kartlegge samfunnets digitale sårbarhet og vurdere hvilke konsekvenser denne sårbarheten har for samfunnssikkerheten. I mandatet pekes det særlig på sårbarheter innen kritiske samfunnsfunksjoner og kritisk infrastruktur, og det nevenes spesifikt ekom, kraftforsyning, bank- og finansielle tjenester og den gjensidige avhengigheten mellom disse.

Lysne-utvalget slår fast at utfordringene innen området er tverrsektorielle. Kritiske samfunnsfunksjoner er blitt avhengige av lange og uoversiktlige digitale verdikjeder som gjerne spenner over mange sektorer og flere land. Slike sammensatte, sektorovergripende verdikjeder finnes nå i alle kritiske samfunnsfunksjoner. Utvalgt har lagt denne definisjonen til grunn:

- *Digital verdikjede*: en struktur av leveranser mellom virksomheter hvor hver leveranse er en digital tjeneste, software eller hardware.

I rapportens del III gjør utvalget en analyse av hver av de kritiske infrastrukturene som Infrastrukturutvalget definerte. Relevant for denne oppgaven er kapitlene for satellittbaserte tjenester og transport.

Samfunnsutviklingen har gått i retning av at tjenester som utnytter infrastruktur i verdensrommet har blitt en integrert del av hverdagen og at antall samfunnsområder som blir berør av bruk av rombasert infrastruktur har økt. Utvalget tar utgangspunkt i KIKS-1-rapportens liste over 12 kritiske samfunnsfunksjoner og knytter dem opp mot GNSS som kilde til *PNT*. Av de 12 er 11 avhengig av GNSS som kilde til nøyaktig tid.

Ivaretakelse av funksjonalitet og sikkerhet knyttet til Svalbardkabelen[53] brukes som eksempel på sårbarhet knyttet til verdikjeder innen satellittbaserte tjenester. Ulike aktører og virksomheter

er et dårlig norsk ord og Njå et. al. har valgt å unngå ordet i sin omtale av KIKS. De bruker i stedet delfunksjon og funksjonsevne (Njå et al., 2020) s. 144. Jeg har likevel valgt å bruke ordet her og senere i oppgaven fordi det har blitt et relativt vanlig ord og er innarbeidet i flere offentlige publikasjoner om samfunnssikkerhet.

[53] Svalbardkabelen er en fiberkabel mellom Svalbard og det norske fastlandet. Kabelen er sentral for å overføre data som tas ned fra satellitter ved Svalsats antennepark på Platåberget.
https://en.wikipedia.org/wiki/Svalbard_Undersea_Cable_System (besøkt 2020-07-02)

er avhengig av hverandre og det er lite ende-til-ende-fokus. Det er ingen overordnet myndighet som har et helhetsbilde av hvilke samfunnstjenester som er avhengig av kabelens funksjonalitet.

For transportsektoren gir Lysne-utvalget sin tilslutning til vurderinger som er gjort av Sårbarhetsutvalget og Infrastrukturutvalget. Utvalget påpeker at digitaliseringen har gitt en økt kompleksitet og derfor økt sårbarhet. Transportsektorens avhengighet av kablede og trådløse ekom-nett har blitt stor. Alle de fire transportsektorene har blitt vurdert og utvalget beskriver digitalisering, kompleksitet og økende avhengigheter relatert til ekom, GNSS, ITS og nøyaktig tid.

6.2.10. KIKS-2

I desember 2016 ga DSB ut rapporten Samfunnets kritiske funksjoner med undertittel «Hvilken funksjonsevne må samfunnet opprettholde til enhver tid». Rapporten, som kalles «KIKS-2», bygger på KIKS-1 og Infrastrukturutvalgets rapport. DSB utleder her hvilke funksjoner som er kritiske for samfunnssikkerheten og hvilke tjenester og leveranser som er nødvendig for å ivareta funksjonsevnen i disse funksjonene. Fokuset settes på samfunnsfunksjoner der en svikt raskt vil føre til tap og skade, og samfunnsfunksjoner som det særlig viktig å unngå avbrudd i.

Rapporten tar utgangspunkt i Infrastrukturutvalgets definisjon av kritisk samfunnsfunksjon som sier at en funksjon er kritisk hvis den truer grunnleggende behov. En annen måte å se det på, sier DSB, er at grunnleggende behov også kan defineres som ivaretakelse av grunnleggende *samfunnsverdier*, og tar med det i bruk igjen et begrep fra Sårbarhetsutvalget. Disse samfunnsverdiene er: Liv og helse, natur og miljø, økonomi, samfunnsstabilitet og styringsevne og kontroll. Dette er en noe kortere liste enn Sårbarhetsutvalgets liste over samfunnsverdier som også hadde med kulturelle verdier, territoriell integritet og materiell trygghet.

I denne rapporten blir kritiske samfunnsfunksjoner presentert i en nivå-delt struktur der de først sorteres i en av tre kategorier:

1. *Styringsevne og suverenitet*. Dette er funksjoner som utgjør grunnleggende rammebetingelser for at andre samfunnsfunksjoner skal kunne ivaretas.
2. *Befolkingens sikkerhet*. Dette er funksjoner som har direkte betydning for samfunnets evne til å ivareta befolkningens grunnleggende sikkerhet.
3. *Samfunnets funksjonalitet*. Dette er funksjoner som har indirekte betydning for samfunnets evne til å opprettholde befolkningens sikkerhet.

På nivået under listes samfunnsfunksjonene som tilhører den enkelte kategori. Under hver samfunnsfunksjon presenteres det kapabiliteter med tilhørende kritisk funksjonsevne. Kapabilitetene til en samfunnsfunksjon beskriver det som samfunnet må planlegge for å kunne opprettholde funksjonen. DSB knytter her kritisk funksjonsevne til begrep som kontinuitet, sikkerhet og beredskap. DSB har definert total 14 kritiske samfunnsfunksjoner fordelt på de tre kategoriene. Dette er to mer enn i KIKS-1. Innenfor kategorien samfunnets funksjonalitet finner vi transport og satellittbaserte tjenester som to av syv kritiske samfunnsfunksjoner.

Samfunnsfunksjonen transport knyttes her til samfunnets ansvar for funksjonaliteten og sikkerheten i de ulike transportformenes transportsystemer. Transportsystemene har avgjørende betydning for samfunnets funksjonalitet og har ulik grad av redundans. Påliteligheten i transportnettet henger nøye sammen med den robusthet som bygges inn i de ulike elementene som utgjør transportnettet. Transportsikkerheten avhenger av sikkerheten i infrastrukturen. Alle aktører skal til enhver tid følge regelverket fra myndighetene som blant annet stiller krav til bruk av risikostyringssystemer. Det er definert tre kapabiliteter til funksjonen transport:

- *Transportevne*. Dette er evnen til å opprettholde funksjonalitet i anlegg og systemer som er nødvendig for å ivareta samfunnets behov for transport.
- *Sikre transportsystemer*. Dette er evnen til å overvåke infrastruktur og styre trafikk for å opprettholde akseptabelt sikkerhetsnivå. DSB sier her at en svikt vil medføre uakseptabel risiko for ulykker og gi stans i trafikken.
- *Sikker transport*. Dette er evnen til å opprettholde akseptabelt sikkerhetsnivå ved transport med potensial for store ulykker. Kapabiliteten retter seg mot sikkerheten hos transportbedrifter.

Samfunnsfunksjonen satellittbaserte tjenester beskrives som en funksjon som består av mange tjenester med et bredt spekter av bruksmuligheter. Tjenestene kategoriseres i satellitt-navigasjon, satellittkommunikasjon og jordobservasjon. Det er definert kun én kapabilitet til denne kritiske samfunnsfunksjonen:

- *Satellittjenester*. Dette er evnen til å ivareta sikkerheten i leveranser av satellittbaserte tjenester til norsk territorium. Det handler om deltakelse i internasjonale organer for å ivareta norske interesser, men også ivaretakelse av kontinuitet og sikkerhet for bakkebaserte funksjoner relatert til satellittjenester. DSB understreker betydningen av

slike tjenester for samfunnet og at bortfall av dem vil med store konsekvenser for en rekke kritiske samfunnsfunksjoner som nødetatene, redningstjenesten, finanssektoren, kraftsektoren og luftfarten.

6.2.11. Risiko i et trygt samfunn

I desember 2016 kom Meld. St. 10 (2016-2017), *Risiko i et trygt samfunn* (JD, 2016). Hensikten med meldingen er bl.a. å følge opp Lysne-utvalget. Solberg-regjeringen skriver at meldingen må sees i sammenheng med langtidsplan for forsvarssektoren som ble utgitt i juni 2016.

Meldingen favner bredt og viser mange aspekter ved samfunnssikkerhet. Regjeringen skriver at samfunnssikkerhet handler om å arbeide systematisk med mulige hendelser som det er usikkert om noen gang vil skje. Det et er ingen sektorer, og få land, som i dag kan kontrollere sin digitale sårbarhet alene.

Regjeringen er tydelig på at vi må leve med risiko på et akseptabelt nivå og at det ikke er ønskelige at det norske åpne samfunnet skal gjennomsyres av sikkerhetstiltak. Det vil komme i konflikt med selvbestemmelse, personlig frihet, rettssikkerhet og personvern.

Meldingen har et kapittel som beskriver/forklarer hva som menes med samfunnssikkerhet. Her sier regjeringen av samfunnssikkerheten påvirkes av tre faktorer:

1. Verdiene vil skal beskyttes og deres sårbarheter
2. Farene og truslene vi står overfor
3. Vår evne til å forebygge og håndtere

Dette er i realiteten V, T og S i trefaktormodellen (ref. pkt. 5.2.2), men det begrepet brukes ikke i meldingen. Regjeringen holder seg konsekvent til den realfaglige tilnærmingen til risiko som produkt av sannsynlighet og konsekvens. Samfunnssikkerhetsarbeidet forklares her som en sammenhengende kjede. Leddene i kjeden er kunnskap, forebygging, beredskap, håndtering, gjenoppretting og læring som grunnlag for ny kunnskap.

Regjeringen skriver at offentlig-privat samarbeid (OPS) er viktig for å oppnå god samfunnssikkerhet. Dette er interessant fordi det viser at politisk ståsted er en faktor for hva som vektlegges i samfunnssikkerheten. OPS er viktig for en «blå» Solberg-regjering, mens

NOU 2006:6 som ble gitt ut under en «rød-grønn» Stoltenberg-regjering, tar til orde for at offentlig eierskap av infrastruktur og dugnadsånd er viktig for samfunnssikkerheten.

Romvirksomhet og norsk deltakelse i Galileo-programmet er omtalt. Regjeringen skriver den vil tydeliggjøre hvilke myndigheter som er ansvarlig for sikkerheten innenfor norsk romvirksomhet med argumentet om at de fleste samfunnskritiske funksjoner er avhengig av satellittbaserte tjenester. Samferdselssektorens betydning for samfunnssikkerhet er ikke omtalt.

6.2.12. Samfunnssikkerhet i en usikker verden

Den foreløpige siste offentlige publikasjonen på fagområdet samfunnssikkerhet er Meld. St. 5 (2020-2021), *Samfunnssikkerhet i en usikker verden,* fra oktober 2020. Budskapet nå er at det må spares. Den forebyggende delen av arbeidet blir viktigere. Utfordringsbildet har blitt bredt og det er nødvendig å vurdere om bestemte trusler bør prioriteres foran andre. Regjeringen skriver det er hverken ønskelig eller mulig å skape et risikofritt samfunn. *Ansvarsprinsippet* får her en utvidet betydning. Det presiseres at ansvarsprinsippet innebærer at ansvarlig instans tar stilling til hva som er akseptabel risiko gjennom å definere risikoakseptkriterier. Dette forventes å gi økt bevissthet om gjenstående risiko.

Stortingsmeldingen bruker plass på å forklare forskjellen mellom begrepene samfunnssikkerhet, statssikkerhet og nasjonal sikkerhet. Definisjonen av samfunnssikkerhet er den samme som i forrige melding. Statssikkerhet knyttes til statens eksistens, suverenitet, territorielle integritet og politisk handlefrihet. Disse to begrepene er gjensidig avhengig av hverandre. Nasjonal sikkerhet handler om å trygge nasjonale sikkerhetsinteresser slik de er beskrevet i den nye sikkerhetsloven fra 2019 (§1).

Samfunnets avhengighet av satellittjenester er beskrevet. Regjeringen skriver at satellitter er avgjørende for mange sentrale tjenester vi tar som en selvfølge. Satellittbaserte tjenester er en integrert det av samfunnets infrastruktur og bidrar til å realisere regjeringens mål innen stats-sikkerhet, samfunnssikkerhet og transport. Samfunnets avhengighet av slike tjenester er også en kilde til sårbarhet, der bortfall av satellittbaserte tjenester vil medføre konsekvenser for en rekke kritiske samfunnsfunksjoner. Transport er nevnt i forbindelse med totalforsvarets rolle, men er ellers lite omtalt i meldingen.

Digitale verdikjeder er omtalt her som i tidligere dokumenter. Denne gangen er fokuset på viktigheten av å drive risikostyring i kjedene og det henvises til rapporten Risikostyring av verdikjeder (DSB, 2020). Rapporten gir en modell for risikostyring rettet mot enkeltvirksomheter og på samfunnsnivå

6.2.13 Strategi for samfunnssikkerhet i samferdselssektoren

I tillegg til de nevnte dokumentene har SD laget en egen strategi for samfunnssikkerhet i samferdselssektoren. Den kom først i 2009 og deretter i ny versjon i 2015. (SD, 2015). Her oppsummeres samfunnssikkerhetsarbeidet i tre overordnede mål.

1. Unngå store, uønskede hendelser som medfører skader på personer, miljø eller materiell
2. Minske følgene av slike hendelser hvis de skulle oppstå
3. Sikre pålitelighet og framkommelighet i transport- og kommunikasjonsnett, både i normalsituasjon og under påkjenninger.

Strategien sier at samfunnssikkerhetsarbeidet handler både om sikkerhet forstått som fravær av skade, og som driftssikkerhet forstått som fravær av driftsstans. Dette vil kreve:

- Sikring av infrastruktur, systemer og funksjoner
- Styring og regulering av trafikk og annen aktivitet i transportnett- og systemer
- Beredskapsplanlegging og håndtering av uønskede hendelser i egen virksomhet og innen eget ansvarsområde.

Strategien inneholder en 8-punkts liste over krav til virksomheten. Et av disse er at samfunnssikkerhetsarbeidet integreres i den ordinære virksomhetsstyringen. Det legges også tydelig føring på at følgende prioritering skal følges:

- Klimatilpasning
- Informasjons- og IKT-sikkerhet
- Sikre kritiske objekter, systemer og funksjoner

6.3. Samfunnssikkerhetsinstruksen og hovedansvar

I september 2017 kom *Samfunnssikkerhetsinstruksen* (JD, 2017) som en oppdatering av samordningsinstruksen fra 2012 (DSB, 2012). Instruksen er publisert av JD og har som formål å presisere kravene til departementenes arbeid med samfunnssikkerhet, og å styrke samfunnets evne til å forebygge kriser gjennom helhetlig og koordinert arbeid med samfunnssikkerhet. Instruksen slår fast at arbeidet skal bygge på de fire prinsippene for samfunnssikkerhetsarbeid. I tillegg sies det eksplisitt at IKT-sikkerhet er en integrert del av arbeidet med

samfunnssikkerhet. I avsnitt fire, om krav til departementene, sier instruksen at arbeidet med samfunnssikkerhet skal være basert på systematisk risikostyring.

6.3.1. Hovedansvar

I tillegg til at alle departementer har et samfunnssikkerhets- og beredskapsansvar for sitt eget ansvarsområde i henhold til ansvarsprinsippet, innfører samfunnssikkerhetsinstruksen begrepet «departement med hovedansvar for kritisk samfunnsfunksjon». Her gis enkelte departementer et særlig ansvar for koordinering og samordning i tillegg til sitt ordinære sektoransvar. Det fremgår ikke av instruksen hvilke departementer som er tildelt slikt hovedansvar. For å finne det må man gå inn i den delen av statsbudsjettet som gjelder for JD. Her finnes en tabellarisk framstilling av denne informasjonen. I statsbudsjett for 2020 ser den delen av tabellen som dekker satellittjenester slik ut:

Samfunns-kritiske funksjo-nar og område	Hovudansvar-leg departement	Utøvande verksemder/forvaltningsnivå	Andre departe-ment med ansvar
elektronisk kommunika-sjonsnett og -tenester (Ekom)	Kommunal- og moderniser-ingsdeparte-mentet (KMD)	Nasjonal kommunikasjonsmyndigheit (Nkom), Direktoratet for samfunnstryggleik og beredskap (DSB), Forsvaret, ekomtilbydarar	Justis- og bered-skapsdeparte-mentet (JD), For-svarsdeparte-mentet (FD)
digital tryggleik i sivil sektor	JD	Nasjonalt tryggingsorgan (NSM), Norsk senter for informasjonstryggleik (NorSIS), Datatilsynet, Nkom, DSB, eigarar av kritisk viktige IKT-system, digitale register og arkiv, Direktoratet for IKT og forvaltning (Difi)	KMD, dei andre departementa
satellittbasert kommunika-sjon og naviga-sjon	KMD Samferdsels-dpartementet (SD er hovud-ansvarleg departement for PNT.) [1]	Norsk romsenter, Kongsberg Satellite Services (KSAT), Space Norway AS, Kystverket, Nkom, Sta-tens kartverk	JD, Nærings- og fiskeridepartе-mentet (NFD)

Figur 21: Utsnitt fra JDs oversikt over departementenes hovedansvar

Tabellen viser at samfunnssikkerhetsmessig hovedansvar for ekom, satellittkommunikasjon og navigasjon er delt mellom KMD og SD. Tilsvarende tabell for året før viste at alt dette lå hos SD. Flytting av hovedansvar er et resultat av Granavolden-plattformen med en ny digitaliseringsminister med ansvar for ekom i KMD. PNT har blitt værende igjen hos SD som har ansvar for sivil radionavigasjonspolitikk. SD har etter dette det samfunnssikkerhetsmessige hovedansvaret for funksjonen nøyaktig tid ved at departementet har hovedansvar for PNT. I statsbudsjett for 2021 er tabellen uendret for dette hovedansvaret.

