SANDRA BLIKÅS JENSEN
VEILEDER: ROGER FLAGE

Hvordan kan kunstig intelligens påvirke arbeidet med risikostyring og samfunnssikkerhet?

Masteroppgave 2024

Risk Analysis and Governance

Institutt for sikkerhet, økonomi og planlegging

Det teknisk-naturvitenskapelige fakultet

Forord

Denne oppgaven symboliserer avslutningen på mine seks år som student, hvor jeg har tatt et årsstudium i Ledelse, en bachelor i Samfunnssikkerhet og miljø, og tilbragt de to siste ved å ta en master i Risikoanalyse og styring ved Universitetet i Stavanger. Det har vært en lang og krevende prosess, men også veldig spennende og lærerikt.

Jeg vil takke alle medstudenter som har bidratt til gode diskusjoner og oppgaver. Takk til de veilederne som har gitt gode råd og veiledning. Takk til foreldrene mine for studiestøtte. Takk til samboeren min som har forsøkt å hjelpe og motivere meg når jeg har trengt det mest. Takk til hunden min for å gjøre arbeidshverdagen hakket koseligere.

Jeg vil rette en særlig takk til min veileder, Roger Flage, for uslåelig veiledning og gode samtaler. Det at du tildelte deg selv som veilederen min har vist seg å være noe av det beste som kunne skjedd for masteroppgaven min. Det har vært gøy og utrolig hyggelig å få samarbeide med deg.

Sandra Blikås Jensen

Stavanger, juni 2024

Sammendrag

Vi lever i et samfunn som blir stadig mer digitalisert, og hvor teknologi er i kontinuerlig utvikling. De siste årene har ord som «kunstig intelligens», «maskinlæring» og «stordata» blitt en del av dagligtalen, og stadig flere virksomheter implementerer slike systemer i sine arbeidsprosesser. Det å benytte seg av kunstig intelligens kan ha både fordeler og ulemper - og fokuset for denne oppgaven vil være å undersøke hvordan kunstig intelligens kan påvirke arbeidet med risikostyring og samfunnssikkerhet. Den overordnede problemstillingen vil, basert på dette, være følgende:

Hvordan kan kunstig intelligens påvirke arbeidet med risikostyring og samfunnssikkerhet?

For å svare på problemstillingen har jeg først sett på grunnleggende teori om risikostyring, samfunnssikkerhet og kunstig intelligens, samt eksisterende bruk av kunstig intelligens innenfor risikostyring og samfunnssikkerhet. Deretter har jeg utført en analyse, hvor jeg har identifisert utfordringer og behov både i litteraturen og praksis, hvilke muligheter kunstig intelligens kan ha for ulike oppgaver innenfor risikostyring og samfunnssikkerhet, samt hvilke aktører som kan ha nytte av dette.

I analysen fant jeg at kunstig intelligens har mange forskjellige muligheter for arbeidet med risikostyring og samfunnssikkerhet. Dette ble gjort ved å se på utvalgte konkrete teknologier, slik som mønstergjenkjenning, prediktiv analyse og automatisert beslutningsstøtte, overvåkning, og nevrale nettverk og veiledet læring, oppgaver som ulike aktører har innenfor risikostyring og samfunnssikkerhet i dag, samt hvilke aktører som kan ha nytte av disse KI-løsningene. For å nevne noen eksempler så kan eksempelvis mønstergjenkjenning brukes til å blant annet analysere, forutsi og advare om naturhendelser, mens overvåkning kan brukes til blant annet digital overvåkning for å oppdage og forebygge cyberangrep.

I diskusjonen tok jeg først for meg hvordan aktørene kan ta de ulike løsningene innenfor kunstig intelligens videre i praksis og implementere de i sin egen

virksomhet, ved hjelp av ni enkle skritt. Deretter så jeg på både utfordringer og etiske og juridiske dilemmaer ved bruk av kunstig intelligens, for å understreke og vise til at det finnes problemstillinger ved kunstig intelligens, som også er viktig å være klar over og ha gode retningslinjer for. Til slutt så jeg på begrensninger med oppgaven, som blant annet begrensninger rundt metoden, oppgaver som ble valgt, teori og konkret teknologi. Basert på disse begrensningene ga jeg også forslag til videre forskning. Et eksempel på dette er at fremtidig forskning bør inkludere et bredere utvalg av oppgaver innenfor risikostyring og samfunnssikkerhet.

Studien konkluderer med at kunstig intelligens kan presentere et betydelig forbedringspotensial med tanke på utfordringer og behov i litteraturen og praksis. Kunstig intelligens-teknologier kan tilby løsninger som blant annet kan effektivisere prosesser og automatisere oppgaver som mennesker ikke kan håndtere like effektivt, brukes til å identifisere og kategorisere risikoer og svakheter, evaluere sannsynligheter og konsekvenser, forutsi hendelser og optimalisere barrierer, samt gi mer presise og nøyaktige analyser. Selv om kunstig intelligens har et stort potensial, er det imidlertid viktig å være oppmerksom på de etiske og juridiske dilemmaene. Dette krever klare retningslinjer for å sikre en ansvarlig implementering av KI i arbeidet risikostyring og samfunnssikkerhet.

Innhold

1. Innledning

Innledningsvis vil jeg presentere bakgrunnen for oppgaven, hva målet med oppgaven er, og valg av problemstilling basert på dette målet, samt metoden som har blitt brukt for å løse denne problemstillingen.

1.1. Bakgrunn

Denne oppgaven forsøker å se på hvilke muligheter kunstig intelligens kan ha for ulike utfordringer og behov innenfor risikostyring og samfunnssikkerhet, både i litteraturen og i praksis. Oppgaven dreier seg i stor grad om tre kjernebegreper: kunstig intelligens, maskinlæring og stordata. Kunstig intelligens er enkel forklart tankeprosesser utført av maskiner (Laskowski & Tucci, 2023). Maskinlæring er vitenskapen om å få en datamaskin til å handle uten programmering (Laskowksi & Tucci, 2023). Stordata er en kombinasjon av strukturert, semistrukturert og ustrukturert data, som organisasjoner samler inn, analyserer og henter informasjon og innsikt i (Bigelow & Botelho, 2022).

Kunstig intelligens, maskinlæring og stordata anvendes allerede i en rekke sektorer. For eksempel benyttes kunstig intelligens i helsevesenet for bedre og mer effektiv diagnostikk, forbedring av pasientenes opplevelse, utnytte begrensede ressurser best mulig og utvikling av nye legemidler (SINTEF, u.å.). Innen finanssektoren har maskinlæring blitt brukt for å identifisere svindel, inkludert avsløring av bedriftssvindel, kredittkortsvindel, hvitvasking av penger, boliglånsvindel, massemarkedsføringssvindel og råvaresvindel (Song et al., 2014).

Det finnes flere eksempler på eksisterende bruk av kunstig intelligens innenfor risikostyring og samfunnssikkerhet. Riddell et al. (2019) har gjennomført en utforskende scenarioanalyse for katastroferisikoreduksjon, hvor de har sett på alternative «veier» i katastroferisikovurdering. FHI (2023) så på scenariomodellering og de ulike fordelene og utfordringer med slike modeller, i sin rapport om erfaringer fra koronapandemien. Et annet eksempel er Casagli et al. (2021) som har studert overvåkning og tidlig varsling i forbindelse med jordskred, for å få en bedre forståelse og redusere risikoen. Boletsis & Nilsson

(2021) har på sin side skrevet en rapport med fokus på risikobevisst beslutningsstøttesystem for tunnelsikkerhet, med fokus på hvordan teknologi kan være et viktig verktøy.

Til tross for at det allerede foreligger eksisterende forskning om kunstig intelligens i tilknytning risikostyring og samfunnssikkerhet mangler der fortsatt en studie som systematisk sammenligner utfordringer og behov knyttet til risikostyring og samfunnssikkerhet, med de mulighetene kunstig intelligens kan ha for å løse eller forbedre disse. Mulighetene er mange, og det finnes både utallige oppgaver og aktører innenfor risikostyring og samfunnssikkerhet, som kan ha nytte av de ulike løsningene som kunstig intelligens kan bidra med.

For å fylle dette kunnskapsgapet har jeg forsøkt, med denne oppgaven, å oppnå ny kunnskap innenfor dette feltet – ved å identifisere ulike utfordringer og behov i litteraturen og praksis, se på konkrete teknologier i forbindelse med mulighetene disse har for ulike oppgaver, og hvilke aktører som er relevant og kan ha nytte av disse løsningene.

1.2. Mål for oppgaven

Målet for oppgaven har vært å *oppnå ny kunnskap* om hvordan kunstig intelligens kan påvirke risikostyring og samfunnssikkerhet. Basert på dette vil den overordnede problemstillingen være følgende:

«Hvordan kan kunstig intelligens påvirke arbeidet med risikostyring og samfunnssikkerhet?».

For å svare på denne problemstillingen, og dermed oppnå målet for oppgaven vil jeg først avklare og se på de ulike aspektene av risikostyring og samfunnssikkerhet. Deretter vil jeg utforske og presentere nye teknologier, i dette tilfellet kunstig intelligens, maskinlæring og stordata. Videre vil jeg se på eksisterende bruk av kunstig intelligens i risikostyring og samfunnssikkerhet. Etter dette vil jeg utforske hvilke utfordringer og behov som finnes i litteraturen og i praksis. Basert på dette vil jeg undersøke hvilke muligheter som konkrete teknologier har for oppgaver innenfor risikostyring og samfunnssikkerhet, og

hvilke aktører dette er relevant for. Jeg vil også se på hvordan kunstig intelligens påvirker risiko- og sårbarhetsanalyser. Deretter vil jeg ta for meg noen steg som aktører kan følge dersom de ønsker å implementere kunstig intelligens. For å få en mer balansert diskusjon vil jeg også ta for meg svakheter og etiske og juridiske dilemmaer med kunstig intelligens. Til slutt vil jeg se på begrensninger med oppgaven og gi forslag for videre forskning, før jeg så gir en konklusjon basert på funnene i oppgaven.

1.3. Metode

I denne delen av oppgaven vil jeg presentere hvilken metode og fremgangsmåte som jeg har benyttet meg av for å belyse oppgavens overordnede problemstilling.

Jeg har valgt å benytte meg av kvalitativ forskning, da jeg anser dette som best egnet for å svare på oppgavens problemstilling. Kvalitativ forskning søker å beskrive og gå i dybden på et fenomen (Ringdal, 2018). Videre har jeg valgt å bruke dokumentanalyser for min oppgave. Dokumentanalyser er en type sekundærdata, som er data som allerede foreligger, i form av artikler, rapporter og bøker. Som Thagaard (2018) fremhever, vil fordelen med å bruke foreliggende tekster være at de ofte er lett tilgjengelig, og at analyser av slike tekster ikke har de etiske begrensningene som analysen av feltdata har. Årsaken til at jeg har valgt å benytte meg av dokumentanalyse er fordi det allerede finnes en del foreliggende data om de områdene som jeg tar for meg i oppgaven. Snyder (2019) viser til at, ved å integrere funn og perspektiver fra mange ulike empiriske studier, så vil en litteraturgjennomgang gi et mye mer omfattende svar på problemstillingen - enn det jeg kunne fått fra å gjøre en egen empirisk studie. Det vil også være en god metode for å oppdage områder hvor det trengs videre forskning.

Ettersom oppgaven handler om hvordan kunstig intelligens kan påvirke arbeidet med risikostyring og samfunnssikkerhet på en generell basis, så jeg i utgangspunktet ikke behovet for å intervjue enkeltpersoner, og intervju ble grunnet dette avskrevet som metode.

Mitt mål for oppgaven har vært å *oppnå ny kunnskap* om hvordan kunstig intelligens kan påvirke arbeidet med risikostyring og samfunnssikkerhet, og jeg har derfor lest, studert og analysert ulike dokumenter for å få en grunnleggende forståelse av teori knyttet til risikostyring og samfunnssikkerhet, kunstig intelligens og eksisterende bruk av kunstig intelligens innenfor risikostyring og samfunnssikkerhet, samt hvordan alt henger sammen. Dette har vært helt essensielt for å kunne analysere hvilke utfordringer og behov som finnes både i litteraturen og praksis når det gjelder risikostyring og samfunnssikkerhet, og se kunstig intelligens i forhold til dette for å finne ut av hvilke muligheter som eksisterer innenfor dette området.

Ved innsamling av de dokumentene som vil danne grunnlaget for den teoretiske delen av oppgaven, må man ha en plan. En slik plan er nødvendig for en systematisk gjennomgang av dokumentene, for å finne relevante funn (Lynggaard, 2010). Innsamling av dokumenter i denne oppgaven, har blitt gjort gjennom systematiske søk i Google Scholar, Oria, bøker, nettsider, artikler og rapporter – med sikte på å finne et solid grunnlag for de ulike områdene som oppgaven gjør rede for. Data jeg har benyttet, tar for seg ulike problemstillinger og har ulike fokus, noe som har gitt meg mulighet til å se på oppgaven fra flere ulike perspektiver. Alle dokumentene som har blitt benyttet i denne oppgaven er også offisielle og lett tilgjengelige, for å sikre transparens i oppgaven.