Tabellen er også tatt inn i Meld. St. 5 (2020-2021). Stortingsmeldingen forklarer hovedansvar med at det innebærer en vurdering av hvilken evne samfunnet har til å opprettholde funksjonene

dersom de utsettes for ulike påkjenninger (s.141). Krav til departementer som har hovedansvar er listet i samfunnssikkerhetsinstruksen kapittel fem. Det skal utarbeides ROS-analyser, holdes oversikt over sårbarheter, lages tilstandsvurderinger, avklare ansvar og gråsoner mellom aktører, gjennomføre felles øvelser, fremlegge forslag til tiltak, planer og regelverk for berørte departementer, sørge for erfaringsutveksling og kompetanseheving og bistå JD med informasjonsinnhenting og rapportering.

I august 2019 ga JD ut en veileder til samfunnssikkerhetsinstruksen (JD, 2019). Om hovedansvar står det at «Hovedansvarlig departement har et særlig ansvar for god samordning innenfor sine kritiske funksjoner. Ansvaret er blant annet knyttet til å ha oversikt, ta initiativ og om nødvendig øve påtrykk». Det settes også fokus på samordning på tvers av departements- og sektorgrensene og at dette krever aktivt involvering. JD anbefaler alle hovedansvarlige departementer å etablere nettverksforum og kontaktmøteordninger innenfor samfunnsfunksjonen.

6.4. Oppsummering av dokumentgjennomgangen

Gjennomgangen av disse dokumentene viser en utvikling fra et samfunn preget av kald krig med en identifisert, ytre fiende til et moderne, digitalisert og komplekst fredstidssamfunn med uoversiktlige sammenhenger på tvers av ansvarsområder. Totalforsvarets rolle er omdefinert og løftet mer fram de siste årene.

Utviklingen preger begrepsbruken og fokuset fra myndighetene. Ordet krig forsvant tidlig selv om Norge har hatt væpnede styrker i utlandet i hele denne perioden. Det fremgår at ingen lenger har særlig tro på et militært angrep på Norge, men at truslene som samfunnet står overfor tar form av ekstremvær, ødeleggelser av infrastruktur og svikt i kritiske samfunnsfunksjoner. Fokuset er flyttet fra militært forsvar til håndtering av terror, storulykker og sikring av infrastruktur.

Ny sikkerhetslov har blitt nødvendig og leder til definering av grunnleggende nasjonale funksjoner (GNF) og krav til objektsikring. Dokumentene viser at det er brukt mye ressurser på å definere hva som i vår tid er kritisk infrastruktur og kritiske samfunnsfunksjoner, og hvor ansvaret for dette ligger i forvaltningen. Samfunnssikkerhet handler om å arbeide systematisk

med mulige hendelser som det er usikkert om noen gang vil skje. Usikkerhet må aksepteres og alle som har et ansvar etter ansvarsprinsippet må prioritere og etablere en risikoaksept.

Samfunnssikkerhetsarbeidet krever høy grad av koordinering og samhandling og det har vært nødvendig å innføre et nytt samvirkeprinsipp for å understreke ansvaret ulike etater og aktører har for å sikre godt samarbeid. Det slås fast at ingen kan klarer dette alene. Koordinering og samhandling er avgjørende. Samfunnssikkerhet har blitt komplekst, det er mange faktorer som spiller inn og det har blitt et akademisk fagfelt med forskningsmiljøer flere steder i Norge.

I den 20-årsperioden som disse dokumentene er utgitt har det foregått en omfattende digitalisering av samfunnet. Betydningen av IKT er enormt mye større nå enn da Sårbarhets-utvalget avga sin rapport og Lysne-utvalgets rapport er i så måte viktig lesning. Digitale verdikjeder, som ofte er uoversiktlig og går på tvers av landegrenser, har blitt sentrale for opprettholdelse av kritiske samfunnsfunksjoner. I disse verdikjedene finner vi satellittsystemer utenfor norske brukeres kontroll, som GNSS. Risikostyring i kjedene har blitt viktig og det stilles krav til systematisk risikostyring i samfunnssikkerhetsarbeidet. Samtidig er det kommet til en erkjennelse av at det hverken er mulig, eller ønskelig, med et risikofritt samfunn. Ansvarsprinsippet som har fulgt alle disse dokumentene siden Sårbarhetsutvalgets rapport, får derfor nå til slutt en utvidet betydning. Det blir en del av ansvaret å lage akseptkriterier og prioritere hvilke risikoer og sårbarheter som skal reduseres/fjernes. Hensikten er å spare, men også å oppnå økt fokus på restrisiko.

Satellittbaserte tjenester er en integrert del av samfunnets infrastruktur og bruken av dem knyttet til statssikkerhet, samfunnssikkerhet og transport. Samfunnets avhengighet av slike tjenester er også en kilde til sårbarhet. Slike systemer er en del av transportinfrastrukturen og samfunnets funksjonsdyktighet er avhengig av transport. Transport er en kritisk samfunnsfunksjon. Transportsikkerheten blir aldri bedre enn sikkerheten i infrastrukturen.

7. METODE

I kapitel 2 beskrev jeg forskningsdesign gjennom bruk av Pentagon-modellen. De tre første av modellens fem spørsmål ble der besvart for å beskrive hva oppgaven spør om, oppgavens formål og empiri. I dette kapittelet går jeg videre med modellen og besvarer spørsmål fire og fem. Jeg beskriver valgt metodikk og gjennomføring av datainnsamling, vurderer dataenes validitet og reliabilitet, og beskriver hvordan de presenteres.

7.1. Pentagonmodellen – spørsmål 4 og 5

7.1.1. Hva spør du med?

Jeg går inn i spørsmålsstillingen med den basis som litteraturgjennomgangen har gitt av teorier, begreper og metoder. Dette vil være teori som er kjent fra masterprogrammets kurspensum innenfor risiko og sikkerhet i tillegg til litteratur jeg har funnet spesielt for denne oppgaven. Relatert til risikostyring vil det være relevant å legge til grunn både naturvitenskapelig og samfunnsvitenskapelig kunnskapssyn. Metodelitteratur vil være Johannessen et al.: Samfunnsvitenskapelig metode (Johannessen et al., 2016) og Dalen: Intervju som forskningsmetode (Dalen, 2013).

Jeg vil gå videre med en faktainnsamling fra de mest sentrale infrastruktureiende samferdsels-aktørene innenfor hver transportform. Faktainnsamlingen vil ha fokus på få kunnskap om praksis hos disse relatert til GNSS, digitalisering, sikkerhetsstyring og samfunnssikkerhet. Jeg ønsker å samle faktainformasjon om praksis hos aktørene som i sum beskriver et oversiktsbilde for transportsektoren.

Dette kunne vært gjort med dokumentstudie av aktørenes strategier, prosesser og sikkerhetsstyringssystem, men jeg har i stedet valgt intervju som metode. En slik kvalitativ metode gir muligheter til å få informasjon ikke bare om hva formelle dokumenter sier, men i tillegg hvordan dette omsettes i praksis og andre forhold av mer uformell art som en informant kan opplyse om. Intervjuene vil derfor ta form av muntlig faktainnsamling og vil kunne gi et mer helhetlig bilde av praksis enn kun en dokumentstudie.

7.1.2. Hvordan spør du?

Intervjuguide

Jeg spør ved å gjennomføre en intervjuserie basert på en utarbeidet intervjuguide (vedlegg 1). Intervjuguiden har en del for hver av de aktørene som faktainnsamlingen retter seg mot. Disse er: Samferdselsdepartementet (SD), Statens Vegvesen (SVV), Kystverket (KYV), Bane NOR (BN) og Avinor. Intervjuguide og planlagt gjennomføring ble godkjent av NSD[54] før oppstart.

Alle de fem aktørene fikk oversendt intervjuguide sammen med et følgeskriv. I følgeskrivet anmodes de om selv å velge ut informant basert på spørsmålenes innhold. Faktainnsamlingen har foregått under corona-pandemien okt/nov 2020, så alle møter har foregått elektronisk på videokonferanse Teams, Skype og Pexip. I tillegg til dette har det vært noe mailutveksling.

Intervjuguiden inneholder et sett av spørsmål for hver etat/virksomhet. Flere av disse er like, men det er også spørsmål som går direkte på den enkelte transportform for å fange opp spesielle forhold som ikke berører andre. Hver etat/virksomhet har kun sett «sine» spørsmål der spørsmålene er gruppert etter tema.

SD skiller seg fra de andre informantene ved at departementet har et overordnet styrings-ansvar for de andre og har en politisk ledelse. Spørsmålene til SD har derfor en annen vinkling, og er gruppert annerledes, enn for de andre etatene/virksomhetene nettopp for å få fram forhold ved den styrende rollen.

Gjennomføring av intervju

SD, KYV, BN og Avinor stilte til intervju, dog etter litt purring. SVV har hatt to informanter hvorav en ønsket intervju og en ønsket å svare skriftlig. Etter konferering med veileder ble dette akseptert ettersom faktainnsamlingen handler om å innhente informasjon om etablert praksis mer enn å få informantens personlig meninger. Det har likevel tatt bort en mulighet for direkte samtale og å stille korte oppklarende/oppfølgende spørsmål underveis i samtalen. KYV stilte med én person, mens det hos de andre var to personer som svarte i fellesskap. Hos BN ble det gjennomført intervju med de to informantene på to ulike tidspunkt. Til sammen har det vært gjennomført seks intervjuer med ni personer i fem organisasjoner. Alle informanter aksepterte lydopptak, noe som forenklet notatarbeidet betraktelig.

[54] Norsk senter for forskningsdata, https://www.nsd.no

Under bearbeiding av den innsamlede informasjonen har det oppstått enkelte behov for oppklaring eller utdyping av ting som ble sagt. Dette er oversendt på e-post og besvart skriftlig av de samme informantene.

Jeg har anonymisert informantene. Det er ikke viktig for oppgaven hvem informantene er eller hvilken stilling/rolle de har så lenge etatene/virksomhetene selv mener de er de riktige personene til å svare ut spørsmålene i intervjuguiden på vegne av dem.

7.2. Vurdering av innsamlede data

7.2.1. Dataenes detaljgrad

Jeg har valgt å henvende meg til så mange aktører for å kunne danne meg et overordnet bilde over sektoren. Ved å velge å hente inn fakta fra både SD og etatene/virksomhetene innenfor de begrensningene oppgaven gir, vil dataene ikke kunne gå i detalj for hver aktør, men gi et oversiktsbilde. Dette vil gi et inntrykk av sektoren, men gir også en begrensning i hvor mye som kan trekkes ut av datagrunnlaget for hver aktør. Det vil likevel være nyttig for å kunne knytte praksis opp mot funn i dokumentgjennomgangen og kunne danne grunnlag for eventuelle oppfølgende studier rettet mot hver aktør.

7.2.2. Fremstilling av data/sitatbruk

På grunn av SDs styrende rolle overfor de andre etatene/virksomhetene har jeg valgt å presentere informasjon fra SD i eget del-kapittel. For de andre etatene/virksomhetene grupperer jeg deres besvarelse etter tema. Det gir en bedre oversikt for å se likheter og forskjeller mellom dem. Temaoverskriftene fra intervjuguiden brukes som avsnittsoverskrift i den sammenhengen.

Enkelte informanter er veldig konkrete og konsise i sine svar, mens andre velger å uttrykke seg gjennom lengere resonnementer. Flere av informantene har også svart på en måte så de i realiteten svarer på flere spørsmål i samme svar. Det har medført at en del av svarene ikke uten videre kan gjengis som sitater under et bestemt spørsmål. Jeg har valgt å ikke bryte opp dette i større grad enn nødvendig for at sentrale momenter skal komme fram, men i enkelte tilfeller har jeg flyttet deler av svaret som ble gitt til det spørsmålet det hører hjemme.

Jeg har valgt å formulere tekst basert på svarene i større grad enn å gjengi det som sitater. Det gir mindre bruk av sitater enn det som trolig vil være vanlig ved bruk av intervju som metode,

men det er valgt av årsaker som nevnt over og for å øke lesbarheten uten at faktainformasjon blir utelatt.

7.2.3. Validitet

Dataenes validitet handler om deres grad av gyldighet. Med det skal forstås i hvilken grad dataene faktisk representeres det fenomenet som studeres (Johannessen et al., 2016). De fleste av dokumentene som er lagt til grunn er offentlig publikasjoner i form av stortingsmeldinger, offentlige utredninger og strategidokumenter. Slike dokumenter er grundig bearbeidet fra utgivers side og vi har sjelden grunn til å tvile på innholdet i slike dokumenter.

Data/informasjon som samles inn gjennom intervjuer kan være litt mer usikkert. Her er jeg avhengig av at de etatene/virksomhetene jeg henvender meg til velger ut informanter som har god nok oversikt og innsikt til å svare på hva som er virksomhetens etablerte praksis. Jeg er også avhengig av at det informanten sier er sant. Kvaliteten på intervjuguiden spiller også en rolle. For at informantene skal fortelle meg det jeg trenger å vite må spørsmålene være riktig formulert og treffe riktig.

7.2.4. Reliabilitet

Reliabilitet kan forstås som pålitelighet og knytter seg her til nøyaktigheten i de dataene som undersøkelsen frembringer (Johannessen et al., 2016). Dette kan også forstås som i hvilken grad dataene kan gjenskapes hvis de samles inn på nytt på samme måte. Når datainnsamling gjøres er det en målsetting at disse skal bli så nøyaktige som mulig, men det må alltid vurderes i hvilken grad dette har lykkes. Det må vurderes hvilke feilkilder som vil være relevante og kunne ha en betydning for resultatet.

Informasjonen i offentlige dokumenter vil naturlig nok være den samme. Stortingsmeldinger er informasjon fra regjeringen til Stortinget om hva som er gjort på et bestemt felt eller informasjon om framtidig politikk[55]. Det kan derfor være en politisk vinkling på det som presenteres som fakta. Hvis f.eks. informasjon skal samles inn på nytt etter et regjeringsskifte kan rådende praksis ha endret seg.

Informasjon fra muntlige kilder vil kunne blir litt annerledes. Hvis informasjonen hentes inn på nytt fra en annen informant så er det mulig at vedkommende har en annen oppfatning av

[55] https://www.stortinget.no/no/Stortinget-og-demokratiet/Storting-og-regjering/Saksgangen-etter-1-10-2009/

virksomhetens praksis eller velger å vektlegge ting annerledes enn forrige informant. Den fakta-informasjonen jeg etterspør vil også være i utvikling og derfor være annerledes i framtiden. Det jeg etterspør vil være fakta slik det ser ut på det tidspunktet jeg spør.

8. FAKTAINNSAMLING

I dette kapitlet presenterer jeg fakta som er samlet inn gjennom intervju av informanter hos Samferdselsdepartementet (SD) og de største etatene/virksomhetene som eier og drifter infrastruktur innenfor hver transportform. Jeg gir først en kort presentasjon av hver aktør som har stilt informant til rådighet før jeg gjengir besvarelsene på spørsmålene i intervjuguiden.

8.1. Departement og etater/virksomheter[56]

- *Samferdselsdepartementet (SD).* SD er samferdselsministerens sekretariat og verktøy for politikkutforming. SD er ansvarlig for rammevilkår for samferdselssektoren og for samfunnssikkerhet innenfor eget politikkområde. Samfunnssikkerhetsinstruksen gir SD hovedansvar for PNT.
- *Statens Vegvesen (SVV).* SVV er etat under SD og har ansvar for europa- og riksveinettet, kjøretøy og trafikanter. Etaten bygger og vedlikeholder veiinfrastruktur. SVV har et stort fokus på ny teknologi og har en egen enhet for utvikling og anvendelser av ITS. Det er også en egen enhet for transport, samfunn og beredskap.
- *Kystverket (KYV).* KYV er en etat under SD med ansvar for kystforvaltning, sjøsikkerhet og beredskap mot akutt forurensning. KYV bygger ut og vedlikeholder farleder, merker, fyr, lykter og havneanlegg, Etaten drifter flere sjøtrafikksentraler for å overvåke og kontrollere skipstrafikken langs kysten.
- *Bane NOR (BN).* BN er et statlig foretak med ansvar for planlegging, utbygging, forvaltning, drift og vedlikehold av det nasjonale jernbanenettet. I tillegg styrer BN trafikken på jernbanenettet fra sine trafikksentraler. BN har koordineringsansvar for sikkerhetsarbeid og operativt ansvar for samordning av beredskap og krisehåndtering.