2. Teori

Dette kapittelet vil ta for seg teori, som vil legge grunnlaget for forståelsen og utgangspunktet for resten av oppgaven. I første delkapittel vil samfunnssikkerhet og risikostyring presenteres, hvor man vil se på viktige områder innenfor arbeidet med samfunnssikkerhet, som blant annet beredskap, og kriseforebygging- og håndtering. Deretter vil et avsnitt om risiko og dets betydning for samfunnssikkerhet presenteres, samt hvordan risikostyring vil forstås i denne oppgaven. Til slutt vil ulike metoder for samfunnssikkerhet og risikostyring presenteres, som vil legge grunnlaget for hvilke potensielle forbedringer og endringer som kan drives frem av kunstig intelligens. I neste delkapittel vil kunstig intelligens, maskinlæring og stordata, forklares og gis med noen eksempler. Det siste delkapittelet vil ta for seg den eksisterende bruken av kunstig intelligens innenfor risikostyring og samfunnssikkerhet, med sikte på risikovurdering, overvåkning, scenariomodellering, sensorteknologi og automatisert beslutningsstøtte.

2.1. Samfunnssikkerhet og risikostyring

Samfunnssikkerhet er et sentralt begrep i Norge. Hvordan man ser på samfunnssikkerhet vil være avhengig av mange faktorer - slik som ståsted, ansvar, bakgrunn, bestemte situasjoner eller hva man ønsker å studere (Engen et al., 2016). Stortingsmelding nr. 17 (2001-2002) definerer samfunnssikkerhet som «den evnen samfunnet som sådan har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger». Denne definisjonen virker derimot å legge mest vekt på evnen til å håndtere kriser etter at de har oppstått. Kruke et al. (2005) viser til at samfunnets evne til å opprettholde viktige samfunnsfunksjoner i høyest grad vil være avhengig av hva man har gjort for å forebygge og forberede seg på kriser *før* de oppstår, samt hvordan man håndterer oppbyggingsfasen etter en krise. Basert på dette kan man si at samfunnssikkerhet omfatter forebygging av kriser, forberedelser for å takle kriser, håndtering av kriser når de oppstår, samt evnen til å gjenvinne funksjonaliteten etterpå (Engen et al., 2016).

Proaktivt sikkerhetsarbeid for forebygging av ulykker, kriser og katastrofer har dermed høy prioritet i arbeidet med samfunnssikkerhet. Noen kriser vil derimot oppstå til tross for godt forebyggende arbeid, som en form for uorden som ikke kan forebygges (Engen et al., 2016). Basert på dette kan man si at en krise medfører en endring fra en normaltilstand, som er uønsket, og som bringer med seg problemer som ikke kan løses gjennom ordinær organisering.

Beredskap er også en viktig del av samfunnssikkerhetsarbeidet, og er de tiltakene som skal bidra til å hindre at farlige situasjoner får utvikle seg til ulykker, eller tiltak rettet mot å redusere konsekvensene av de uønskede hendelsene når de først har oppstått (Njå et al., 2020). Kruke et al. (2005) sitt syn på forebygging, forberedelser og håndtering, som sett over, understreker viktigheten av beredskap og planlegging, da det er dette som vil legge føringer for arbeidet med kriser. Beredskapsplanlegging kan defineres som bruken av egen metodologi for å lage planer for håndteringen av uønskede hendelser (Bjelland & Nakstad, 2018).

Sentralt i tenkningen om, og arbeidet med sikkerhet, står begrepet risiko (Engen et al., 2016). Grunnleggende så handler risiko om fremtiden og hva som eventuelt kan skje, og hvilke konsekvenser dette potensielt kan medføre. Usikkerhet er blant de viktigste dimensjonene når man snakker om risiko og har stadig fått en større rolle, noe som også har gjort at de etiske og politiske dimensjonene både ved arbeidet med risiko og sikkerhet mer tydelig (Engen et al., 2016). Årsakene til uønskede hendelser foreligger ofte i et komplekst samspill mellom teknologi, organisatoriske og menneskelig faktorer (Aven et al., 2004). Begrepet sikkerhet brukes ofte om forebyggende tiltak der hensikten er å redusere sannsynligheten for at noe uønsket skal skje, eller redusere konsekvensene av slike uønskede hendelser. Dagens trusselbilde handler ikke bare om ulykker og hendelser som faktisk forekommer, selv om disse kan være viktige indikasjoner på risiko - men også trusler som vi har liten eller ingen erfaring med (Aven et al., 2004). Med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko (Aven, 2015). På den ene siden handler risikostyring om å få innsikt i risikoforhold, effekt av tiltak, grad av styrbarhet av risikoer og så videre, mens på den andre siden har man metoder, prosesser og strategier for å

kunne kartlegge og styre risikoene. Oppgaven vil i størst grad ta for seg ulike metoder for risikostyring, slik som risiko- og sårbarhetsanalyser, risikomatriser og sløyfemodeller.

Risikostyring innebærer ofte beslutningstaking i situasjoner med høy risiko og store usikkerheter. Slik beslutningstaking er utfordrende ettersom det er vanskelig å forutsi konsekvensene av beslutningene (Aven, 2015). Ved å ta riktige beslutninger kan vi være med på å påvirke fremtiden, og dermed øke sjansene for å oppnå ønskede utfall av våre aktiviteter. Risikostyring kan forstås både smalt og bredt, avhengig av hvilke aspekter man ser på. I denne oppgaven vil risikostyring omfatte risikovurdering og risikohåndtering. Risikovurdering vil her referere til totaliteten av analyse og evaluering som risikovurdering. I en risikostyringsprosess vil risikovurdering følges av risikohåndtering. Risikohåndtering er prosessen og implementeringen av virkemidler for å modifisere risiko, herunder virkemidler som benyttes for å unngå, redusere, optimalisere, overføre og beholde risiko (Aven, 2015).

2.1.1. Metoder for samfunnssikkerhet og risikostyring

Samfunnssikkerhet og risikostyring er komplekse fagområder, og inneholder mange forskjellige metoder, prosesser, modeller, rammeverk også videre. Her vil fokuset være på ulike metodiske prosesser og modeller som er en del av slike prosesser – hvordan disse brukes i dag, og senere i oppgaven, hvordan kunstig intelligens potensielt kan forbedre og styrke disse metodene.

2.1.1.1 Kriseforebygging og beredskapsplanlegging

Kriseforebygging er de tiltakene man gjør for å forhindre at en krise oppstår. Slike tiltak kan for eksempel være risikoanalyser og beredskapsplanlegging. Som sett så vil beredskapsplanlegging legge føringer for håndteringen av kriser, og omfatter utvikling av planer og prosedyrer for å håndtere ulike kriser eller nødssituasjoner. Også her vil det være viktig å vurdere hvilke risikoer som kan være av betydning.

2.1.1.2 Risiko- og sårbarhetsanalyser

Risiko- og sårbarhetsanalyser (ROS-analyser) innebærer en systematisk identifisering og kategorisering av risiko, og skal hjelpe til med å kartlegge behovet for sikkerhetsstyring, iverksetting av tiltak og hvordan ulike virkemidler og løsningsforslag kan lede til definerte mål (Aven et al., 2004). ROS-analyser kan brukes til å identifisere faremomenter og sårbarhet for virksomheter som skal planlegge fremtidige løsninger og tiltak. Ved å benytte seg av slike analyser vil det være mulig å skille mellom ulike løsningers og tiltaks effekt på sikkerhetsnivået. Resultatene av dette kan videre integreres i virksomheters generelle beredskaps- og planarbeid, og kan danne grunnlaget for å etablere risikoreduserende tiltak.