[56] Informasjonen i de påfølgende kulepunktene er hentet fra etatenes/virksomhetenes nettsider. (Sist besøkt 2020-10-11)

- *Avinor*. Avinor er et aksjeselskap heleid av staten. Eierskapet forvaltes av SD. Avinor ivaretar eierskap, drift og vedlikehold av et landsomfattende nett av lufthavner for den sivile luftfarten, og en samlet flysikringstjeneste for den militær og sivile luftfarten. Datterselskapet Avinor Flysikring, leverer lufttrafikktjenester fra kontrollsentraler og kontrolltårn og drifter en landsdekkende infrastruktur av radionavigasjonssystemer og trafikkovervåkingssystemer.

8.2. Samferdselsdepartementet

I dette delkapitlet presenteres SDs svar på spørsmålene i intervjuguiden. Temaene som berøres er sektorens betydning for samfunnssikkerhet og SDs styrende rolle, SDs hovedansvar for PNT, GNSS-avhengighet og mulig sårbarhet og krav til sikkerhetsstyring. Det fremkommer at sektoren betraktes som viktig både for samfunnssikkerhet og statssikkerhet. SD anser sitt hovedansvar primært som et koordineringsansvar der brukere av PNT selv har ansvar for avhengighet og sårbarhet gjennom ansvarsprinsippet og sektorprinsippet. SD styrer gjennom etatsstyring og eierstyring og gir ikke konkrete føringer på sikkerhetsstyring.

8.2.1. Samferdsel og samfunnssikkerhet generelt

Samferdselssektorens rolle inn mot samfunnssikkerhet

SD sier at sektoren spiller en viktig rolle ved at SD har et ansvar for funksjonen transport relatert til KIKS-rammeverket. I tillegg til dette har SD ansvar for kapabiliteter som hører innunder andre departementers hovedansvar. SD sier at PNT er et eksempel på dette. Videre sier SD at det har ansvar for funksjoner, som f.eks. post, som ikke fremkommer i KIKS, men som likevel er viktig for samfunnssikkerhet og totalforsvar. SD understreker forskjellen mellom samfunns-sikkerhet og statssikkerhet og har erfart et økt fokus på totalforsvaret de senere årene bl.a. gjennom arbeidet med ny sikkerhetslov, GNF (se fotnote nr. 1) og skjermingsverdige objekter. SD mener dette har gitt en økt bevissthet om at det er mange av tjenestene som SD er ansvarlige for som sorterer inn under statssikkerhetsbegrepet. SD har en viktig rolle inn mot totalforsvaret i kraft av å være ansvarlig for transport og PNT der hvor forsvaret har nytt av sivile tjenester. Når det gjelder samfunnskritiske funksjoner i KIKS i forhold til GNF sier SD at det er en stor sammenheng mellom disse, men det er ingen automatikk i at en funksjon i KIKS blir en GNF.

SD opplyser at det ikke er besluttet om satellittbaserte tjenester skal være en GNF (pr. okt. 2020).

Hvordan ivaretar SD denne rollen?

SD ivaretar sin styringsrolle og sitt ansvar for samfunnssikkerhet i egen sektor gjennom det informanten kaller de vanlige styringslinjene. Dvs. at etatsstyring og eierstyring sammen med rammene i etablerte sektorregelverk for de ulike transportformene, er sentrale verktøy. Et annet virkemiddel, som SD betrakter som litt «mykere», er å være pådriver for samfunnssikkerhet i egen sektor gjennom strategidokumenter. SD har laget en strategi for samfunnssikkerhet som gjelder både for etater og selskaper. Informanten sier hensikten er å gi føringer fra SD på hvordan etatene/virksomhetene skal jobbe med dette og hva som skal være prioriterte områder. Utover dette foregår det prosesser mellom departement og etat i større enkeltsaker, ikke minst relatert til totalforsvaret. Det kan handle om regelverksendringer, beredskapsplanlegging, sivilt beredskapssystem, m.m.

Hva legger SD i begrepet transportberedskap?

Relatert til samfunnssikkerhet og totalforsvar bekrefter SD å ha et ansvar for sivil transportberedskap. SD forklarer at transportberedskap handler om å fremskaffe nødvendige transportmidler i en situasjon der markedet ikke ellers løser transportbehovet samtidig som det er noe som tilsier at man virkelig trenger transportressurser. Informanten sier transportberedskap i realiteten skal forstås som transporttjenesteberedskap. SD har hjemler til å pålegge aktører å utføre transportoppdrag, men det er noen begrensninger overfor utenlandske aktører i Norge. SD opplyser at her er det variasjoner mellom del-sektorene. F.eks. innen luftfart er dette begrenset til norskregistrerte fly. Utviklingen har gått fra kald krig til en digital verden, men SD sier vi er litt tilbake i kald krig modus pga. utviklingen i det sikkerhetspolitiske bildet. Forsvaret er betydelig omstrukturert og SD erfarer at det har blitt veldig avhengig av sivil side for å kunne

Figur 22: Sivil transport av militært materiell (kilde: https://jernbanemagasinet.no/artikler/nato-pa-skinner/)

levere forsvarskraft. SD sier at bruk av sivile ressurser også handler om folkerett[57]. Hvem kan pålegges hva, og i hvilke situasjoner? Informanten opplyser at beredskapsbegrepet i samferdselssektoren også kan omfatte evne til å utføre reparasjoner på infrastruktur. F.eks. har SVV en omfattende beredskap for å kunne gjenåpne ødelagte veier og broer.

SD har hovedansvar for PNT. Hva betyr det at SD med dette har ansvar for nøyaktig tid?

I samfunnssikkerhetsinstruksen gis SD et hovedansvar for PNT, dvs. blant annet for nøyaktig tid. Informanten sier dette er et eksempel på at SD har ansvar for en kapabilitet under en funksjon som et annet departement er ansvarlig for. Dette ligger under KMDs ansvar for satellittjenester. SDs informant sier at et å ha et hovedansvar skal forstås som å ha et koordineringsansvar. Informanten utdyper at SDs oppgave relatert til hovedansvar går ut på å ha en oversikt over status, formidle kunnskap om sårbarheter, risikofaktorer og eventuelt ta initiativ for å håndtere rene tverrsektorielle spørsmål. Mye av samfunnssikkerhetsarbeidet foregår innenfor sektorene, men det kan være noen sektorovergripende temaer. SD understreker at sektoransvaret er sentralt. Nøyaktig tid brukes av mange i ulike sektorer. Sektoransvaret sier da at alle har ansvar for egen bruk av nøyaktig tid og hva dette gir av eventuelle konsekvenser som er relevant for samfunnssikkerhet i sin sektor. SDs informant opplyser at hvis det oppstår temaer knyttet til nøyaktig tid på tvers av sektorene som det er hensiktsmessig at sektorene finner en felles løsning på, vil SDs hovedansvar bety at SD koordinerer dette. PNT-strategien som SD ga ut i 2018 har en funksjon i dette, sier SD. NFD med Justervesenet som underliggende etat er ansvarlig «tidsdepartement» og ansvarlig for dette i egen sektor. SD opplyser at SDs hovedansvar for nøyaktig tid vil ikke redusere næringsministerens ansvar for tid.

8.2.2. Samferdselssektoren og GNSS

SDs ansvar for sivil radionavigasjonspolitikk

Bruken av satellittnavigasjon og satellittbasert PNT øker stort og SD ser at stadig flere sektorer tar dette i bruk og blir avhengig av det. Da vil det følge av sektoransvaret og ansvarsprinsippet, sier SD, at hver enkelt sektor må ta ansvar for egen sikkerhet og for å gjøre nødvendig risikovurderinger. SD opplyser at ansvaret for sivil radionavigasjonspolitikk vil si at

[57] Etter intervjuet med SD har dette vært tema i nyhetsbildet. I desember 2020 var det debatt i Stortinget om at sivile leverandører til Forsvaret kan bli angrepsmål i krig og at sivilt ansatte slik blir legitime mål på linje med soldater. (https://www.vg.no/nyheter/innenriks/i/1BvmmJ/opposisjonen-reagerer-forsvarets-leverandoerer-kan-bli-angrepsmaal-i-krig)

departementet har et ansvar for å sørge for at det finnes en helhetlig og tverrsektoriell strategi og poltikk for å håndtere disse spørsmålene.

Har SD ansvar for bruk av GNSS utenfor samferdselssektoren?

SD har ikke noe direkte ansvar for hvordan satellittbasert PNT anvendes i andre sektorer. Problemstillinger som er utpreget tverrsektorielle vil SD ha et koordineringsansvar for. SD sier at departementets fokus er på koordineringsansvaret og den strategiske biten av det. En viktig del av strategien er å synliggjøre avhengighetene og prøve å redusere sårbarhetene.

GNSS avhengighet og sårbarhet

SD opplyser å være godt kjent med den omfattende bruken av GNSS i transportsektoren og den økende avhengigheten. Det skjer innenfor alle transportformer og anleggsvirksomhet for infrastruktur for alle transportformer. Når sektoren går i retning av økende automatisering og autonomi vil GNSS være veldig viktig. Innenfor sjøtransport og luftfart er i tillegg trafikk-overvåking veldig avhengig av GNSS både for posisjonsangivelse og nøyaktig tid. SD sier at hele sektoren er i økende grad avhengig av GNSS. SD har derfor et stadig større fokus på at en ikke kun skal basere seg på GNSS. SD presiserer at det skal være mulig å gjennomføre transport selv om GNSS faller ut. Innenfor luftfart er det gjort en vurdering av en tverrdepartemental/tverrfaglig gruppe av denne utfordringen. Det er stadig viktigere at det jobbes med risikoen knyttet til bortfall av GNSS. Bortfall av GNSS forekommer og det kan ha betydelige konsekvenser. SD sier det skal finnes fornuftige systemer for backup.

Hvordan tar SD styring over disse utfordringene?

Hvis SD mener det er nødvendig å gi konkrete føringer innenfor denne problematikken, gjøres det overfor underliggende etater gjennom de vanlige styringsmekanismene. Utgangspunktet er at virksomhetene selv har et selvstendig ansvar for å ivareta sikkerheten i sine leveranser. SD legger til grunn at virksomhetene selv må ha oversikt over hva de er avhengig av, f.eks. PNT. Det ligger til virksomhetene selv å identifisere sårbarhet og gjøre det de kan for å redusere sårbarheter uten av SD må gå inn og stille tydelig krav på avgrensede faglige områder. SDs mål er å bidra til godt nok kunnskapsgrunnlag slik at de blir i stand til å gjøre de vurderingene og tiltakene de mener er nødvendig.

8.2.3. Krav til sikkerhetsstyring

Gir SD sine etater føringer på håndtering av risiko relater til samfunnssikkerhet?

SD opplyser at det ikke gir underliggende etater/virksomheter konkrete føringer på dette, ei heller på risikostyring av nøyaktig tid. Etatene/virksomhetene har et eget ansvar for sikkerhetsstyring innenfor sine ansvarsområder og de har sektorregelverket som sier hva de skal ha og hva de skal gjøre på dette området. SD sier strategien som er etablert for samfunnssikkerhet i samferdselssektoren penser inn på disse tingene og hva SD forventer at de gjør som en del av sin sikkerhetsstyring. SD opplyser å ha en forventning om at etatene/virksomhetene er aktive bidragsytere, tar et samfunnsansvar utover egen virksomhet og er aktive bidragsytere til samfunnssikkerhet i samferdselssektoren.

SD utdyper at det er en tendens i sikkerhetsarbeidet i stort, også på regelverkssiden, at det i stadig større grad brukes funksjonsbaserte krav. Når SD ber virksomhetene gjennomføre ROS-analyser i egen sektor så stilles de ganske fritt til å legge til grunn de modellene som de mener er fornuftige relatert til de scenarioene, casene og den tilnærmingen de bruker.

8.2.4. GNSS og IKT-sikkerhet

Anser SD at GNSS faller inn under IKT?

SD ønsker ikke å ha noen konkret mening om GNSS er å betrakte som IKT. Det viktigste er hva etatene/virksomhetene selv mener om det, sier SD. Hvis de mener at deres systemer som bruker nøyaktig tid er på linje med andre IKT-systemer, så må de forholde seg til det på den måten. I så fall forventer SD at NSMs grunnprinsipper[58] benyttes. Dette er prinsipper som SD har bedt etatene/virksomhetene legge til grunn i sitt arbeid på IKT-sikkerhetsområdet.

SD sier at slik departementet kjenner systemene i egen sektor er det ikke unaturlig å tenke på det som IKT med den problematikken som er knyttet til lange digitale verdikjeder og sårbarhet det er vanskelig å holde kontroll på.

[58] Med dette menes NSMs grunnprinsipper for IKT-sikkerhet som er et sett med prinsipper og tiltak for å beskytte informasjonssystemer, data og tjenester mot uautorisert tilgang, skade og misbruk. (https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt)

8.3. Transport og samfunnssikkerhet

I dette delkapitlet gjengis hvordan SVV, KYV, BN og Avinor har svart på første gruppe av spørsmål i intervjuguiden med tema transport og samfunnssikkerhet. Temaene er hvordan de ser på egen del-sektor og egen rolle relatert til samfunnssikkerhet, hvordan rollen ivaretas, om trenden med digitalisering påvirker dette og om de lager regler/forskrifter som andre aktører i sin del-sektor må følge.

Det fremgår at alle betrakter sin del-sektor som viktig for samfunnssikkerhet. SDs strategi for samfunnssikkerhet legges til grunn for arbeidet med samfunnssikkerhet hos de fleste. Digitalisering påvirker i stor grad tjenester og funksjoner og det refereres til arbeid med NIS-direktivet[59]. Det gis uttrykk for at digitalisering medfører sårbarhet, men at det er fokus på dette og at digitaliseringen generelt er en positiv ting.

8.3.1. Statens Vegvesen

SVVs informant sier vegtransport er svært viktig for samfunnssikkerhet fordi fremkommelighet er viktig for sivil transport, nødetater, godstransport og militær aktivitet. SVV siterer fra forslag til statsbudsjett for 2021 der etatens ansvar er beskrevet slik: «SVV er veimyndighet for riksveiene og har et nasjonalt ansvar for veidata og veitrafikkinformasjon, nasjonale oppgaver knyttet til samfunnssikkerhet og beredskap og er SDs fagorgan i veisektoren. Videre har etaten ansvaret for trafikant- og kjøretøyområdet og følger opp nasjonale oppgaver for hele veitransport-systemet.»

SVV opplyser å ha utarbeidet et policy-dokument basert på SDs strategi for samfunnssikkerhet i samferdselssektoren, samt krav i veilov og veitrafikklov. Her beskrives de ulike divisjonenes ansvar for beredskap, men mye av det som skjer langs veiene faller innunder normalsituasjonen for divisjon drift og vedlikehold. SVV samler inn informasjon fra veieierne for holde oppdaterte statusoversikter. Policy-dokumentet er også basis for SVVs beredskapsplan. SVV har et omfattende opplegg knyttet til beredskap for å holde veier og bruer åpne.

SVV sier de har et tett samarbeid med Forsvaret i totalforsvarssammenheng. Dette gjelder også øvelsesplanlegging der mye tungt materiell skal ut på veiene. Veistandarder må tas hensyn til og SVV kan gi forsvaret dispensasjoner.

[59] (EU) 2016/1148 om tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU.

SVV opplyser at digitalisering er et tema med stor innvirkning hos etaten. Økende grad av digitalisering vil gi økt sårbarhet for digitale angrep eller svikt i bakenforliggende systemer. SVV har fokus på å bygge forsvarsverk mot digital inntrengning, etablere redundans i systemer og innføre backup der det er mulig og hensiktsmessig. SVV er tillagt myndighet etter både vegtrafikkloven og vegloven og ivaretar direktoratsfunksjon for veitransport. Dette innebærer utvikling av lover, forskrifter og regler som andre aktører i vegsektoren må følge.

8.3.2. Kystverket

KYV er tydelig på at sjøtransporten av gods er viktig for samfunnet. Informanten sier det er to egenskaper ved sjøtransporten som er viktig for samfunnssikkerheten. Det ene er å unngå ulykker. Det andre er å opprettholde transport-evnen. Utenfor kysten går det skip med flere tusen passasjerer og skip med olje og farlig gods. Ulykker kan få store konsekvenser. Transportevnen, dvs. åpne leder og havner, er viktig for å holde samfunnet i gang.

Figur 23: Viking Sky i havsnød i Hustadvika mars 2019 (kilde: https://www.rbnett.no/nyheter/2019/04/02/)

KYV opplyser at etaten griper an samfunnssikkerhet ved å ta utgangspunkt i SDs strategi for samfunnssikkerhet i samferdselssektoren. På bakgrunn av denne, og sektorregelverket, har KYV laget sin egen strategi for samfunnssikkerhet med tilhørende handlingsplan. KYVs mål er de samme som samfunnssikkerhetsmålene i SDs strategi. KYV jobber systematisk med dette og informanten hevder at nær alt KYV gjør kan relateres til å støtte opp under disse samfunnssikkerhetsmålene. Det jobbes også med innføring av NIS-direktiv og ny sikkerhetslov.