Risikomatrise

En risikomatrise er en tabell som har flere kategorier av sannsynlighet eller frekvens for radene, og flere kategorier av konsekvens, alvorlighet og innvirkning for kolonnene – eller motsatt (Cox, 2008). Det er vanlig å dele inn i 3-5 kategorier for hver av de to dimensjonene, som også viser til om risikoen er lav, medium eller høy med utgangspunkt i fargene grønn, gul og rød.

Sløyfemodell

Et av hovedmålene med å utføre risikoanalyser er å beskrive risiko, eller med andre ord, å presentere et informativt risikobilde (Aven, 2015). En av måtene å gjøre dette på, er å bruke sløyfemodell (bow-tie) som metode. En sløyfemodell er formet som en sløyfe, og viser hendelsesforløpet før og etter en uønsket hendelse. I midten av sløyfen har man den initierende hendelsen, på venstresiden finner man medvirkende faktorer som kan føre til den initierende hendelsen, mens på høyresiden finner man de mulige konsekvensene dersom den initierende hendelsen oppstår. På venstresiden vil man også finne ulike barrierer som har som mål å forhindre den initierende hendelsen, såkalte sannsynlighetsreduserende barrierer, mens på høyresiden er det barrierer som har som mål å forhindre at den initierende hendelsen medfører alvorlige konsekvenser, såkalte konsekvensreduserende barrierer. Om den initierende

hendelsen oppstår, og hvor bra de ulike barrierene fungerer, vil også påvirkes av en rekke faktorer. Risikoanalysen har som formål å identifisere de relevante initierende hendelsene og utvikle sannsynlighets- og konsekvensbildet (Aven, 2015). Hvordan dette gjøres er avhengig av hvilken metode som blir brukt og hvordan resultatene skal brukes.

2.2. Kunstig intelligens, maskinlæring og stordata

Utforskning av innovative tilnærminger til risikostyring og samfunnssikkerhet, som for eksempel bruk av kunstig intelligens (KI), maskinlæring og stordataanalyse, er viktig da det kan gi nye og potensielt bedre løsninger for hvordan man arbeider med disse områdene i dag - eller med andre ord, hvordan KI kan transformere praksis. Det er også viktig å vurdere hvordan endringer i teknologi kan påvirke organisatoriske prosesser, beslutningstaking og samarbeid på tvers av ulike aktører innen samfunnssikkerhetsområdet.

I dette delkapittelet vil både KI, maskinlæring, dyp læring og stordata presenteres, ved å se på hva det er, hvordan det kan tas i bruk, hva slags potensialet det har, samt likheter og forskjeller.

2.2.1. KI

KI, maskinlæring og stordata har blitt vanlige begreper, ikke bare innen bedrifts-IT, men også generelt i samfunnet - og brukes noen ganger om hverandre (Laskowski & Tucci, 2023). Selv om de til tider brukes om hverandre har de ulikheter.

KI referer til simulering av menneskelig intelligens av maskiner, og dekker et sett med evner i stadig endring, etter hvert som nye teknologier utvikles. KI er, med andre ord, menneskelige tankeprosesser utført av maskiner, og da særlig datamaskiner (Laskowski & Tucci, 2023). Generelt fungerer KI-systemer ved å innta store mengder av merkede treningsdata, analysere dataen for korrelasjoner og mønstre, samt å bruke disse mønstrene til å forutse fremtidige tilstander. KI-

programmering fokuserer på kognitive ferdigheter slik som læring, resonnering, selvkorrigering og kreativitet (Laskowski & Tucci, 2023). Lærings-aspektet fokuserer på å innhente data og lage regler for hvordan det kan omgjøres til brukbar informasjon. Reglene som KI baserer seg på, også kalt algoritmer, gir datamaskiner trinnvise instruksjoner for hvordan de skal fullføre en spesifikk oppgave. Resonnerings-aspektet fokuserer på å velge den riktige algoritmen for å nå et ønsket resultat, mens selvkorrigerings-aspektet er lagd for å kontinuerlig finjustere algoritmer og sikre at de gir mest mulig nøyaktig resultat. Kreativitets-aspektet bruker nevrale nettverk, regelbaserte systemer, statistiske metoder og andre KI-teknikker for å generere nye bilder, tekst, musikk og ideer (Laskowski & Tucci, 2023).

KI er viktig grunnet det potensialet det har til å endre hvordan vi lever og jobber. Det har blitt effektivt brukt i virksomheter for å automatisere oppgaver utført av mennesker, som for eksempel servicearbeid, oppdagelse av svindel og kvalitetskontroll (Laskowski & Tucci, 2023). KI kan, på en rekke områder, utføre oppgaver mye bedre enn mennesker - særlig når det kommer til oppgaver som er repeterende og detaljorientert. KI-verktøy utfører ofte jobben raskt og med relativt få feil. Grunnet de enorme datasettene som KI kan behandle, vil den også kunne gi bedrifter innsikt i deres egen drift, som de kanskje ikke var klar over (Laskowski & Tucci, 2023). Teknologier som kommer under «paraplyen» til KI inkluderer både maskinlæring, dyp læring og stordata.

2.2.2. Maskinlæring og stordata

Maskinlæring gjør det mulig for programvareapplikasjoner å bli mer nøyaktige til å forutse utfall uten å være eksplisitt programmert til å gjøre det (Laskowski & Tucci, 2023). Maskinlæringsalgoritmer bruker historiske data som input for å forutsi nye utgangsverdier. Denne tilnærmingen ble mye mer effektiv med fremveksten av store datasett å trene på. Dyp læring er en undergruppe av maskinlæring, og er basert på vår forståelse av hvordan hjernen er strukturert. Det bruker kunstige nevrale nettverksstrukturer som grunnlag for nyere fremskritt innen KI, inkludert selvkjørende biler og chatgpt. Det enorme volumet av data

som opprettes på daglig basis vil begrave mennesker, mens KI-applikasjoner som bruker maskinlæring, kan ta disse dataene og raskt omgjøre de til brukbar informasjon (Laskowski & Tucci, 2023).

Maskinlæring og stordata brukes ofte sammen, men er samtidig forskjellig. I mange tilfeller vil stordata være så stort og komplekst at tradisjonelle databehandlingsteknologier ikke greier å prosessere, lagre og administrere dem effektivt (Walch, 2021). Fremtidstenkende selskaper bruker intelligente og avanserte analyser for å trekke ut mer verdi fra dataene i systemene deres, derav særlig maskinlæring. Maskinlæring kan oppdage mønstre og gi kognitive evner på tvers av store datavolumer, noe som gir organisasjoner evnen til å ta initiativene sine for stordataanalyse til neste nivå (Walch, 2021).