Digitaliseringen gjøres med to hensikter, opplyser KYV. Det ene er å øke sikkerheten gjennom å forbedre tjenester og forbedre operasjonen av skip. Den andre er å øke effektiviteten ved å flytte informasjon lettere og gjøre den lettere tilgjengelig. KYVs syn er at digitaliseringen vil redusere omfanget av ulykker som et samfunnssikkerhetsmål. Det vil også bidra til å styrke transportevnen siden tjenester og operasjon av skip blir bedre. KYV understreker at en

konsekvens av digitalisering er at samfunnsmessig risiko flyttes inn på det digitale området. Det kan skapes en sikkerhetsrisiko ved at det digitale systemet må fungere.
Formelt er det SD som fastsetter forskrifter for sjøtransport, men KYV bidrar mye inn i slikt arbeid.

8.3.3. Bane NOR

Informanten hos BN opplyser at samfunnssikkerhet i BN har to dimensjoner. Den ene er hvordan samfunnsikkerhetsansvaret ivaretas i egen sektor og overfor egne kunder. Dette er fire-delt og handler om sikring av objekter, digital sikkerhet, nasjonal sikkerhet og beredskap-/krisehåndtering. Kundene skal føle seg trygge og sikre på BNs områder. Innholdet i dette oppfattes som klart.
Den andre dimensjonen er at BN som virksomhet har et samfunnsansvar. BN hevder det ikke er helt avklart hva som her legges i begrepet samfunnsansvar, men det handler om det ansvaret BN har som transportaktør relatert til samfunnets og statens kriser. Det er pågående arbeid om dette i form av to initiativer. Det ene er definering av GNF-er med tilhørende objekter og infrastruktur. Det andre er utredning av eventuelt behov for en forskrift som regulerer dette samfunnsansvaret.

Arbeidet med samfunnssikkerhet skjer på tre nivåer, sier BN. Det er virksomhetskritisk, samfunnskritisk og statskritisk[60]. GNF-en transport er delt i fire og definert for hver transportform. Jernbanetransport er videre delt opp i tre funksjoner: tjenester, infrastrukturforvaltning og trafikkstyring/overvåking. Under hver funksjon er det kartlagt og skadevurdert objekter og infrastruktur. Resultatet av det er gradert og BN vil ikke si mer om det annet enn at forsvarets behov er med i vurderingene.

BN sier at digitalisering påvirker og setter i høy grad preg på virksomheten. Det er i høyeste grad den digitaliserte jernbanen, med bl.a. GSM-R og ERTMS som utgjør den største sårbarheten. Digital sårbarhet og digital risiko opplyses å være helt på topp blant fokusområdene i konsernet. Det handler om driftsstabilitet, oppetid, pålitelighet og tilgjengelighet. Med et trusselbilde som endrer seg og som stadig er mer krevende å holde tritt med, er det et kontinuerlig løp med å ha riktige barrierer og være så robust som mulig.

[60] Informanten bruker dette ordet, men gir uttrykk for usikkerhet om det er korrekt begrep

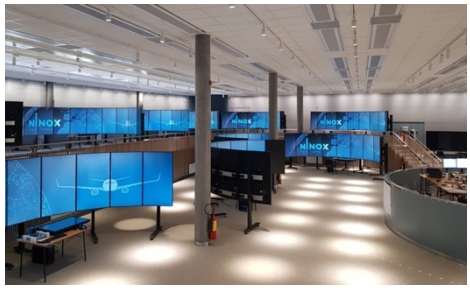
BN bekrefter at digitalisering i stor grad benytter GNSS. I stedet for å gå gjennom alle tekniske aspekter ved det og beskrive sårbarhet med mulige tiltak, går BN heller rett på konsekvensen og spør: «Hva er konsekvensen for BN hvis f.eks. en solstorm slår ut GNSS?» BN opplyser å ha et konsekvensfokus på dette. Her kommer BNs beredskapssystem inn i bildet som håndterer hendelser på taktisk, operasjonelt og strategisk nivå.

8.3.3. Avinor

Avinor er eier av kritisk infrastruktur og informanten hevder at konsernet har en viktig posisjon for at daglig drift av samfunnet skal kunne gå rundt. I en situasjon med krise/krig i en totalforsvarssammenheng så vil luftfarten være viktig for å støtte forsvarets behov. Skillet mellom samfunnssikkerhet og statssikkerhet påvirker i liten grad Avinors rolle. Avinor understøtter statens interesser også i det daglige. Avinor opplyser at konsernet har tre «pilarer» i forbindelse med samfunnssikkerhet og lufttransport. Det første er den daglige transporten av personer og gods i landet og ut/inn av landet. Det andre er syketransport/luftambulanse der Avinor har en viktig rolle i sammenheng med helsevesenets funksjonalitet. Det tredje er som aktør i totalforsvaret og det som ligger i det for statens interesser. Informanten opplyser å være ukjent med KIKS.

Avinor ivaretar sin rolle i dette gjennom interne prosesser og vurderinger som skal ivareta alle aktørene ved en lufthavn eller brukerne av et luftrom. Det finnes også ulike forordninger og sektorregelverk. Avinor har «§10-planen»[61] som bl.a. beskriver Avinor sine strategiske og samfunnsmessige disposisjoner inn mot luftfartens samfunnsnytte. Hvilken rolle Avinor skal spille i å støtte oppunder luftfartens bidrag til samfunnssikkerhet beskrives gjennom eierstyringen der man veier ulike argumenter og får politiske styringssignal.

Avinors informant er tydelig på at digitaliseringen påvirker virksomheten. Et eksempel på utnyttelse av digitale muligheter er prosjektet Remote Tower. Her skal lufttrafikken på inntil 15 lufthavner fjernstyres fra et kontrollsenter i Bodø. Det påvirker lufttransportens rolle ved at en rekke kontrolltårn legges ned, men Avinor sier det neppe påvirker lufttransporten rolle inn mot



Figur 24: Avinors Remote Control Centre i Bodø (kilde: https://avinor.no/flysikring/vare-tjenester/remote-towers/)

[61] Refererer til §10 i Avinors vedtekter, https://avinor.no/konsern/om-oss/konsernet/vedtekter

samfunnssikkerhet. Lufttransportens rolle i samfunnssikkerheten er mer eller mindre den samme, men digitaliseringen endrer arbeidsmåten. Gamle risikoer lukkes og nye åpnes. Det er en del av utviklingen. Avinors regime for håndtering av endringsprosesser ivaretar dette. Informanten slår fast at «digitaliseringen vil gi vridninger i bruksområder, men vi vil alltid trenge flyplasser og lufttrafikktjeneste».

Avinor lager ikke forskrifter for luftfarten, men utarbeider lokalt regelverk for alle lufthavner for å ivareta sikkerheten. Alle aktører som har aktiviteter på lufthavnene må følge disse.

8.4. Digitalisering, GNSS og sikkerhetsstyring

I dette del-kapitlet gjengis hvordan de ulike etatene/virksomhetene har svart på annen gruppe av spørsmål i intervjuguiden med tema digitalisering, GNSS og sikkerhetsstyring. Temaene som berøres er om sikkerhetsstyringen fanger opp digitaliseringen, hvordan GNSS brukes som kilde til nøyaktig tid, risikovurderinger relatert til GNSS, digitale verdikjeder, IKT-sikkerhet relatert til GNSS og om hvilke standarder eller kunnskapssyn som er lagt til grunn for sikkerhetsstyringen.
Det fremkommer at digitaliseringen er omfattende og påvirker mange sentrale forhold. SVV etterlyser ansvarsavklaring når nye aktører som ikke er myndighet blir sentrale i transportsystemet. Det er fokus på sikkerhetsstyring relatert til digitalisering. Alle nevner ISO 27000-serien og KYV og BN nevner NIS-direktivet. Avinor skiller seg ut med et tydelig fokus på å redusere avhengighet av nøyaktig tid fra GNSS. For de andre er dette sett på i varierende grad og flere har sikkerhetskritisk avhengighet av GNSS. Kunnskapssynet kan være ulike i ulike deler av organisasjonen.

8.4.1. Statens vegvesen

Digitalisering av samferdselssektoren påvirker SVV på mange måter, også hvordan sikkerhetsstyring utøves. SVV påpeker at skal data benyttes til å ta beslutninger av eksterne må man kunne garantere for opprinnelsen av dataene og at de ikke er påvirket underveis til mottakeren. En ting er å informere trafikanter som tar avgjørelser som de selv er ansvarlige for basert på dette. Noe helt annet er å distribuere data til maskiner som tar avgjørelser. Her mener SVV at ansvarsspørsmålet ikke er avklart og hevder det er en utfordring at digitaliseringen fører til at kjøretøy og sjåfører blir avhengig av flere systemer som SVV ikke har myndighet over.

Eksempel på dette er digitale kommunikasjonssystem og systemer for posisjonsbestemmelse. SVV mener at innenfor dette er det behov for utvikling av nytt regelverk.

SVV er en stor organisasjon med ulike fagområder og ulike syn på risiko- og sikkerhetsstyring. SVV er en ingeniørtung organisasjon og informanten sier håndbøkene som gjelder bærer preg av det naturvitenskapelig synet. Størrelser tallfestes og risiko blir sannsynlighet ganger konsekvens. Deler av organisasjonen, som jobber med mindre «harde fakta», vil likevel legge et mer samfunnsvitenskapelig syn til grunn. SVV opplyser at innenfor IKT brukes ISO 27001[62]. Internrevisjon og kvalitetsrevisjon følger sine egne spesifikke standarder. ALARP-begrepet brukes ikke i det daglige, men det er likevel det som legges til grunn. Null-visjonen om null drepte og hardt skadde i trafikken forutsetter kontinuerlig fokus på at risiko skal være så lav som mulig.
Informantene fra SVV er ikke kjent med om det er gjort en kartlegging av avhengigheter av GNSS, ei heller om det er gjort noen risikoanalyse av evt. bortfall av GNSS. Det er mulig å gå inn i spesifikasjonene for de ulike systemene og finne ut om det brukes en tidssynkroniseringsmekanisme mot GNSS, men det er ukjent om det finnes en oversikt som viser samlet eksponering mot tidsangrep på GNSS. SVV opplyser at Veitrafikksentralen Øst henter tid fra «ntp.uio.no»[63].

FoU-miljøet i SVV deltar i det faglige samarbeidet knyttet til GNSS bortfall og interferens som ledes av Nkom og Norsk Romsenter. SVVs rolle i håndtering av GNSS-forstyrrelser har vært diskutert. SVV ser ikke at det vil være kritisk for veitransporten ved et evt. bortfall av GNSS. Det jobbes med teknologi som kan registrere GNSS-forstyrrelser. SVV benytter oftest GNSS for landmålingsformål og entreprenørene bruker det i økende grad for maskinstyring. SVV sier at erfaring viser at for landmålerne er mobildekning en større utfordring enn GNSS-problemer.

I den skriftlige besvarelsen som den ene informanten fra SVV har oversendt er spørsmål 5, 7 og 8 i annen gruppe i intervjuguiden besvart med «ukjent for respondentene» og «et omfattende spørsmål som vi ikke har grunnlag for å svare på».

[62] Internasjonal standard for informasjonssikkerhetsstyring
[63] Jeg har spurt tidslaboratoriet hos Justervesenet om hva som ligger i opplysningen fra SVV om veitrafikksentralens kilde til tid. Der opplyses det at dette er en stratum 2-tjener som henter synkronisering fra en eller flere stratum 1-tjenere. Stratum 1 kan være både fra GPS og andre kilder til UTC-tid. Kilden SVV bruker skifter mellom GPS og atomklokke og benytter stratum 1-tjenere i Danmark og Sverige.

8.4.2. Kystverket

KYVs digitalisering av egne tjenester, som AIS og SafeSeaNet[64], anser KYV som viktigst. Los-tjenesten opereres også med digital støtte. Ved sjøtrafikksentralene brukes digitale systemer for å holde oversikt, kommunisere, osv. De digitale systemene, og operasjonen av dem, får stadig større betydning for KYV. Sikkerheten og tilgjengeligheten på systemene får større oppmerksomhet og det er større krav til profesjonalitet i operasjonen av dem. KYV sier digitalisering ombord i skip får ingen direkte betydning for hvordan KYV utøver sikkerhetsstyring. Likevel, digitalisering ombord, som f.eks. GNSS, får en betydning for KYV ved at skipene baserer seg i større grad på det enn på tradisjonell observasjonsbasert navigasjon. Da vil støtte fra KYV for den nye navigasjonsmetodikken være viktigere enn før. Fyr og merker har gått fra å være den dominerende måten til å bli en av flere måter å navigere på. KYV hevder at det som var normalen før er i realiteten nå en reservenavigasjon. I lys av dette jobber KYV og Sjøfartsdirektoratet sammen om å lage en maritim cybersikkerhetsstrategi (pr. okt. 2020).

KYV opplyser at det ikke er laget noen konkret oversikt over hvordan nøyaktig tid anvendes innen sjøtransport. Det henvises til underlaget KYV utarbeidet til nasjonal PNT-strategi og som ble oversendt til Norsk Romsenter i 2017[65]. Konklusjonene der er fortsatt gyldige og strategien fikk en tydelig samfunnssikkerhetsvinkling. Det gjelder også betraktninger rundt scenario «bortfall av GNSS».

Figur 25: Kystverkets AIS basestasjon på Svalbard (kilde: https://www.tv2.no/a/11651762/

KYVs konklusjons den gang var at kommunikasjonssystemer som kystradio og NAVTEX[66], som opereres av Telenor, i liten grad er avhengig av GPS. Ombord i skipene er kritisk tidsavhengighet avgrenset til tidsstempling av logger. AIS ombord i alle skip som er innenfor samme basestasjonsområde vil være synkronisert mot klokken i den aktuelle basestasjonen på land. Denne er GPS-basert, men den har en intern klokke som vil holde en god stund selv om GPS skulle falle bort. KYV mener at det mest kritiske med bortfall av GPS er at skipet mister posisjonen i AIS. Da forsvinner verdien av

[64] Nasjonal meldeportal der skipsfarten sender pliktige ankomst- og avgangsopplysninger til myndighetene (https://www.kystverket.no/safeseanet)
[65] Informanten hos KYV er kjent med min deltakelse i arbeidet med PNT-strategien og at jeg derfor har tilgang til informasjon KYV utarbeidet i forbindelse med dette.
[66] NAVTEX er et radiobasert system for å distribuere maritime sikkerhetsmeldinger til skip

systemet fordi man har ikke lenger mulighet til å stedfeste all annen AIS-informasjon. Ute på havet utenfor dekning av basestasjonene er det mer usikkert hva som vil skje. Det er mulig skipenes klokker vil drifte uavhengig av hverandre og da vil ikke AIS fungere mellom skip. KYV bekrefter at AIS er et sikkerhetskritisk system. Det er en viktig barriere mot skipskollisjoner og det gir kritisk grunnlagsinformasjon for å ha oversikt over trafikksituasjonen. KYV sier AIS er 100% avhengig av GPS med tanke på posisjon, men ikke fullt så avhengig av nøyaktig tid.

KYV hevder å være bevisst på digitale verdikjeder, men har i første omgang fokus på tjenester KYV produserer selv. Eksempel på det er AIS som en tjeneste som KYV produserer for egne sjøtrafikksentraler. Ettersom sjøtrafikksentraltjenesten motvirker ulykker betraktes AIS som en tjeneste som produseres for samfunnssikkerhetsarbeidet. Der hvor det er tjenesteleverandører ettergås avtaler og vilkår i avtaler ved revisjoner.

KYV sier at det er ingen fremtredende holdning hos KYV at GNSS betraktes som IKT. I den grad tid og synkronisering er en del av revidering eller styring av leveranser så er det et moment, men GNSS, eller nøyaktig tid, har ikke vært oppe som eget tema. Det KYV er avhengig av får etaten gjennom sambandsleveranser. Hvis sambandsleverandøren er avhengig av GNSS for å synkronisere nettet er KYV det også. KYV sier at Telenor tidligere har opplyst til KYV at de ikke er avhengig av GPS, men det begynner å bli noen år siden og det er ikke sikkert konklusjonene er de samme nå.

I sin sikkerhetsstyring legger KYV til grunn NS5832 og NS5814, men følger ikke nødvendigvis alt til minste detalj. Det brukes en god del kvalitativ metode og vurderinger i tillegg til kvantitativ metode. Når det gjelder å sikre kritiske system så brukes kvalitative metoder. Det vurderes sjøsikkerhetstiltak og det måles ulykkesfrekvens, skader og omkomne. Sannsynlighet for ulykker beregnes ut fra utseilt distanse og historiske tall for et begrenset geografisk område. Det er litt forskjellig metodikk og nøyaktighet i det å vurdere virkning av potensielle tiltak. Hvis det er kjent teknologi er det greit. Hvis det er ny teknologi, f.eks. å analysere skipets seilas automatisk, så er det mer komplisert å vurdere hvor godt det blir. Ved sikring av havneanlegg brukes metodikk for sikringsrisikoanalyse.

8.4.3. Bane NOR

BN opplyser at digitaliseringen påvirker infrastrukturen og måten det jobbes på i jernbanen i stor grad. Utviklingen har gått fra en tradisjonell jernbane basert på gammel teknologi der GSM-R var det nyeste, til nye systemer og nytt digitalt signalsystem (ERTMS). Dette setter helt andre krav til arbeidet med sikkerhetssystemet, sier informanten. BN blir stadig utfordret på å tenke sikkerhet og sikkerhetsstyring jo mer som digitaliseres, og det jobbes etter et cybersikkerhetsfokus som var ikke-eksisterende for noen år tilbake. Informanten sier dette har stor innvirkning på organisasjonen og for mange har nok dette være nytt og uvant. Digitaliseringen hos BN endrer sikkerhetsstyringen på den måten at det settes et nytt og betydelig fokus på å vurdere sårbarheter og trusler i den digitale infrastrukturen. BN stiller sikkerhetskrav på områder som ikke ble gjort tidligere og det har effekt på leverandørene våre.

Informanten fra BN er ikke kjent med om det finnes en helhetlig oversikt over tidsavhengighet i jernbanesektoren, men BN har god kjennskap til det for egen del på utstyr brukt i GSM-R og ERTMS.

BN opplyser at GSM-R er informasjonsbærer i ERTMS og GSM-R bruker tid fra GNSS til synkronisering. Det samme gjelder BNs eget transmisjonsnettverk[67]. Dette gir sikkerhetskritisk avhengighet av GNSS. Sikkerhetsstyringen må derfor ta utgangspunkt i hvilke risikoer og sårbarheter en slik avhengighet kan medføre. BN erkjenner at man ikke har kontroll over tilgangen på GNSS så BN prøver å bygge robusthet med fokus på opprettholdelse av tjenester. Et tiltak i dette er at tidssignal fra GPS tas inn i nettet flere steder i Norge. Det er bygget inn utstyr som kan holde nøyaktig synk over en lang periode. BN mener dette vil fungere ved bortfall av GPS, men kanskje ikke være like godt mot manipulasjon av tidssignalet. Bortfall av GNSS er påpekt som sårbarhet ifm. risikovurderinger, men informanten tror ikke det er utført noen spesifikk vurdering av dette. BN har bygget inn en teknisk barriere slik at svikt i GSM-R vil gi automatisk togstans.

Relatert til de systemene som er nødvendig for sikker operativt drift, dvs. GSM-R, ERTMS og transmisjon, så eier og drifter BN egen infrastruktur. BN mener det betyr at problematikk rundt digitale verdikjeder er mindre aktuelt fordi BN selv sitter med oversikten fra ende til ende. Det som likevel kan være en utfordring er at ansvaret for ulike deler av helheten ligger i ulike

[67] Nasjonalt og regionalt transportnett for tele/data.

organisatoriske enheter internt hos BN. Det gir ulike leverandører som leverer ulike deler av helheten og der risiko derfor håndteres avgrenset av personer på ulike steder i organisasjonen. BN sier at hvis de hadde hatt leid løsning hadde det vært krevende å sikre kontroll på hvor data og informasjon går mellom A og B.

BN innser at jernbaneinfrastruktur mer og mer smelter sammen med IKT. Den operative delen av den digitale infrastrukturen er sertifisert etter ISO 27001. Standarden ble innført samtidig med etableringen av GSM-R. Det som har kommet til av nye ting senere er tatt inn i samme systematikk. Konfidensialitet, integritet og tilgjengelighet legges til grunn. Mange av de som er rekruttert de siste årene kommer fra IKT-miljø med sikkerhetsrelatert bakgrunn. Informanten har inntrykk av at når BN sammenlikner seg med tilsvarende organisasjoner i andre land så har de andre en tilsynelatende mer tilfeldig tilnærming til dette. Lov om digital sikkerhet og arbeid med NIS-direktivet er også relevant her.

Den kjøreveikritiske delen av BNs sikkerhetsstyringssystem er ISO-sertifisert. BN bruker ALARP mot det mest kritiske for verdivurderinger, sikring av objekter og informasjonssystemer. Da er fokuset på tilsiktede uønskede handlinger. Her brukes ALARP og kost/nytte-analyser.

8.4.4. Avinor

Avinor opplyser at digitaliseringen av luftfarten påvirke de verktøyene som brukes. De største endringene ligger i dette. Det gir behov for å ha kontinuerlig kontroll på krav til sikkerhet, robusthet, oppetider, integritet, osv. Det er en kontinuerlig utvikling der mye skjer som respons på europeisk regelverk i form av direktiver fra EU.

Avinor opplyser å ha en svært detaljert oversikt over avhengighet av tid fra GNSS. Dette gjelder særlig eget område, men også hele systemet i den grad det har vært mulig. Avinor har gjennomført et kartleggingsprosjekt i konsernet på tidsavhengighet og hvordan dette kunne gi sårbarheter. Noe av dette er relatert til ny teknologi som ADS-B og WAM. Det er gjort risikovurderinger og det er tatt inn i virksomhetens risikobilde. Det er tatt flere grep, både tekniske og operative, for å redusere den sårbarheten som ble avdekket. Avinor har gjennomført tiltak for å stå på egne ben uten å være avhengig av tid fra GNSS, men informanten vil ikke å gå mer i detalj da dette er informasjon Avinor ønsker å ha kontroll på.

Der hvor Avinor leier nettkapasitet settes det krav til tilgjengelighet på nett, integritet og konfidensialitet. Det gjøres i kontrakten med leverandøren. Avinor er kjent med DSBs rapport om risikovurdering av digitale verdikjeder, men praktiserer ikke metodikken som presenteres. Luftfarten er internasjonal og det går verdikjeder som strekker seg langt utover Norges landegrenser. Avinor har fokus på sikker informasjon foran det å sikre hele verdikjeden. F.eks. har Telenor en beredskapslinje som vår via Sverige som har akseptabel risiko sett med Avinors øyne.

Avinor sier det er mange ulike standarder og syn som virker inn på sikkerhetsstyringen avhengig av hvilket system som betraktes. I utgangspunktet har Avinor krav til å følge forskjellige sikkerhetsstyringssystemer i forbindelse med EU Basic Regulation 2018/1139 (EASA, 2018) som regulerer mange av de sikkerhetsmessige problemstillingene rundt lufthavndrift og flysikring. Videre finnes begreper som ATM[68] security og det er hensyn å ta relatert til objektsikkerhet. Det som er typisk for disse EU-standardene, sier Avinor, er at de sier klart hvordan du skal gjøre mange av oppgavene, og hvilke tall og mål du skal legge til grunn for å oppnå det. For IKT-området legger Avinor til grunn ISO 27000-serien.

8.5. Transport og GNSS

I dette avsnittet gjengis hvordan de ulike etatene/virksomhetene har svart på tredje gruppe av spørsmål i intervjuguiden med tema transport og GNSS. Spørsmålene er tilpasset spesielle forhold hos hver aktør så svarene er ikke uten videre sammenlignbare. Temaene som berøres er GNSS-sårbarhet relatert til veiprising, veibyggeprosjekter, automatisering/selvkjøring, utfasing av Kystverkets DGPS-system, posisjonsbestemmelse av materiell langs togspor, og GNSS relatert til fjernstyre kontrolltårn og droner.

8.5.1. Statens vegvesen

Informanten er ikke kjent med om det er foretatt noen konsekvensvurdering hos SVV av bortfall/redusert tilgang til GNSS ved evt. innføring av GNSS-basert veiprising. Det er derimot godt kjent for SVV at mange aktiviteter innen veisektoren forutsetter bruk av GNSS, ikke minst relatert til veibyggingsprosjekter. Et uventet bortfall som påvirker kritiske funksjoner vil derfor kunne få uheldige konsekvenser. SVV holder på å utvikle et veikart for automatisert transport og vil trekke inne denne problematikken i prosjektet.

[68] Air Traffic Management.

8.5.2. Kystverket

Informanten sier at tidligere var KYV av den oppfatning at EGNOS[69] ville være et godt alternativ til IALA-DGPS[70], men at det har endret seg. Forbedring av nøyaktighet i posisjonsbestemmelse sammenliknet med kun bruk av GNSS betraktes som liten. GNSS er nøyaktig nok i seg selv. Det EGNOS kan brukes til, og som er relevant for samfunnssikkerheten, er at systemet kan brukes til å alarmere skip hvis GPS-posisjonen blir usikker. Da kan besetningen bytte navigasjonsmetode. SBAS[71] er ikke en del av typegodkjenningen for maritime navigasjonsmottakere. Det må derfor gjøres et internasjonalt standardiseringsarbeid før SBAS/EGNOS kan tas i bruk. Andre land som legger ned IALA-DGPS argumenterer med at GPS er nøyaktig nok alene og at det kan benyttes RAIM[72]-metodikk.

8.5.3. Bane NOR

I dag benyttes GPS for flåtestyring av rullende materiell. Dette er ikke sikkerhetskritisk posisjonsbestemmelse. For sikkerhetskritisk posisjonsbestemmelse brukes baliser og aksel-tellere. En balise vil fortelle at toget var akkurat der balisen ligger på det tidspunktet toget passerte, men den kan ikke si hvor toget er etter at det har passert før det kommer til neste balise. BN sier det ikke er mulig å si i dag om GNSS vil bli det eneste systemet for sikkerhetskritisk posisjonsbestemmelse i framtiden. Informanten mener det likevel er sannsynlig at bruken av GNSS vil øke. Jernbanen vil ha økt behov for nøyaktig posisjonering framover. GNSS er billig, pålitelig, nøyaktig og folk flest har stor tillit til det. Her ligger også risikoen, mener BN.

8.5.4. Avinor

Avinor opplyser at det er gjort vurderinger av bortfall/redusert tilgang til GNSS relatert til prosjektet med fjernstyrte tårn. Det foregår også vurderinger knyttet til utfasing av bakkebaserte

[69] EGNOS = European Geostationary Navigation Overlay Service. Dette er et EU-eid satellittsystem som brukes sammen med amerikanske GPS over Europa. Dette gir økt nøyaktighet i posisjonsbestemmelse og økt systemintegritet. En egen tjeneste i EGNOS brukes av luftfarten for innflyging til flyplasser. Tjenesten kan også brukes av skip.

[70] IALA er en internasjonal sammenslutning av «kystverkene» i verden. IALA har utarbeidet en standard for Differensiell GPS (DGPS). Systemer bygget etter standarden sender ut korreksjonsdata som fartøy kan bruke sammen med GPS for å øke nøyaktigheten i posisjonsbestemmelsen. KYV har en rekke slike installasjoner.

[71] SBAS = Satellite Based Augmentation System. Dette er et samlebegrep for systemer av typen EGNOS

[72] RAIM = Receiver Autonomous Integrity Monitoring. Teknikk der mottakeren selv varsler hvis integriteten i GNSS-signalene ikke er god nok basert på samtidig tilgang på flere satellitter enn nødvendig for posisjons-bestemmelse.

PNT-systemer til fordel for GNSS. Dette baseres på EU forordning 1048/2018[73] og det skal ferdigstilles en transisjonsplan innen utløpet av 2020.

Informanten har ikke detaljkunnskap om Avinor Flysikrings arbeid med å tilrettelegge for droner, men antar de problemstillingene som ligger til grunn for dette intervjuet også er kjent i prosjektet. Prosjektet skal etablere et UTM[74]-system hvor det bl.a. er sikkerhetsmessige utfordringer ved droners tilgang til luftrommet.

[73] (EU) 2018/1048 laying down airspace usage requirements and operating procedures concerning performance-based navigation (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1048)
[74] Unmanned Aircraft System Traffic Managemet. Parallell til ATM, men for droner.

9. DISKUSJON

I dette kapittelet drøfter jeg forhold som har fremkommet i intervjuene opp mot innhold i kapitlene i empirien. Dette vil danne grunnlag for å besvare forskningsspørsmålene i neste kapittel.

9.1 Etatenes digitalisering og sikkerhetsstyring

Faktainnsamlingen bekrefter det bildet jeg beskrev av digitalisering av transportsektoren i kapittel 3. I alle del-sektorer foregår en omfattende digitaliseringsprosess som berører transport-midler, trafikkovervåking og -styring og utøvelse av etatenes/virksomhetenes funksjoner. Dette viser at nøyaktig tid er en sentral ressurs på ulike nivåer i transportsystemet og at GNSS som regel er hovedkilden. Bruken av tid spenner fra styring av lyskryss til kontroll av flytrafikk og kontor-IKT hos etatene.

Det er viktig å forstå hvordan teknologiske endringer, organisatoriske endringer og endringer i forutsetninger for hvordan organisasjonen fungerer, påvirker risikobildet. Kystverket viser forståelse for dette når de uttaler at digitaliseringen ikke nødvendigvis gjør at risikoen blir høyere eller lavere, men den blir helt sikkert annerledes. Bane NOR er også tydelig på at digitaliseringen av jernbanen medfører en stor omlegging fra gammel til ny teknologi og at dette igjen har gitt et mye mer omfattende opplegg for sikkerhetsstyring. Vegvesenet setter fokus på hvordan utviklingen medfører oppdeling av ansvarsområder og at nye aktører eier infrastruktur. Hvordan håndtere at nye aktører uten myndighetsansvar får en sentral rolle?

Det er mange faktorer som spiller inn på hva som er et godt sikkerhetsstyringssystem for den enkelte virksomhet. Det er viktig å være bevisst på hva man kan gjøre noe med og hva man ikke kan gjøre noe med. Det siste vil utgjøre rammebetingelser for sikkerhetsstyringen. Innenfor disse rammene må det identifiseres hensiktsmessige virkemidler for å nå de ønskede målene. Avinor sier at i deres internasjonale/europeiske sektorregelverk er ofte målene tallfestet. Mitt inntrykk etter faktainnsamlingen er at det ikke nødvendigvis er tilfellet for de andre del-sektorene.

Det betyr at etatene/virksomhetene må jobbe med risikoreduksjon slik at de når de målene de selv har identifisert. Til en viss grad bruker de ALARP der kost/nytte-analyser legges til grunn, men det ser ut til å være et økende fokus på å utarbeide risikoakseptkriterier for den enkelte organisasjon eller enkelte funksjon/aktivitet. Dette prinsippet legges også til grunn i den siste stortingsmeldingen om samfunnssikkerhet og utøvelse av ansvarsprinsippet.

Digitaliseringen skjer ikke bare internt i del-sektorene, men også på tvers av del-sektorene og på tvers av samferdselssektoren og andre deler av samfunnet. Kritiske infrastrukturer er blitt gjensidig avhengig av hverandre og alle samfunnsfunksjoner er avhengig av transport. En fungerende transportsektor er derfor av stor betydning for et fungerende samfunn og tilstrekkelig god samfunnssikkerhet. Det gir komplekse sammenhenger med digitale verdikjeder som det er utfordrende for aktørene å ha oversikt over. Dette viser at Perrows teori, som beskriver en ikke-lineær ulykkesmodell, sannsynligvis er relevant for norsk samferdsel. På grunn av kompleksiteten begrenses organisasjoners evne til å forutse og organisere arbeidet med risiko og sikkerhet.

Digitaliseringen av samferdselssektoren, og alle endringer som skjer i lys av det, ser ut til også å ha en effekt på begrepsbruken. Der det før var snakk om transport av mennesker er det nå snakk om mobilitet. Begrepet brukes i mange offentlige dokumenter, men gis sjelden en forklaring og det er ikke definert. Mobilitet ser ut til å handle om å kunne bevege seg raskt, enkelt og effektivt ved hjelp av fleksible løsninger når man har et transportbehov. Dette oppnås gjennom å skape en helhet av de ulike transportformene som fyller den reisendes behov i større grad enn at den reisende må tilpasse seg ulike transportformer.

Safety-I/Safety-II

Jeg har ikke funnet noe som tyder på at aktørene legger til grunn safety-II-tankegang. Resiliens har blitt et mye brukt begrep, men det ser ikke ut til at begrepets kilde, Resilience Engineering og Hollnagels tanker om dette, er lagt til grunn for bruk av begrepet. Etatene legger ned betydelig ressurser i å utvikle og etterleve et sikkerhetsstyringssystem slik at feil og ulykker unngås, men det er like fullt et safety-I-fokus i dette arbeidet. I intervjurunden er det ingen som har signalisert at de bruker ressurser på å analysere hvorfor ting går bra eller at de legger til grunn prinsippene som kjennetegner en resilient organisasjon. Mitt inntrykk etter dette er at resiliens brukes synonymt med robusthet i en safety-I-tankegang med fokus på eget teknisk utstyr som muliggjør en operativ funksjon.

Digitale verdikjeder

Det er interessant å se etatene/virksomhetene ulike forhold til digitale verdikjeder. Ingen av dem legger til grunn metodikken DSB har publisert. Vegvesenet henter tid fra en tidsserver i utlandet, men har ikke gitt noe informasjon som tyder på aktivt forhold til verdikjeden. Kystverket sier de bruker internrevisjonsverktøyet overfor leverandører på dette. Avinor opplyser at de ikke er så opptatt av hvor informasjonen går så lenge de er trygge på at informasjonen er sikker. Bane NORs svar er interessant fordi det snur litt på hele problemstillingen. Bane NOR opplyser at fordi de eier egen infrastruktur har de kontroll på hele dataflyten og at verdikjeder med eksterne leverandører og fare for manglende kontroll ikke er en relevant problemstilling. Derimot opplever de denne problematikken internt. Ansvaret for infrastrukturen er fordelt på ulike organisatoriske enheter og utfordringer rundt kommunikasjon på tvers gir tilsvarende effekter på risiko som når ulike eksterne leverandører bidrar med hver sin del av helheten. På bakgrunn av dette er et av mine forslag til videre arbeid å gjøre en studie av hvordan interne organisatoriske forhold i en virksomhet kan skape digital verdikjede-problematikk internt i egen organisasjon.