Stordata er en kombinasjon av strukturert, semistrukturert og ustrukturert data samlet inn av organisasjoner, og som kan utvinnes for informasjon og brukes i maskinlæringsprosjekter, prediktiv modellering og andre avanserte analyseapplikasjoner (Bigelow & Bothelo, 2022). Stordata blir ofte karakterisert av de «tre V'ene» (volume, variety og velocity). Dette referer til det store volumet av data i mange miljøer, den store variasjonen av datatyper som ofte lagres i store datasystemer, og den hastigheten som mye av dataene genereres, samles inn og behandles med.

Det finnes utallige eksempler på hva maskinlæring og stordata kan brukes til i et risiko-perspektiv. Blant disse kan man trekke frem kredittvurdering hvor maskinlæring kan brukes til å vurdere kredittrisiko, og sikkerhetsanalyser som kan benytte maskinlæring for å oppdage unormale aktiviteter og potensielle sikkerhetsbrudd.

Basert på dette kan man se at det å bruke maskinlæringsalgoritmer for stordataanalyse er et logisk skritt for selskaper som ønsker å maksimere dataenes potensielle verdi. Maskinlæringsverktøy bruker datadrevne algoritmer og statistiske modeller for å analysere datasett og deretter trekke slutninger fra identifiserte mønstre, eller å forsøke å forutse hva som vil skje basert på dem. Algoritmene lærer av dataene når de blir kjørt opp mot hverandre, i motsetning til

tradisjonelle regelbaserte analytiske system som følger eksplisitte instruksjoner (Walch, 2021).

2.3. Eksisterende bruk av KI for risikostyring og samfunnssikkerhet

I dette delkapittelet oppsummeres publiserte eksempler på eksisterende bruk av KI. KI har potensial for å forbedre effektiviteten og nøyaktigheten til tradisjonelle risikostyringsmetoder, og dermed styrke samfunnets evne til å identifisere, vurdere og håndtere risikoer på en proaktiv måte. Teknologi, og derav bruken av KI, kan være nyttig innenfor mange områder, men omfanget er her avgrenset til risikovurdering, scenariomodellering og overvåkning, tidlig varsling, overvåking og sensorteknologi, og automatisert beslutningsstøtte.

2.3.1. Risikovurdering, scenariomodellering og overvåkning

KI kan brukes til å modellere komplekse scenarioer og vurdere risiko ved å analysere historiske data, simuleringsmodeller og sanntidsinformasjon. Dette kan hjelpe myndigheter med å forstå potensielle konsekvenser og utvikle effektive beredskapsplaner.

Riddell et al. (2019) utførte en utforskende scenarioanalyse for katastroferisikoreduksjon, hvor de så på alternative «veier» i katastroferisikovurdering. Scenarioene som ble utviklet, og de påfølgende analysene av dem, kombinerer kunnskap og innsikt fra interessenter og eksperter, samt bruken av simuleringsmodellering til å muliggjøre at scenarioer med kvalitative og kvantitative elementer kunne integreres i risikovurderingsprosesser og bidra til strategiske risikobehandlinger.

Riddell et al. (2019) definerer scenariomodellering som bruken av datamaskin-baserte modelleringssystemer til å simulere fremtidige dynamikker basert på input-drivere og modellparametere. For å vurdere scenarioer ved bruk av simulering, parametere, innganger, grensebetingelser og selve modellstrukturen, vil disse områdene bli tilpasset for å representere og bedre informere scenarioets

narrativ. Riddell et al. (2019) argumenterer videre for at simuleringsmodeller av scenarioer støtter utforskning av usikkerhet ved at man vurderer alternative drivere i en konsekvent og sammenlignbar måte med de samme kvantitative utgangene, og at det også kan støtte utforskning og reduksjon av kompleksitet og kommunikasjon av usikkerhet, gjennom det kravet det har om å vurdere ulike tolkninger av fremtiden gjennom utforskning av et begrenset antall parametere og dens verdi som en struktureringsenhet for problemer. Et eksempel de så på var utviklingen av alternative risikoscenario-veier, hvor de simulerte risikoer for hvert år over ulike fremtidige scenarioer, og dermed kunne se risikoene opp mot tid for hver vei.

Disse alternative veiene i risikokatastrofevurdering ble deretter anvendt i en case-studie i Greater Adelaide i Sør-Australia, for å demonstrere nytten av tilnærmingen i form av dets evne til å innarbeide usikkerhet og kompleksitet for fremtidig risikovurdering. Sør-Australia består av en risikoprofil med ulike farer, hvor den største er flom og kostnadene dette medfører, samt betydelige skogbranner (Riddell et al., 2019).

Implementeringen av denne tilnærmingen ble støttet ved å bruke «UNHaRMED», en programvare-applikasjon som er designet for å utforske fremtidige katastroferisikoer og forbedre langtids forståelsen av katastroferisiko, og tillater testing av ulike risikoreduksjonsmuligheter opp mot alternative scenarioer av sosio-økonomiske og miljømessige faktorer. Programvaren modellerer risikoen fra flere ulike typer naturfarer, og i denne case-studien baserte den seg på kystflom, skogbranner og jordskjelv. Dette vil vise brukerne hvordan risikoer fra de ulike farene endrer seg i fremtiden, basert på produksjonen av policy-relevante beregninger, slik som gjennomsnittlig årlig tap for ulike scenarioer og risikoreduksjonsbeslutninger.

Basert på dette kan man se at scenariomodellering av risiko muliggjør en dynamisk representasjon av hvordan risiko endres over den modellerte horisonten, med variasjoner i risikoprofiler som blir drevet av forskjellene i scenariovariabler, slik som modelldrivere og parametere. Resultatene av denne

modelleringen vil deretter kunne brukes til å vurdere drivere og systemer for risiko.

Et annet eksempel på hvor scenariomodellering har vært av betydning for risikostyring, både i praksis og som er litt nærmere oss, var under koronapandemien. Folkehelseinstituttet (FHI) (2023) presenterte en rapport om erfaringer fra koronapandemien, med fokus på lærdommer og anbefalinger for FHI og den nasjonale beredskapen. Blant aktuelle kunnskapsfunksjoner som de mener er viktige i kriser blir det vist til at det bør øves på kobling av analyse og utbruddsrelevant registerdata, å sette opp prioriterte systematiske søk, og modellering av pandemiscenarioer og andre mulige scenarioer for den videre utviklingen, gitt den kunnskapen som man har tilgjengelig. FHI (2023) trekker videre frem scenariomodellering som viktig beslutningsstøtte til nasjonale myndigheter. I FHI's arbeid med å anbefale strategier mot pandemien var scenariomodellering sammen med annen kunnskap og risikovurdering nyttig. FHI (2023) trekker imidlertid frem utfordringer ved slike modeller, da det kan være vanskelig å kommunisere usikkerheten og forskjellen mellom scenarioer og prognoser. Videre anbefales det at scenariomodelleringen bør videreutvikles. FHI (2023) påpeker at nytten og kvaliteten av scenariomodellering kan økes ved bedre integrering av modelleringsarbeid i en eventuell fremtidig krisehåndtering, mer samarbeid med andre modelleringsmiljøer både nasjonalt og internasjonalt, ved planlagt tilgang til regnekraft, samt ved tilgang til bedre datagrunnlag gjennom overvåkning og forskning. Dersom FHI's modelleringsgruppe greier å opprettholde og videreutvikle kompetansen gjennom modellering til bruk i det daglige, bygge erfaring med ulike modeller og analyseprosesser som kan være aktuell ved fremtidige kriser, og ved å øve på og utvikle kunnskapen om å kommunisere resultater og usikkerhet i offentligheten, samt dialog med beslutningstakere, kan også beredskapen forbedres.