9.2 Transport og samfunnssikkerhet

Alle etatene/virksomhetene som har blitt intervjuet er tydelig på at deres sektor er viktig for samfunnssikkerheten, men begrunner det noe ulikt. Vegvesenet vektlegger at opprettholdelse av framkommelighet ved at veier og broer er åpne er viktig for nødetater, godstransport og militær aktivitet. Kystverket tar utgangspunkt i sjøtrafikkens betydning for å holde samfunnet i gang og sier at det å arbeide for å unngå ulykker og holde leder og havner åpne er del-sektorens viktigste bidrag til samfunnssikkerheten. Bane NOR har også et todelt fokus. Det ene er å sikre infrastruktur og opprettholde funksjonalitet i egen del-sektor for å ivare samfunnssikkerhets-ansvaret overfor egne kunder. Det andre er å ivareta ansvaret som nasjonal infrastruktureier ved statens og samfunnets kriser. Avinor vektlegger sin rolle som nasjonal infrastruktureier og viktigheten av å holde flyplassene åpne for persontransport og ambulanseflytjenesten. Avinor har også en viktig oppgave rettet mot totalforsvaret ved å levere flysikringstjenester og åpne flyplasser for luftforsvarets bruk. Ved hjelp av Avinors tjenester kan luftforsvaret levere suverenitetshevdelse i norsk luftrom som en faktor i statssikkerheten.

Relatert til de tre overordnede målene for samfunnssikkerhet i samferdselssektoren har alle etatene/virksomhetene fokusert på det å sikre pålitelighet og framkommelighet når de har blitt

spurt om sin betydning for samfunnssikkerheten. Fokuset ser ut til å ligge på å holde infrastrukturen operativ og åpen slik at trafikken kommer fram, men implisitt i dette ligger at ulykker unngås. Kystverket er den etaten som er tydeligst på at målet om å unngå ulykker er viktig i deres arbeid med samfunnssikkerhet.

Samfunnssikkerhet knyttes til folks trygghetsfølelse. Ettersom en fungerende transportsektor er en viktig faktor for mange kritiske samfunnsfunksjoner, betyr det at transportsektoren også må bidra til denne tryggheten. Folk flest må føle seg trygge på at sannsynligheten for ulykker er lav nok til at de kan stole på transportsystemet. Mobilitetstjenestene man trenger må være der når man trenger det. Det samme gjelder totalforsvar og statssikkerhet. Myndighetene må være tilstrekkelig trygge på at infrastruktur og tjenester er robust nok til å kunne dekke nødvendige transportbehov til riktig tid selv i en ekstraordinær situasjon. Datagrunnlaget viser at i en moderne, digitalisert transportsektor kan ikke det oppnås uten robust tilgang på nøyaktig tid.

Alle etatene/virksomhetene har fått spørsmål om digitalisering og eventuell betydning av GNSS. Vegvesenet sier digitaliseringen påvirker på mange måter bl.a. sikkerhetsstyringen. Digitalisering har medført at både kjøretøyet og sjåføren er avhengig av teknologi som ligger utenfor Vegvesenets myndighet. Vegvesenet gir uttrykk for at det mangler formelle avklaringer om ansvar i dette bildet. Kystverket fokuserer digitalisering av egne tjenester og i liten grad digitalisering ombord i skip. Drift og bruk av digitale systemer får stadig økene betydning og etaten har sett behovet for en cybersikkerhetsstrategi. Bane NOR har også digitalisert infrastruktur for den operative driften og har sikkerhetskritisk avhengighet GPS som tidskilde for synkronisering av kommunikasjonsnett som inngår i digitalt signalsystem.
Hos Avinor påvirker digitaliseringen flere av de verktøyene som brukes med krav til kontinuerlig kontroll på sikkerhet, integritet, osv. Avinor Flysikring har innført ny teknologi for overvåking av flytrafikken der funksjonaliteten er kritisk avhengig nøyaktig tid.

Dette viser at digitaliseringen påvirker hvordan etatene løser sine oppdrag både for intern drift og i systemer som er del av operative løsninger med betydning for sikkerhet. Det viser også at evnen til å fylle rollen i samfunnssikkerheten er sårbar for bortfall av tilgangen til nøyaktig tid. Det ser ut til at det kun er Avinor som har gjort en spesifikk analyse av avhengighet av tid fra GNSS. Det kan indikere et forbedringspotensial når det kommer til bevissthet om bruk av kilder til nøyaktig tid

Problematikken som beskrives her er i realiteten et eksempel på hva som kan skje når en vellykket teknologisk løsning tas mye i bruk. GNSS er tilgjengelig, pålitelig og gratis og anvendelsesområdene har blitt svært mange. Dette gir ubevisste avhengigheter og sårbarheter. Dette gjelder ikke bare GNSS og nøyaktig tid, men også andre teknologier. Et eksempel er bruken av BankID som Lysne-utvalget skriver om. Dette har blitt den mest brukte måten å identifisere seg på i Norge ved bruk av digitale tjenester på nettet og har mer enn 3 millioner brukere. En svikt i denne teknologien vil kunne ha store konsekvenser for befolkningens tilgang til digitale tjenester.

9.3 Håndtering av tidsavhengighet

Faktainnsamlingen viser at GNSS er den foretrukne kilden til nøyaktig tid og at dette håndteres ulikt hos etatene/virksomhetene. Det fremkommer stor variasjon i hvordan etatene forholder seg til GNSS som et system som leverer noe de er helt avhengig av. Det fremkommer at Kystverket og Bane NOR har GNSS-avhengige sikkerhetskritiske systemer/funksjoner.

Dette indikerer ulik bevissthet rundt tid som ressurs og denne ressursen betydning. Avinor har gått grundig til verks og innført ny teknologi som gjør at virksomheten vil klare seg godt selv om tilgangen på tid fra GNSS skulle bli redusert eller falle bort. Avinors informant har ikke villet utdype hva dette innebærer, men basert på egen erfaring vil jeg si at det sannsynligvis er snakk om atomklokker og trolig flere klokker med geografisk spredning. Relatert til bow-tie kan atomklokker utgjøre både aktive og reaktive barrierer, men det er også mulig å basere seg kun å atomklokke og slik fjerne svikt i GNSS som en risikofaktor.

Ban NOR har også tenkt i riktig retning, men er etter min vurdering ikke mål. Mangelen ser ut til å være at det kun er tenkt på lokale forstyrrelse av GPS-signaler og ikke på feil i GPS på systemnivå. Bane NOR har flere GPS-mottakere med stor geografisk spredning som er en bra ting for å sikre tilgang til satellittsignalene. Dette vil fungere som barriere mot lokale tilsiktede og utilsiktede forstyrrelser. Skulle det derimot f.eks. skje en romværhendelse som rammer store deler av landet eller svikt i GPS på systemnivå, vil det kunne påvirke signalene som mottas på alle mottakerne. Da holder ikke barrieren. Etter det vi nå har sett vil det gi forstyrrelser i sikkerhetskritisk funksjoner hos Bane NOR. Tiltak mot dette vil kunne være multi-GNSS eller atomklokker som hos Avinor. Vegvesenet og Kystverket har ikke gitt noe informasjon som

tyder på at kartlegging av bruk av nøyaktig tid og vurderinger av alternativ kilde til nøyaktig tid er et tema som får oppmerksomhet.

Tiltakene som Avinor og Bane NOR har innført er i tråd med hensikten i den nasjonale PNT-strategien SD har publisert. Hensikten er at departementer, etater og fagmiljøer som bruker satellittbasert PNT skal analysere sin egen bruk og avhengighet og selv identifisere og gjennomføre nødvendige tiltak.

Det som etatene/virksomheten gir av informasjon gir inntrykk av at det er en bevissthet om hvordan digitalisering kan påvirke risikobildet, men at det er forskjeller i hvordan tid isolert sett er håndtert. Systematikken som velges er litt forskjellig og er iht. sektorregelverk. Bortsett fra hos Avinor ser det ikke ut til at det er gjort grundige vurderinger av om alternative kilder til nøyaktig tid trengs, og hva som i så fall kunne vært slike kilder. Det bekrefter inntrykket av nøyaktig tid som den usynlige ressursen som mye avhenger av, men som ikke får oppmerksomhet fordi den ikke synes. Slike avhengigheter, som kan være ukjente for de som faktisk har gjort seg avhengig, er nettopp det Pescaroli hevder bereder grunnen for kaskadeeffekter.

Det ser ut til at tilgangen til, og anvendelsene av, ressursen nøyaktig tid med fordel kan knyttes tettere til IKT-sikkerhetsstyringen i organisasjonene enn det som fremkommer i datagrunnlaget. Samfunnssikkerhetsinstruksen sier at IKT-sikkerhet er en integrert del av arbeidet med samfunnssikkerhet. Samtidig sier SD i sin strategi for samfunnssikkerhet at informasjons- og IKT-sikkerhet skal prioriteres og at samfunnssikkerhetsarbeidet skal integreres i den ordinære virksomhetsstyringen. Dette viser at myndighetene knytter sammen IKT-sikkerhet, samfunns-sikkerhet og etatenes virksomhets-/sikkerhetsstyring.

Utviklingen går raskt videre og stadig flere områder tar i bruk GNSS. F.eks. er teknologien i de nye 5G-nettene svært avhengig av nøyaktig tid og utbyggerne vil i de aller fleste tilfellene basere seg på GNSS-tid. Nye løsninger innen automatisering og autonomi vil baseres på 5G. Utviklingen har gitt en stadig tettere knytning mellom satellittnavigasjon og IKT der tid fra GNSS holder IKT-systemene i gang. Det gir en knyting mellom GNSS og IKT-sikkerhet. Intervjuene viser at etatene/virksomhetene tenker litt ulikt om dette. SD ønsker i utgangspunktet ikke å mene noe om det, men synes likevel ikke det er unaturlig hvis underliggende etater betrakter GNSS som IKT. Kystverket behandler tid fra GNSS i risikovurderinger, men har ikke

en etablert praksis på å betrakte GNSS som IKT. Avinor derimot, gjør det. Avinor ser på GNSS som et IT-produkt, en server, der etablerte IKT-sikkerhetsprinsipper i virksomheten legges til grunn. Vegvesenet benytter en tidsserver i utlandet som veksler mellom atomklokke og GNSS-tid, men har ikke opplyst om bruk av IKT-sikkerhetsprinsipper i så måte.

Nasjonal tidsdistribusjon

Et digitalisert samfunn trenger ressursen nøyaktig tid. Avinor har etablert sin egen alternative kilde til nøyaktig tid etter en risikovurdering av egen GNSS-avhengighet. Det kan stilles spørsmål om også andre bør gjøre det. Et slikt grep forutsetter en bevissthet rundt egen tidsavhengighet og hvordan den virksomheten man har ansvar for kan klare seg hvis denne ressursen forsvinner. Som tidligere omtalt så har Sverige etablert et system for nasjonal tidsdistribusjon i fibernett uavhengig av GNSS og UK planlegger det samme. Amerikanske myndigheter tilbyr også flere løsninger for tidsdistribusjon.

I Norge har vi foreløpig ikke en slik tjeneste. Noen husker kanskje NRKs tidssignal og Televerkets «frøken Ur», men det er for lengst historie. Nå er det mye strengere og annerledes krav til presis tid og i et samfunn som det norske, med så omfattende digitalisering, er det et stort behov. Behovet dekkes gjennom GNSS. Det er ikke unaturlig å tenke seg at en nasjonal tjeneste også etableres i Norge. Selv om PNT-strategien legger opp til at dette er de enkelte brukergruppers ansvar så vil det være dårlig ressursutnyttelse om alle skal gjøre det Avinor nå har gjort. Det er ikke utenkelig at Avinor kan videreutvikle sin løsning til å bli den nasjonale tjenesten. Min oppfatning er at det vil være en naturlig del av SDs hovedansvar for nøyaktig tid å gjøre nødvendige utredninger av dette. På bakgrunn av det er et av mine forslag til videre arbeid at det gjøres en analyse av relevante alternative kilder til tid for samfunnet generelt og samferdselssektoren spesielt.

9.4 Samfunnssikkerhet, prinsipper og hovedansvar

Gjennomgangen av dokumenter, fra Sårbarhetsutvalget til en nyeste stortingsmeldingen om samfunnssikkerhet, viser en omfattende utvikling og endring fra kald krig med en ytre fiende til dagens digitaliserte samfunn. Det viser også en omfattende utvikling i samfunnssikkerhet som fagområde. Fra å være noe det gamle totalforsvaret holdt på med har det blitt et akademisk fagfelt med ulike teorier og vinklinger, og der kommuner, regioner og stat har sine fagmiljø på samfunnssikkerhet og beredskap. Totalforsvarstanken har etter hvert kommer tilbake, men i en

annen form enn før. Nå skal det være gjensidig støtte mellom militære og sivile ressurser og det handler ikke om et militær angrep på Norge, men om følgene av naturkatastrofer, ekstremvær og svikt i en kompleks samfunnsinfrastruktur. Et stadig mer digitalisert samfunn der kritiske infrastrukturer henger sammen og gir fare for kaskadefeil, gjør bildet enda mer komplekst. I jakten på reduserte kostnader ser det ut til at Forsvaret i stadig større grad baserer seg på sivile ressurser i stedet for å ha egne ressurser der det ansees som økonomisk fordelaktig. Dette skjer bl.a. innenfor transporttjenester. Det har skapt debatt om at sivile personer og ressurser gjøres til legitime militære mål.

I alle dokumentene brukes begrepet myndighetene. Det fremstår i denne sammenhengen som et noe upresist begrep. Myndighetene har mange «hoder» og det fremgår i dokumentene behov for å avklare ansvarsforhold mellom myndighetsaktører og å etablere struktur relatert til ivaretakelse av samfunnssikkerhet. Sårbarhetsutvalget ønsket et nytt departement for dette, men det ble løst ved å gi JD et overordnet ansvar som lederdepartement for samfunnssikkerhet med etaten DSB som utøvende ledd og Koordineringsenheten som verktøy når noe skjer.

Det fremstår som relativt tydelig at JD har møtt utfordringer når departementets overordnede ansvar skal konkretiseres og delansvar fordeles til andre fagdepartement. Utfordringen ser ut til å bunne i sektoransvaret. Samfunnssikkerhetsarbeid krever samarbeid på tvers av sektorgrensene og det utfordrer sektoransvaret i statsforvaltningen. For å fordele ansvar, etablere struktur og utpeke hovedansvarlige departement, har JD laget samfunnssikkerhetsinstruksen på 10 sider og sett det nødvendig med en veileder til instruksen på 50 sider. Utfordringene med å jobbe på tvers synliggjøres også ved at det har vært behov for å formalisere et samordningsprinsipp som et nytt fjerde prinsipp for arbeidet med samfunnssikkerhet.

Sentralt i dette er departementenes hovedansvar og hvordan det skal ivaretas. Alle departementer som har et hovedansvar skal ivareta dette på tvers av sektorgrensene. SD er gitt et hovedansvar for PNT og med det et hovedansvar for nøyaktig tid.

Min oppfatning er at SDs beskrivelse av hva hovedansvar betyr gir inntrykk av å være noe avgrenset sammenliknet med syvpunktsbeskrivelsen av hovedansvar i samfunnssikkerhets-instruksen. Etter dette skal SD ha oppdaterte ROS-analyser for nøyaktig tid, ha oversikt over sårbarheter, avklare ansvarsdeling på tvers, gjennomføre øvelser og følge opp læringspunkter,

foreslå beredskapsplaner og -tiltak og jobbe med kompetanseheving for berørte aktører. Jeg forstår av det SD sier at sektoransvaret står sterkt. Hovedansvar skal ikke redusere andre departementers sektoransvar, men det SD sier gir inntrykk av at sektoransvaret står så sterkt at det blir utfordrende å utøve hovedansvaret iht. instruksen. Det er mitt inntrykk at det er høy terskel for å ta initiativ som kan bli tolket som å «blande seg borti» det andre sektorer holder på med. Det er kanskje derfor man har endt opp med det litt ubestemmelige «koordineringsansvaret».

Etterlevelse av ansvarsprinsippet er også en faktor i dette. Prinsippet sier i korthet at den som har ansvaret i en normalsituasjon også har ansvaret ved ekstraordinære hendelser. Av det ser vi at ansvarsprinsippet og sektoransvaret henger tett sammen. Relatert til nøyaktig tid gir dette etter, min vurdering, en uklar situasjon. Norges bidrag til UTC kommer fra JV som ligger under NFD. Det gir næringsministeren et beredskapsansvar for tid etter ansvarsprinsippet. Samtidig har SD hovedansvar for nøyaktig tid og et ansvar for å foreslå beredskapsplaner og -tiltak på tvers av sektorgrensene etter samfunnssikkerhetsinstruksen. I tillegg til dette sier den nye stortingsmeldingen for samfunnssikkerhet, Meld. St. 5 (2020-2021), at den som sitter med et ansvar etter ansvarsprinsippet skal gjøre prioriteringer basert på en etablert aksept av risiko knyttet sil samfunnssikkerhet.

Jeg synes dette gir et noe uklart myndighetsansvar for nøyaktig tid og på bakgrunn av det er et av mine forslag til videre arbeid å se på hovedansvarets betydning og «kår» i lys av sektoransvaret og ny utvidet betydning av ansvarsprinsippet.

10. BESVARELSE AV FORSKNINGSSPØRSMÅL

I dette kapittelet besvares forskningsspørsmålene basert på det som har fremkommet gjennom teori, dokumentstudie, intervjuer og diskusjon.

10.1 Spørsmål 1

«Hva menes med en GNSS-avhengig digitalisert transportsektor?»

Digitaliseringen og elektrifiseringen av samferdselssektoren skjer på mange plan. Det er systemer i kjøretøy, tog, fly og fartøy, det er i kommunikasjon mellom disse og infrastruktur, det er i styring av infrastruktur, det er i systemer for overvåking og kontroll av trafikken, det er i hvordan reisende benytter kollektivtransport og det er i hvordan informasjon utveksles på tvers av systemer for å oppnå effektivisering, nye tjenester og positive miljøeffekter. Samferdsel henger nøye sammen med hvor folk bor og hvordan samfunnet er innrettet. Digitalisering av sektoren gir nye muligheter som påvirker samfunnet. Dette gir utslag som mikromobilitet, delte ressurser og smarte samfunn. Utviklingen preges av automatisering, samvirke, elektrifisering og deling.

GNSS er en muliggjørende teknologi for alt dette som verktøy for å posisjonsbestemme med høy nøyaktighet og som global, gratis kilde til nøyaktig tid. Dette gjør en digitalisert samferdselssektor GNSS-avhengig der avhengigheten også omfatter kritisk infrastruktur og systemer med sikkerhetskritiske funksjoner. Med denne avhengigheten følger sårbarheter som har sitt utspring i hvordan GNSS er sårbart. Det kan være kilder som er naturlige eller menneskeskapte, utilsiktede eller tilsiktede.

10.2 Spørsmål 2

«Hva er transportsektorens rolle inn mot samfunnssikkerhet og hvordan påvirker GNSS-avhengigheten dette?»

Samfunnssikkerhet kan defineres som en evne samfunnet har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov. I grunnleggende

behov legges ofte befolkningens trygghetsfølelse. Samfunnsfunksjonene realiseres vha. infrastruktur som kan være kritisk hvis det ikke finnes fungerende alternativer til den. Transport er en slik kritisk funksjon bestående av kapabilitetene transportevne, sikre transportsystemer og sikker transport.

Samferdselssektorens rolle inn mot samfunnssikkerhet blir etter dette å sørge for at disse kapabiliteten er på plass innenfor alle transportformer. Det vil si at nødvendig infrastruktur skal fungere slik at samfunnets behov for transport ivaretas, at et akseptabelt sikkerhetsnivå opprettholdes med nødvendig infrastruktur for å overvåke og styre trafikk, og at det opprettholdes et akseptabelt sikkerhetsnivå ved transport med potensial for store ulykker. Dette må så holdes opp mot mål og prioriteringer som SD gir. Gjeldende overordnede mål er å unngå store uønskede hendelser som medfører skade, minske følgene av slike hendelser hvis de skjer og sikre pålitelighet og framkommelighet i transport- og kommunikasjonsnett både i normal-situasjon og under påkjenninger. Samfunnsfunksjonen transport vil ha avgjørende betydning for andre kritiske funksjoner som f.eks. forsyningssikkerhet, lov og orden, og helse og omsorg. Funksjonen vil også ha stor betydning som bidragsyter til totalforsvaret.

GNSS-avhengigheten påvirker dette ved at alle de tre kapabilitetene under den kritiske samfunnsfunksjonen transport påvirkes av digitaliseringen og kan i så måte bli avhengig av nøyaktig tid. Transportevne påvirkes ved at kjøretøy, fartøy og infrastruktur digitaliseres. Sikre transportsystemer påvirkes ved at verktøy og hjelpemidler ved trafikksentralene digitaliseres og teknologien knyttet til trafikkovervåking blir avhengig av nøyaktig tid. Sikker transport påvirkes ved at sikkerhetskritiske funksjoner digitaliseres og blir GNSS-avhengig. Digitale ekom-nett med krav til synkronisering er nødvendig for at alt skal fungere. GNSS påvirker derfor rollen samferdselssektoren har ved at GNSS som kilde til tid kan bli en forutsetning for å klare å fylle denne rollen. Uten tilgang på tid vil mange av disse systemene kunne feile eller komme i utakt med hverandre. Det vil gi driftsutfordringer og fare for stans i viktige tjenester.

10.3 Spørsmål 3

«Hvordan håndterer transportetatene i sine risiko-/sikkerhetsstyringssystemer at de er avhengig av GNSS som ligger utenfor deres kontroll?»

Informantene er gitt ulik informasjon med ulik detaljeringsgrad om dette så det er ikke mulig å gi en god helhetlig beskrivelse. Her kommer også sektorregelverket inn bildet som påvirker hva som gjøres innenfor de ulike transportformene.
Alle informanter gir uttrykk for at digitaliseringen setter preg på sikkerhetsstyringen og systematikken som benyttes. Det jobbes med cybersikkerhet og NIS-direktivet, ROS-analyser og barrierer. Det er høy bevissthet på at digitalisering gjør noe med risikobildet. Risikoen blir ikke nødvendigvis høyere eller lavere, men den blir annerledes. Det er til dels store forskjeller på hvor stor vekt som konkret legges på nøyaktig tid hos de ulike etatene/virksomhetene.

Vegvesenet sier at digitaliseringen påvirker sikkerhetsstyringen. Det jobbes med sikringsrisiko, IKT-sikkerhet og løsninger for redundans og back-up. FoU-miljøet deres har prosjekter rettet mot selvkjøring, ITS og forstyrrelser i GNSS-signaler. For Vegvesenet er det viktig å sikre GNSS-signaler sammen med god mobildekning for å kunne gjennomføre anleggsprosjekter og oppmåling.

Kystverket legger til grunn både naturvitenskapelig og samfunnsvitenskapelig kunnskapssyn i sin sikkerhetsstyring. Kystverket sier at digitaliseringen har som konsekvens økt sikkerhet, men at det er viktig å være klar over hvordan det digitale risikobildet blir. Det er nødvendig med økt fokus på IKT-sikkerhet og at de digitale systemene fungerer. Ved sikring av havneanlegg brukes sikringsrisikoanalyse.

Bane NOR har satt digital sikkerhet høyt på dagsorden og det er fokus på at risikobildet stadig endres. Dette krever aktivt forhold til barrierer og robusthet. Bane NOR har valgt å vinkle arbeidet inn mot konsekvensene av mulige feil og håndterer det gjennom et beredskapssystem med taktisk, operasjonelt og strategisk nivå. Virksomheten bruker NSMs retningslinjer for IKT-sikkerhet og har tatt flere standarder inn i styringssystemet. Det brukes både kvantitative og kvalitative teknikker i sikkerhetsarbeidet og innenfor deler av det brukes ALARP-prinsippet. Relatert til sikring av objekter og sikringsrisiko benyttes trefaktormodellen.
Bane NOR har bygget inn en teknisk barriere i form av at GNSS-signaler tas inn i systemet flere steder i Norge.

Avinors sikkerhetsstyring baseres på en rekke nasjonale og internasjonale regelverk. Det er ulike hensyn og krav for ulike systemer og om det er snakk om safety eller security. Avinor har utarbeidet tall for risikoaksept på ulike områder og bruker det i stedet for ALARP-prinsippet.

Avinor har analysert hvordan virksomheten er avhengig av nøyaktig tid. Dette har resultert i både operative og tekniske tiltak. Avinor opplyser at pga. disse tiltakene er ikke lenger virksomheten avhengig av tid fra GNSS selv om den fortsatt er svært avhengig av nøyaktig tid. Alternativ teknologi er innført.

10.4 Spørsmål 4

«Hva er SDs rolle for å sikre bruken av nøyaktig tid i en digitalisert transportsektor?»

SD beskriver sin styrende rolle som overordnet og vil ikke gi underliggende etater/virksomheter konkrete føringer med mindre det er spesielle forhold som krever det i en bestemt sak. Det gjelder også nøyaktig tid og risikostyring relatert til nøyaktig tid selv om SD er godt kjent med stor avhengighet av GNSS i egen sektor og at tilgang til nøyaktig tid er kritisk for mange anvendelsesområder.

Retningslinjer og styringssignaler fra SD i egen sektor gis primært gjennom de mekanismene som er knyttet til etatsstyring og eierstyring. I tillegg brukes «mykere» verktøy som f.eks. strategidokumenter. Innenfor disse rammene, sammen med funksjonsbaserte krav i sektorregelverket for den enkelte del-sektor, forventer SD at etatene/virksomhetene selv tar ansvar for sin egen risiko-/sikkerhetsstyring.

Sikkerhetsstyringen forventes å håndtere forhold knyttet til bruk av nøyaktig tid og det som måtte følge med av sårbarheter relatert til dette. Det ligger til virksomhetene å selv identifisere sårbarheter og gjøre det de kan for å redusere dem uten at SD skal trenge å stille krav om det.

I tillegg til sitt sektoransvar for PNT innen samferdsel, har SD et hovedansvar for PNT iht. samfunnssikkerhetsinstruksen. Det vil si et tverrsektorielt ansvar for nøyaktig tid relatert til samfunnssikkerhet. Til tross for at samfunnssikkerhetsinstruksen lister opp en rekke aktiviteter tillagt hovedansvaret hevder SD at dette skal forstås som et koordineringsansvar som handler om informasjonsdeling og der tiltak på tvers kun blir gjeldende hvis det er fordelaktig at samme utfordring i flere sektorer får en felles løsning.

Hver sektor har ansvar for egen bruk av PNT og dermed egne sårbarheter og avhengigheter. Samferdselsministerens ansvar for tid relatert til samfunnssikkerhet påvirker derfor ikke næringsministerens ansvar som «tidsminister». Et departements hovedansvar reduserer ikke et

annets departements sektoransvar. I diskusjonskapittelet argumenterer jeg for hvorfor jeg synes teori og praksis ikke går godt i hop på dette området.

10. KONKLUSJON

Samfunnssikkerhet som begrep og fagområde har gjennomgått en omfattende utvikling de siste 20 årene. Det handler om å gjøre befolkningen trygg gjennom å sikre leveranse av kritiske funksjoner ved hjelp av kritisk infrastruktur. Mye av dette kan relateres til en fungerende samferdselssektor.

Den pågående digitaliseringen er omfattende i samferdselssektoren som i samfunnet ellers. Digitalisering krever tilgang til nøyaktig tid som i svært mange tilfeller hentes fra GNSS. Alle de infrastruktureiende etatene/virksomhetene under SD opplyser at de har en viktig funksjon for å fylle samferdselssektorens rolle inn mot samfunnssikkerhet og totalforsvar. Alle viktige samfunnsfunksjoner er på en eller annen måte avhengig av transport. Det resulterer i en GNSS-avhengig samfunnssikkerhet der GNSS-avhengigheten er en kilde til sårbarhet. Dette håndteres ulikt i de ulike etatenes sikkerhetsstyring med ulik grad av bevissthet på tid og hvor tiden kommer fra.

Det skapes et inntrykk av nøyaktig tid som en usynlig ressurs mange er avhengig av, men som ikke får tilstrekkelig fokus fordi det ikke synes. GNSS som en kilde til nøyaktig tid fremstår som et eksempel på hvordan vellykkede teknologiske løsninger får stor anvendelse og derfor kan skape ubevisste avhengigheter og sårbarheter. Sammenhengen mellom IKT-sikkerhet, samfunnssikkerhet og etatenes sikkerhetsstyring bør bli tydeligere hos etatene/virksomhetene.

SD har en overordnet, styrende rolle overfor sine etater/virksomheter og ønsker ikke å detaljstyre hvordan risikostyring relatert til samfunnssikkerhet skal skje. Det må etatene selv finne ut av innenfor sitt sektorregelverk. SD har i tillegg et hovedansvar for nøyaktig tid utover egen sektor. Jeg har argumentert for hvorfor jeg mener SDs praksis på dette området er til dels i utakt med samfunnssikkerhetsinstruksens ordlyd og at det er uklarheter rundt myndighetsansvaret for nøyaktig tid.

Oppgaven gir tre forslag til videre arbeid relater til digitale verdikjeder, nasjonal tjeneste for distribusjon av tid og betydning av hovedansvar etter samfunnssikkerhetsinstruksen.

11. FORSLAG TIL VIDERE ARBEID

I diskusjonskapitlet har jeg omtalt tre forslag til videre arbeid. Disse er:

1. Gjøre en studie av hvordan interne organisatoriske forhold i en virksomhet kan skape digital verdikjede-problematikk internt i egen organisasjon.

2. Gjøre en studie av behovet for en nasjonal tjeneste for distribusjon av nøyaktig tid alternative kilder til tid og se på hvordan en slik tjenesten eventuelt kan realiseres.

3. Gjøre en studie av hovedansvarets betydning og «kår» i lys av sektoransvaret og innføring av prioritering og risikoaksept i forståelse av ansvarsprinsippet.

Vedlegg 1 – Intervjuguide

INTERVJUGUIDE FOR MUNTLIG FAKTAINNSMALING TIL MASTEROPPGAVE VED INSTITUTT FOR SOSIOLOGI OG STATSVITENSKAP VED NTNU

Karl Bjarne Kapaasen

1. Bakgrunn

Denne intervjuguiden skal brukes i forbindelse med faktainnsamling relatert til masteroppgave i organisasjon og ledelse ved NTNU Videre. Innenfor temaet organisasjon og ledelse er det valgt spesialisering sikkerhet, pålitelighet og vedlikehold. Oppgaven gjennomføres hos institutt for sosiologi og samfunnsvitenskap ved NTNU.

2. Hensikt

Intervjuenes hensikt er å frembringe fakta relatert til oppgavens problemstilling fra sentrale samferdselsetater. Intervjuobjektene forventes å bidra med faktakunnskap om etatspraksis forankret i strategier, planer, instrukser, kvalitets-/sikkerhetsstyringssystem, m.m. Faktainnsamlingen vil fungere som et supplement til oppgavens dokumentstudium, både ved å si noe om etatenes strategi innenfor feltet, men også som kilde til mulige videre dokumentanalyser.

3. Gjennomføring

Faktainnsamlingen gjennomføres muntlig, dvs. som intervju med fagperson som etaten selv velger ut. Under forutsetning om intervjuobjektets aksept, vil det bli tatt lydopptak under samtalen.

Det er ønskelig å gjennomføre intervju hos

- Samferdselsdepartementet
- Statens Vegvesen
- Kystverket
- Bane NOR
- Avinor

Intervjuguiden inneholder et sett med spørsmål for hver dept/etat. Den enkelte dept/etat vil kun få tilsendt «sine» spørsmål.

Se infoskriv for mer om prosjektet og for hvordan intervjudataene skal behandles.

Spørsmål til Samferdselsdepartementet

Tema	Spørsmål
Samferdsel og samfunnssikkerhet	1. Hvilken rolle har samferdselssektoren inn mot samfunnssikkerhet 2. På hvilken måte ivaretas denne rollen fra SDs side? 3. Hva legger SD i begrepet transportberedskap? 4. Samfunnssikkerhetsinstruksen gir SD hovedansvar for PNT. Hva betyr det at SD har ansvar for nøyaktig tid?
Samferdselssektoren og GNSS	1. SD er ansvarlig for sivil radionavigasjonspolitikk. Hva vil det si? 2. Har SD noe ansvar for anvendelser av GNSS utenfor samferdselssektoren 3. Hva betrakter SD som de viktigste risiko-/ sårbarhetsfaktorene relatert til at samferdselssektoren har gjort seg avhengig av GNSS? 4. Hvordan tar SD styring over disse utfordringene? 5. Hvilke forventninger har SD til hvordan samferdselssektoren jobber med problemstillingen «mulig bortfall av GNSS»
Krav til sikkerhetsstyring	1. Har SD gitt underliggende etater føringer på hvordan håndtere risiko/sikkerhet relatert til samfunnssikkerhet? 2. Har SD gitt underliggende etater føringer på hvordan håndtere risiko/sikkerhet relatert til nøyaktig tid? 3. Hvis «ja» på spm 1 og/eller 2: Hvilke modeller, standarder, eller kunnskapssyn legges til grunn?
GNSS og IKT-sikkerhet	1. Der GNSS brukes som kilde til nøyaktig tid, anser SD dette som IKT? 2. Forventes det i så fall fra SD at prinsipper for IKT-sikkerhet legges til grunn i slike tilfeller?

Spørsmål til Statens Vegvesen (SVV)

Tema	Spørsmål
Vegtransport og samfunnssikkerhet	1. Hvilken rolle spiller vegtransport for samfunns-sikkerhet? 2. Hvordan jobber SVV med å ivareta denne rollen? 3. Er det forhold ved digitalisering av vegtransporten som påvirker vegtransportens rolle ifm. samfunnssikkerhet? 4. Lager SVV regler/forskrifter relatert til sikker-hetsstyring og samfunnssikkerhet som andre aktører i vegsektoren må følge?
Digitalisering, GNSS og sikkerhetsstyring	1. Hvordan påvirker digitaliseringen av samferdselssektoren måten SVV utøver sikkerhetsstyring? 2. Har SVV laget en oversikt over hvordan nøyaktig tid fra GNSS anvendes innen vegsektoren? 3. Digitale systemer i vegtransport benytter gjerne tid fra GNSS som kilde til synkronisering. Hvordan håndteres risiko/sårbarhet relatert til GNSS-avhengighet og drift av veitrafikksentraler? 4. Har SVV gjort en risikovurdering av scenario «bortfall av GNSS»? 5. ITS er avhengig av ekom-nett som igjen er avhengig av nøyaktig tid fra GNSS. Stiller SVV krav til robusthet/resiliens overfor netteier og tjenestetilbydere? 6. Hvordan jobber SVV for å ha kontroll over risikofaktorer langs digitale verdikjeder? 7. Legges prinsipper for IKT-sikkerhet til grunn der hvor GNSS er kilde til nøyaktig tid? 8. Hvilke modeller/standarder/kunnskapssyn legger SVV til grunn i sin sikkerhetsstyring?
Vegtransport og GNSS	1. Har SVV gjort noen vurderinger av konsekvenser av bortfall/redusert tilgang til GNSS relatert til å innføre GNSS-basert veiprising? 2. Har SVV gjort noen vurderinger av konsekvenser av bortfall/redusert tilgang til GNSS relatert til vegbyggingsprosjekter? 3. GNSS er en forutsetning for selvkjøring. Har SVV vurdering konsekvenser av norsk topografi og signaldekningsproblematikk?