2.3.2. Tidlig varsling, overvåkning og sensorteknologi

KI algoritmer kan analysere store mengder av data fra sensorer og andre kilder for å identifisere potensielle risikofaktorer. Sensorer, overvåkningssystem og

droner, samt andre enheter, kan for eksempel gi informasjon i sanntid om naturkatastrofer, ulykker og andre trusler. Det kan også samle inn sanntidsinformasjon for å overvåke miljømessige, geopolitiske og sosiale forhold.

Casagli et al. (2021) så på overvåkning og tidlig varsling i forbindelse med å få en bedre forståelse og redusere risikoen for jordskred. Basert på flere case-studier trekker de frem tidlige varslingssystem som det mest effektive og kostnads-effektive verktøyet, som risikoreduserende tiltak. Overvåkningssystemer, basert på fjernmålingsteknikker, representerer effektive og robuste verktøy for risikoreduksjon, og tillater en lav miljømessig og økonomisk påvirkning, samt høy operasjonssikkerhet i vanskelige forhold. Ettersom studien omhandlet jordskred, brukte de «radar interferometry», oversatt til norsk som «syntetisk apertur radar interferometri» (InSAR), som teknikk. InSAR er den teknikken som gjør det mulig å måle bakkens bevegelser med mm til cm oppløsning, og er derfor egnet til å detektere, kartlegge og overvåke dyptliggende fjellskred og overflatiske krypende landformer (NORCE, u.å.). Casagli et al. (2021) påpeker at InSAR er en av de mest utbredte og pålitelige metodene, med fordeler som veldig høy nøyaktighet, mulighet for å operere under alle slags værforhold, og høy romslig og tidsmessig dekning. Til tross for at hovedfokuset var jordskred, så de også på hvordan man kan bruke tidlige varslingssystemer for steinras og vulkansk miljø.

2.3.3. Automatisert beslutningsstøtte

Implementering av automatiserte systemer basert på KI kan hjelpe beslutningstakere med å håndtere informasjonsstrømmen mer effektivt. Dette kan være spesielt viktig under kritiske situasjoner.

SINTEF utga i 2021 en rapport om risikobevisst beslutningsstøttesystem for tunnelsikkerhet. Her trekker de frem hvordan teknologi kan være et viktig verktøy for å forbedre effektiviteten i beredskapsledelse og personsikkerhet i tunneler. De definerer beslutningsstøttesystemer som automatiserte prosesser som kan brukes til å analysere «inputs» som de får fra tunnelsensorer og data, og som kan hjelpe tunneloperatører med å ta en beslutning i nødssituasjoner. De viser også til

viktigheten av ulykkesforebygging. Ettersom GPS ikke fungerer i tunneler så vil det være ekstra viktig å ha andre sikkerhetstiltak som kan gi den informasjonen man trenger.

I nødssituasjoner vil man ofte være utsatt for tidspress og vil dermed også måtte ta raske avgjørelser, og det er derfor viktig å ha tilgjengelig beslutningsstøtte. Tidligere undersøkelser har vist til beslutningsstøttesystemer som fordelaktig for beredskapsledelse i komplekse situasjoner (Boletsis & Nilsson, 2021). Boletsis & Nilsson (2021) sin rapport baserer beslutningsstøttesystemer sin forebyggende operasjon på innsamling av «inputs» fra tilgjengelige tunnelteknologier/sensorer, som deretter analyseres, og tildeler en risikoklasse til hvert kjøretøy i tunnelen. Dersom risikoklassen anses som for høy, vil et forslag til handling samt en forklaring på dette forslaget bli sendt fra systemet til tunneloperatøren. Tunneloperatøren vil da kunne ta en informert beslutning for å forhindre ulykker og informere trafikantene, kontakte førstehjelpspersonell dersom nødvendig, samt ta i bruk tunnelens nødutstyr.

3. Analyse

Denne delen av oppgaven vil være min egen analyse av hvilke utfordringer og behov som eksisterer innenfor risikostyring og samfunnssikkerhet i dag, med fokus på både litteratur og praksis, og deretter hvilke muligheter jeg ser for bruk av KI for å løse disse utfordringene og behovene.

3.1. Utfordringer og behov innenfor risikostyring og samfunnssikkerhet i dag

Risikostyring og samfunnssikkerhet er begge fagområder med mange utfordringer, behov, kunnskapshull og forbedringspotensialer. I denne delen vil det først presenteres en analyse av utfordringer og behov i litteraturen med utgangspunkt i teori-delen, og deretter en analyse av utfordringer og behov i praksis.

Basert på teorien om risikostyring og samfunnssikkerhet som har blitt sett på så langt, er det et klart fokus på det å identifisere og vurdere risikoer, og å implementere tiltak for å håndtere disse. De ulike konseptene og metodene som tidligere har blitt nevnt, slik som risikoanalyse, risikovurdering, krisehåndtering og beredskapsplanlegging, gir et godt grunnlag for å både forstå og håndtere ulike risikoscenarioer, samt for å bygge robuste systemer som effektivt kan respondere på kriser. Til tross for at disse gir et godt grunnlag, er det likevel noen utfordringer og behov både i litteraturen og i praksis, som muligens kan ha nytte av ulike KI-løsninger.

3.1.1. Utfordringer og behov i litteraturen

Det finnes flere utfordringer og kunnskapshull, som er viktig å adressere. Samfunnssikkerhet er et begrep som er definert på ulike måter. Mens den generelle definisjonen i Stortingsmelding nr. 17 (2001-2002) anses som omfattende, påpeker Kruke et al. (2005) visse mangler. De hevder at samfunnets evne til å opprettholde viktige funksjoner ikke bare avhenger av responsen under

en hendelse, men også av forberedelsene i forkant og gjenoppbyggingen i etterkant. Til tross for innsatsen i å forebygge, vil noen kriser være uunngåelig. En nøkkelutfordring er dermed å forberede seg på og håndtere disse uforutsette hendelsene.

Beredskap og planlegging, som fremhevet av Kruke et al. (2005), er avgjørende for effektiv håndtering av kriser. Imidlertid kan kontinuerlig oppdatering og utvikling av beredskapsplaner være en utfordring. Det er vanskelig å planlegge for hendelser som man ikke kjenner til eller som anses som usannsynlige, og som kan føre til uforutsette konsekvenser.

Arbeidet med risikohåndtering er ytterligere komplisert av usikkerhet, som påpekt av Engen et al. (2016). Mangelen på kunnskap om fremtidige risikoer og deres implikasjoner er dermed en annen svakhet.

Komplekse samspill mellom teknologiske, organisatoriske og menneskelige faktorer, som påpekt av Aven et al. (2004), er en annen utfordring som krever en helhetlig tilnærming til risikostyring. I tillegg kan trusler som er ukjente eller som man har begrenset erfaring med, forverre denne kompleksiteten.

Beslutningstaking i risikostyring, som påpekt av Aven (2015), er også en utfordring. Konsekvensene av beslutninger er ofte vanskelige å forutsi, og det kan være vanskelig å ta de «riktige» beslutningene - til tross for at dette kan være helt avgjørende.

3.1.2. Utfordringer og behov i praksis

I dagens samfunn vil offentlige myndigheter, bedrifter, nødetater og frivillige organisasjoner møte en rekke utfordringer knyttet til risikostyring og samfunnssikkerhet. Disse utfordringene varierer fra generelle utfordringer som berører flere institusjoner, til mer spesifikke utfordringer som kun er relevant for enkelte enheter. Denne delen av oppgaven vil derfor ta sikte på å utforske både de mer generelle og de spesifikke utfordringene, samt undersøke hvilke behov disse utfordringene medfører.

3.1.2.1. Offentlige myndigheter

Ettersom offentlige myndigheter omfatter både regjeringen, departementer, direktorater og tilsyn, kommuner og fylker, samt stortinget – er det klart at det vil være mange ulike utfordringer og behov innenfor de ulike områdene når det kommer til det praktiske arbeidet med risikostyring og samfunnssikkerhet.

Regjeringen og departementene er sentrale når det gjelder samfunnssikkerhet og beredskap. Av de viktigste oppgavene er forebygging av hendelser som truer sentrale samfunnsinstitusjoner, felles sikkerhet og den enkeltes trygghetsfølelse (Regjeringen, 2018). Regjeringen anser videre arbeidet med samfunnssikkerhet som en kjede, hvor systematisk kunnskapsutvikling ligger som grunnlag for forebyggende tiltak, og skal bidra til færre hendelser og et bedre beredskapsarbeid. Samfunnssikkerhetskjeden er kjennetegnet av mange aktører som ivaretar ulike deler av arbeidet, og stiller store krav til samordning på tvers av sektorer og forvaltningsnivå, samt godt samarbeid med private og frivillige aktører (Regjeringen, 2018). Basert på dette kan man enkelt identifisere flere mulige utfordringer, som blant annet koordinering og samhandling på tvers av de ulike aktørene, sikre kunnskapsutvikling på ulike nivåer og på tvers av ulike aktører, øvelser som både involverer alle parter og er god nok, samt god og effektiv kommunikasjon.

Når det gjelder kommuner og fylkers arbeid med samfunnssikkerhet så vil dette ha store ulikheter og dermed ulike utfordringer. Et eksempel på dette kan være geografiske forhold. Det er klart at Stavanger kommune og Tromsø kommune vil ha forskjellige utfordringer når det gjelder både topografi, klima og værforhold. Næringsliv og økonomi vil også være ulik. Eksempelvis er Stavanger ansett som energihovedstad, og er særlig godt kjent for oljen. Hvis man ser på fylket Rogaland og fylket Troms (har fra 1. januar i år blitt delt inn i Troms fylke og Finnmark fylke, etter å ha vært Troms og Finnmark fylke siden 2020, noe som naturligvis ville hatt større forskjeller og flere utfordringer og behov) vil det også her være mange forskjellige utfordringer. Blant annet så grenser Troms mot både Sverige og Russland, noe som har gitt/kan gi utfordringer knyttet til for eksempel smittekontroll (da særlig med tanke på koronapandemien), grensekontroll, og

samarbeid på tvers av landegrenser. Ifølge Direktoratet for samfunnssikkerhet og beredskap (DSB) (2023) sin kommuneundersøkelse kommer det tydelig frem at det blant annet forekommer naturhendelser oftere, og som er mer alvorlig enn før, samt at over halvparten av kommunene i Norge har blitt rammet av alvorlige naturhendelser de siste to årene. Det kommer også frem at nesten alle kommuner i Norge har en ROS-analyse, samt en overordnet beredskapsplan, men at i flere av kommunene så er disse mer enn fire og to år gamle. Flere av kommunene svarer også at de «ikke er sikker» eller «nei» til om kommunen har utarbeidet mål for arbeidet med samfunnssikkerhet og beredskap. Dette understreker det som ble poengtert tidligere, om at kontinuerlig oppdatering og utvikling av beredskapsplaner kan være en utfordring, og at det dermed er behov for å finne gode løsninger på dette.

DSB spiller også en sentral rolle i samfunnssikkerhet og risikostyring. DSB skal ha oversikt over risiko og sårbarhet i samfunnet, og skal være pådrivere i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser, samt sørge for god beredskap og effektiv ulykkes- og krisehåndtering (DSB, u.å.). DSB har blant annet ansvar for å føre tilsyn innenfor områder for farlig stoff og gods, produkter og forbrukertjenester, brannsikkerhet, elsikkerhet, kommunal beredskap og tilfluktsrom. Tilsyn benyttes også i oppfølging av samfunnssikkerhetsarbeidet lokalt, og DSB gir føringer for statsforvalterens tilsyn med kommunal beredskapsplikt, samtidig som det er statsforvalteren som velger tema og kommuner for tilsyn. Som sett over så er det et behov for bedre og tettere oppfølging, og det bør kanskje prioriteres å føre tilsyn med de kommunene som sliter mest. Riksrevisjonen, som er Stortingets største og eldste kontrollorgan, utga i 2023 en rapport om DSB sin tilsynvirksomhet på elsikkerhetsområdet - hvor de konkluderte med at DSB ikke har tilstrekkelig oversikt over elsikkerheten. De viser blant annet til at direktoratets valg av tilsynsobjekter ikke er basert på risikovurderinger, at de mangler oversikt, ikke ivaretar ansvaret sitt, at det har vært nedgang i antall tilsyn, mangel på oppfølging av el-ulykker, at de ikke kan dokumentere at tilsynsgebyrene ikke er overpriset, og at urealistisk budsjettering vrir tilsynsaktivitetene mot de mest betalingsdyktige aktørene (Riksrevisjonen, 2023). I rapporten oppgir DSB blant annet at de mangler nødvendig statistikk og

kunnskapsgrunnlag til å gjennomføre risikovurderinger, at de ikke har hatt kapasitet til å skaffe seg oversikt over tilsynsporteføljen på flere av områdene, og at de tidligere har påpekt flere utfordringer med dagens forvaltningsmodell (Riksrevisjonen, 2023). Alle disse punktene viser til store utfordringer når det gjelder DSB sin rolle som tilsynsvirksomhet, og at det er et klart behov for blant annet bedre løsninger når det gjelder valg av tilsyn, system for å holde oversikt over både hva som har blitt gjort og områder hvor de ikke strekker til, samt bedre løsninger når det gjelder budsjett og gebyrer for tilsyn.