Spørsmål til Kystverket (KYV)

Tema	Spørsmål
Sjøtransport og samfunnssikkerhet	1. Hvilken rolle spiller sjøtransport for samfunns-sikkerheten? 2. Hvordan jobber KYV med å ivareta denne rollen? 3. Er det forhold ved digitalisering av sjøtransporten som påvirker sjøtransportens rolle ifm. samfunnssikkerhet? 4. Hvis «ja» på spm. 3, hvordan sørger KYV for at samfunnssikkerheten ivaretas? 5. Lager KYV regler/forskrifter relatert til sikker-hetsstyring og samfunnssikkerhet som andre aktører i sektoren må følge?
Digitalisering, GNSS og sikkerhetsstyring	1. Hvordan påvirker elektrifiseringen/digitali-seringen av sjøfarten måten KYV utøver sikkerhetsstyring? 2. Har KYV laget en oversikt over hvordan nøyaktig tid fra GNSS anvendes innen sjøtransport? 3. AIS, som er en barriere mot skipskollisjoner, benytter nøyaktig tid fra GNSS. Hvordan håndteres risiko/sårbarhet fra GNSS-avhengig-het i sikkerhetskritiske systemer? 4. Har KYV gjort en risikovurdering av scenario «bortfall av GNSS»? 5. Hvordan jobber KYV for å ha kontroll over risikofaktorer langs digitale verdikjeder? 6. Legges prinsipper for IKT-sikkerhet til grunn der hvor GNSS er kilde til nøyaktig tid? 7. Hvilke modeller/standarder/kunnskapssyn legger KYV til grunn i sin sikkerhetsstyring?
Sjøtransport og GNSS	1. Det er et mulig scenario at KYVs kjede av IALA-DGPS-stasjoner fases ut til fordel for EUs EGNOS-system. Har KYV vurdert om det er noe forskjell i risikonivået mellom disse to løsningene relatert til samfunnssikkerhet?

Spørsmål til Bane NOR (BN)

Tema	Spørsmål
Jernbanetransport og samfunnssikkerhet	1. Hvilken rolle spiller jernbanetransporten for samfunnssikkerheten? 2. Hvordan jobber BN med å ivareta denne rollen? 3. Er det forhold ved digitalisering av jernbanetransporten som påvirker jernbanetransportens rolle ifm. samfunnssikkerhet? 4. Hvis «ja» på spm. 3, hvordan sørger BN for at samfunnssikkerheten ivaretas? 5. Lager BN regler/forskrifter relatert til sikkerhetsstyring og samfunnssikkerhet som andre aktører i sektoren må følge?
Digitalisering, GNSS og sikkerhetsstyring	1. Hvordan påvirker digitaliseringen av jernbanetransporten måten BN utøver sikkerhetsstyring? 2. Har BN laget en oversikt over hvordan nøyaktig tid fra GNSS anvendes innen jernbanetransport? 3. GSM-R benytter tid fra GNSS som kilde til synkronisering. Hvordan håndteres risiko/sårbarhet fra GNSS-avhengighet i sikkerhetskritiske systemer? 4. Har BN gjort en risikovurdering av scenario «bortfall av GNSS»? 5. Hvordan jobber BN for å ha kontroll over risikofaktorer langs digitale verdikjeder? 6. Legges prinsipper for IKT-sikkerhet til grunn der hvor GNSS er kilde til nøyaktig tid? 7. Hvilke modeller/standarder/kunnskapssyn legger BN til grunn i sin sikkerhetsstyring?
Jernbanetransport og GNSS	2. Forventes det en utvikling der GNSS blir eneste verktøy for posisjonsbestemmelse av rullende materiell langs sporet?

Spørsmål til Avinor

Tema	Spørsmål
Lufttransport og samfunnssikkerhet	1. Hvilken rolle spiller lufttransporten for samfunnssikkerheten? 2. Hvordan jobber Avinor med å ivareta denne rollen? 3. Er det forhold ved digitalisering av lufttransporten som påvirker lufttransportens rolle ifm. samfunnssikkerhet? 4. Hvis «ja» på spm. 3, hvordan sørger Avinor for at samfunnssikkerheten ivaretas? 5. Lager Avinor regler/forskrifter relatert til sikkerhetsstyring og samfunnssikkerhet som andre aktører i sektoren må følge?
Digitalisering, GNSS og sikkerhetsstyring	1. Hvordan påvirker digitaliseringen av jernbanetransporten måten Avinor utøver sikkerhetsstyring? 2. Har Avinor laget en oversikt over hvordan nøyaktig tid fra GNSS anvendes innen lufttransportsystemet? 3. Digitale systemer innen flynavigasjons-/flysikringstjenesten benytter gjerne tid fra GNSS som kilde til synkronisering. Hvordan håndteres risiko/sårbarhet relatert til GNSS-avhengighet? 4. Har Avinor gjort en risikovurdering av scenario «bortfall av GNSS»? 5. ADS-B og WAM er avhengig av ekom-nett som igjen er avhengig av tid fra GNSS. Stiller Avinor krav til robusthet/resiliens over netteiere og tjenestetilbydere? 6. Hvordan jobber Avinor for å ha kontroll over risikofaktorer langs digitale verdikjeder? 7. Legges prinsipper for IKT-sikkerhet til grunn der hvor GNSS er kilde til nøyaktig tid? 8. Hvilke modeller/standarder/kunnskapssyn legger Avinor til grunn i sin sikkerhetsstyring?
Lufttransport og GNSS	*3. Har Avinor gjort noen vurderinger av konsekvenser av bortfall/redusert tilgang til GNSS relatert til satsingen på fjernstyrte tårn?* 4. Har Avinor gjort noen vurderinger av konsekvenser av bortfall/redusert tilgang til GNSS relatert til utfasing av bakkebaserte radionavigasjonssystemer?

	5. Har Avinor gjort noen vurderinger av konsekvenser av bortfall/redusert tilgang til GNSS relatert til droner/U-space?

Vedlegg 2 – Akronymer

ADS-B	Automatic Dependent Surveillanve – Broadcast
AIS	Automatic Identification System
AKS	Analyse av krisescenarioer
ALARP	As Low As Reasonably Practical
BAS	Beskyttelse Av Samfunnet (serie av forskningsrapporter fra FFI)
C-ITS	Connected ITS, samvirkende ITS
CBTC	Communications-based Train Control
DSB	Direktoratet for samfunnssikkerhet og beredskap
EASA	European Aviation Safety Agency
ECDIS	Electronic Chart Display Information System
EGNSS	European GNSS, fellesbetegnelse for Galileo og EGNOS
EGNOS	European Geostationary Navigation Overlay System
eLoran	enhanced Long Range Navigation (oppgradert versjon av Loran-C)
ERTMS	European Rail Traffic Management System
ESA	European Space Agency
ETCS	European Train Control System
EØS	Europeisk Økonomisk Samarbeidsområde
FFI	Forsvarets forskningsinstitutt
GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sist'ema (russisk GNSS)
GMT	Greenwich Mean Time
GNF	Grunnleggende Nasjonal Funksjon
GNSS	Global Navigation Satellite Systems
GSM-R	Global System for Mobile Communication - Railway
GPS	Global Positioning System
HMS	Helse, Miljø og Sikkerhet
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commision
IKT	Informasjons- og kommunikasjonssystemer
IMO	International Maritime Organization
IRPA	Individual Risk Per Annum
ITS	Intelligente Trafikksystemer

JD	Justisdepartementet
JV	Justervesenet
JRC	Joint Research Centre (EUs forskningssenter i Roma)
KIKS	Kritisk infrastruktur og kritiske samfunnsfunksjoner
KMD	Kommunal og moderniseringsdepartementet
KYV	Kystverket
MaaS	Mobility-as-a-Service
MSB	Myndigheten för Samhällsskydd och Beredskap (Sveriges DSB)
NATO	North Atlantic Treaty Organization
NOU	Norsk offentlig utredning
NSM	Nasjonal sikkerhetsmyndighet
NTP	Nasjonal transportplan
PNT	Posisjonsbestemmelse, Navigasjon og Tidsbestemmelse
POD	Politidirektoratet
PRS	Public Regulated Service
PST	Politiets sikkerhetstjeneste
ROS	Risiko- og sårbarhetsanalyse
RAMS	Reliability, Availability, Maintainability and Safety
RE	Resilience Engineering
SAR	Search and Rescue
SAMRISK	Samfunnssikkerhet og risikoforskning
SD	Samferdselsdepartementet
SNL	Store norske leksikon
SVV	Statens Vegvesen
TAI	International Atomic Time
TØI	Transportøkonomisk institutt
UAM	Urban Air Mobility
UCL	University College London
USNO	United States Naval Observatory
UTC	Universal Time Coordinated
UTC(JV)	Norsk bidrag til UTC fra Justervesenets tidslaboratorium
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
WAM	Wide Area Multilateration

Vedlegg 3 – Referanser

Almklov, P. G., Antonsen, S., Bye, R., & Øren, A. (2018). Organizational culture and societal safety: Collaborating across boundaries. *Safety Science*, *110*, 89–99. https://doi.org/10.1016/j.ssci.2017.12.029

Almklov, P. G., Antonsen, S., Størkersen, K. V., & Roe, E. (2018). Safer societies. *Safety Science*, *110*, 1–6. https://doi.org/10.1016/j.ssci.2018.03.018

Antonsen, S., Heldal, F., & Kvalheim, S. A. (2017). *Sikkerhet og ledelse*. Gyldendal akademisk.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608. JSTOR. https://doi.org/10.2307/2094589

Dalen, M. (2013). *Intervju som forskningsmetode: En kvalitativ tilnærming* (2. utg). Universitetsforl.

DSB. (2012). *Samordningsresolusjonen*. https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/pdf-er/kongelig_resolusjon_15_06_2012.pdf

DSB. (2020). *Risikostyring i digitale verdikjeder* (Nr. 978-82-7768-496–3). https://www.dsb.no/rapporter-og-evalueringer/risikostyring-i-digitale-verdikjeder/

EASA. (2018). *(EU) 2018/1139*. EASA. https://www.easa.europa.eu/document-library/regulations/regulation-eu-20181139

Ebenhag, S.-C., Hedekvist, P. O., Jarlemark, P., & Sundblad, R. (2019). Redundant Distributed Timescale Traceable to UTC(SP). *2019 Joint Conference of the IEEE International Frequency Control Symposium and European Frequency and Time Forum (EFTF/IFC)*, 1–4. https://doi.org/10.1109/FCS.2019.8856058

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

Haddon, W. (1973). Energy Damage and the Ten Countermeasure Strategies. *Human Factors*, *15*(4), 355–366. https://doi.org/10.1177/001872087301500407

Hofmann-Wellenhof, B., Legat, K., & Wieser, M. (2003). *Navigation, principles of position and guidance*. Springer-Verlag Wien New York.

Hovden, J., Albrechtsen, E., & Herrera, I. A. (2010). Is there a need for new theories, models and approaches to occupational accident prevention? *Safety Science*, *48*(8), 950–956. https://doi.org/10.1016/j.ssci.2009.06.002

JD. (2000). *NOU 2000: 24* [NOU]. regjeringen.no. https://www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/

JD. (2001, desember 13). *NOU 2001: 31* [NOU]. 012001-020013; regjeringen.no. https://www.regjeringen.no/no/dokumenter/nou-2001-31/id144519/

JD. (2002). *St.meld. Nr. 17 (2001-2002)* [Stortingsmelding]. regjeringen.no. https://www.regjeringen.no/no/dokumenter/stmeld-nr-17-2001-2002-/id402587/

JD. (2004). *St.meld. Nr. 39 (2003-2004)* [Stortingsmelding]. regjeringen.no. https://www.regjeringen.no/no/dokumenter/stmeld-nr-39-2003-2004-/id198241/

JD. (2006, april 5). *NOU 2006: 6* [NOU]. 012001-020038; regjeringen.no. https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/

JD. (2008). *St.meld. Nr. 22 (2007-2008)* [Stortingsmelding]. regjeringen.no. https://www.regjeringen.no/no/dokumenter/stmeld-nr-22-2007-2008-/id510655/

JD. (2012, juni 15). *Meld. St. 29 (2011–2012)* [Stortingsmelding]. Regjeringen.no; regjeringen.no. https://www.regjeringen.no/no/dokumenter/meld-st-29-20112012/id685578/

JD. (2015). *NOU 2015: 13* [NOU]. regjeringen.no. https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

JD. (2016). *Meld. St. 10 (2016–2017)* [Stortingsmelding]. regjeringen.no. https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/

JD. (2017, september 1). *Samfunnssikkerhetsinstruksen*. https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349/KAPITTEL_1#KAPITTEL_1

JD. (2019, september 3). *Veileder til samfunnssikkerhetsinstruksen* [BrosjyreVeiledning]. Regjeringen.no; regjeringen.no. https://www.regjeringen.no/no/dokumenter/veileder-til-samfunnssikkerhetsinstruksen/id2666864/

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2016). *Introduksjon til samfunnsvitenskapelig metode* (5. utg). Abstrakt.

JRC. (2019, juni 14). *The future of road transport* [Text]. EU Science Hub - European Commission. https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/future-road-transport

KMD. (2016, april 15). *Digital Agenda for Norge* [Stortingsmelding]. Regjeringen.no; regjeringen.no. https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/

Kongsvik, T., Albrechtsen, E., Antonsen, S., Herrera, I., Hovden, J., & Schifloe, P. M. (2018). *Sikkerhet i arbeidslivet*. Fagbokforl.

Nilsen, M., Haavik, T., & Almklov, P. (2019). *Social Capital and Disaster Resilience* (s. 3729). https://doi.org/10.3850/978-981-11-2724-3_0582-cd

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

Nkom. (2019). *EkomROS 2019* [Nyhet]. https://www.nkom.no/aktuelt/nyheter/tillit-aller-viktigst-i-sikkerhetsarbeidet

Perrow, C. (1999). *Normal Accidents—Living with high-risk technology*. Princeton Universiyt Press.

Pescaroli, G., & Alexander, D. E. (2015). A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos " metaphor. *Planet at Risk*, *Vol 3*(No 1).

Pescaroli, G., Green, L. M., Wicks, R. T., Turner, S., & Bhattarai, S. (2019). Cascading effects of global positioning and navigation satellite service failures. I *UCL Institute for Disaster and Risk Reduction: London, UK.* [Report]. UCL Institute for Disaster and Risk Reduction. https://doi.org/10.14324/000.rp.10076568

Rausand, M., & Utne, I. B. (2009). *Risikoanalyse teori og metoder*. Tapir akademisk.

Reason, J. (2000). Human error: Models and management. *BMJ*, *320*(7237), 768–770. https://doi.org/10.1136/bmj.320.7237.768

Rienecker, L., Stray Jørgensen, P., Skov, S., & Landaas, W. (2013). *Den gode oppgaven håndbok i oppgaveskriving på universitet og høyskole*. Fagbokforl.

SD. (2015, november 3). *Strategi for samfunnssikkerhet i samferdselssektoren* [Plan]. Regjeringen.no; regjeringen.no. https://www.regjeringen.no/no/dokumenter/strategi-for-samfunnssikkerhet-i-samferdselssektoren/id2460094/

SD. (2018a, mars 31). *Norges dronestrategi* [Plan]. Regjeringen.no; regjeringen.no. https://www.regjeringen.no/no/dokumenter/norges-dronestrategi/id2594965/

SD. (2018b, november 6). *På rett sted til rett tid* [Pressemelding]. Regjeringa.no; regjeringen.no. https://www.regjeringen.no/nn/aktuelt/ny-strategi-om-posisjon-navigasjon-og-tid/id2618052/

SD. (2019, juni 27). *Teknologi for bærekraftig bevegelsesfrihet og mobilitet. Rapport fra Ekspertutvalget—Teknologi og fremtidens transportinfrastruktur* [Rapport]. Regjeringen.no; regjeringen.no. https://www.regjeringen.no/no/dokumenter/teknologi-for-barekraftig-bevegelsesfrihet-og-mobilitet.-rapport-fra-ekspertutvalget---teknologi-og-fremtidens-transportinfrastruktur/id2662050/

Stortinget. (1996). *Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere («Lund-rapporten»)* [Dok]. Utvalg og kommisjoner. https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Dokumentserien/1995-1996/Dok15-199596/?lvl=0

SVV. (2020). *ITS – mer enn selvkjørende biler*. Statens vegvesen. https://www.vegvesen.no/fag/trafikk/its

Theunissen, E. (2014). So you think you are safe. *Coordinates*, *X*, 12.
VG. (2019, april 22). *Slik slår GPS-jammerne ut i helikoptrene*. VG. https://www.vg.no/i/BRxaL7

Karl Bjarne Kapaasen

Når tiden går i bane

NTNU
Kunnskap for en bedre verden