3.1.2.2. Nødetater

Det finnes flere utfordringer når det gjelder nødetater, og blant disse er samhandling og koordinering et hovedpunkt. For å løse denne utfordringen ble nødnett grunnlagt i 2009, og fungerer som et digitalt kommunikasjonssystem (digitalt samband) for de ulike etatene og aktørene med nød- og beredskapsansvar i Norge (Nodnett, u.å.). DSB utførte i 2023 en brukerevaluering av nødnettet, som viste at nødnett bidrar til effektiv kommunikasjon internt i etater/organisasjoner og på tvers av nødetater/beredskapsaktører, samt felles situasjonsforståelse under hendelser (DSB, 2023). Til tross for at det generelt er stor tilfredshet med nødnettet, eksisterer det imidlertid flere utfordringer og behov. Blant annet så er det behov for flere øvelser. Det å benytte seg av et digitalt samband krever øvelse, repetisjon og jevnlig bruk for å opprettholde kompetansen (DSB, 2023). Brukerevalueringen viser derimot til at det er stor mangel på nettopp disse punktene når det kommer til nødnett. For at digitale verktøy, slik som nødnett, skal være nyttig eller bidra til effektiv kommunikasjon, er det essensielt at etater og aktører som benytter seg av disse verktøyene vet hvordan de skal bruke dem. Hvis en hendelse oppstår, og etatene og aktørene ikke kan å bruke nødnettet, vil det ikke være til nytte, og kan i verste fall gjøre kommunikasjonen mindre effektiv enn det den var i utgangspunktet. Det å øve sammen på tvers av ulike etater og aktører er altså viktig, slik at man vet hva man skal gjøre dersom en hendelse oppstår. Flere av nødnett-brukerne trekker likevel frem at slike øvelser er mangelfulle (DSB, 2023). På generell basis kan man argumentere for at man aldri får øvd nok, særlig på tvers av etater og

aktører, og at det kan være vanskelig å ha realistiske øvelser hvor alle parter får øvd på sine områder. Basert på dette, kan man se at det er behov for mer øving på nødnett, både innad i de ulike etatene og aktørene og på tvers av dem. Det er også behov for bedre løsninger når det gjelder å planlegge øvelser, for å sikre at øvelsene er realistiske og at alle får øvd.

3.1.2.3. Bedrifter og næringsliv

Det er mange eksempler på bedrifter og næringsliv som jobber med samfunnssikkerhet og risikostyring. I stedet for å gå inn på spesifikke bedrifter, vil heller fokuset være på generelle utfordringer og behov mange av disse står overfor i dagens samfunn. Eksempler på slike utfordringer er informasjonssikkerhet og cybertrusler, kontinuerlig oppdatering av planer og vurderinger, ekstremvær, naturkatastrofer og klimaendringer. Det vil derfor være behov for å bedre få oversikt over mulige trusler, effektivisering og automatisering når det gjelder planer og vurderinger, systemer for å samle inn data og statistikk, samt varsling av hendelser.

3.1.2.4. Frivillige organisasjoner

Frivillige aktører er også helt essensielt i arbeidet med samfunnssikkerhet og beredskap. For eksempel så er Røde Kors en beredskapsorganisasjon som fungerer som en støtteaktør for norske myndigheter (Rodekors, u.å.). Ved større hendelser kan frivillige organisasjoner som Røde Kors bistå med, for eksempel, psykososial førstehjelp og opprette evakuert- og pårørendesenter. Frivillighet har derimot også flere utfordringer, og blant de viktigste er mangel på ressurser, derunder både økonomiske og menneskelige. For å øke effektiviteten og utnytte potensialet til frivillige organisasjoner er det, for eksempel, behov for systemer som kan hjelpe til med å prioritere hvor økonomiske midler bør gå, hvilke områder som har størst behov for hjelp fra disse organisasjonene, samt hvordan timene til de frivillige bør prioriteres. Det er også behov for bedre samarbeidsplattformer og nettverksbygging. Næringsliv og bedrifter kan inneha både kunnskap og ressurser som er viktig for beredskapen, men ettersom de ofte ikke er har nød- og beredskapsansvar, og dermed ikke er med i kriser eller øvinger rundt disse, vil de være vanskelig å benytte - ettersom de ikke står på

lister/man ikke har kontaktinformasjon eller at man ikke er vant til å bruke disse, til tross for at de kan utgjøre en viktig ressurs.

3.2. Muligheter for bruk av KI innenfor risikostyring og samfunnssikkerhet

I denne delen vil fokuset være på hvordan KI kan løse flere av utfordringene og behovene som har blitt identifisert så langt. Det som presenteres her er ikke en uttømmende liste, men eksempler på hvor det finnes potensial for å løse disse utfordringene og behovene man står overfor i ulike oppgaver innenfor risikostyring og samfunnssikkerhet.

Først presenteres et forslag til hvordan man kan løse de utfordringene og behovene man så i litteraturen i del 3.1.1 med KI, basert på teori-delen om risikostyring og samfunnssikkerhet, og KI. Deretter vil fokuset være på hvilke muligheter KI kan ha for å løse de utfordringene og behovene som sett i praksis i del 3.2.1, satt sammen i Tabell 1 nedenfor. Den konkrete teknologien baserer seg på KI, maskinlæring og stordata - og er eksempler på hvor det finnes potensial for å løse oppgaver innenfor risikostyring og samfunnssikkerhet, noe som også er tredje punkt i tabellen. Til slutt ser man hvilke aktører som er relevant for disse oppgavene. Tabellen kan leses både fra venstre mot høyre, og fra høyre mot venstre.

Tabell 1 – Oversikt over hvilke muligheter teknologi kan ha for ulike oppgaver innen risikostyring og samfunnssikkerhet, samt hvilke aktører som kan ha nytte av disse.

Konkret teknologi	**Oppgaver innen risikostyring og samfunnssikkerhet**	**Relevante aktører**
Mønstergjenkjenning	Optimalisere kommunikasjonsprosesser	Regjeringen, kommuner og fylker, nødetater og frivillige organisasjoner

	Innsikt i hvilke områder som trenger forbedring og hva som har fungert godt tidligere	Regjeringen, kommuner og fylker, nødetater og frivillige organisasjoner
	Identifisere og analysere mønster i ulike kommuner og fylker med tanke på risikofaktorer og hendelser	Kommuner og fylker, DSB
	Analysere, forutsi og advare om naturhendelser	Kommuner og fylker, nødetater og frivillige organisasjoner
Prediktiv analyse og automatisert beslutningsstøtte	Analysere kriminalitet	Politiet
	Planlegging og tilpassing i tråd med fremtidige behov og utfordringer	Regjeringen, kommuner og fylker, DSB, nødetater og frivillige organisasjoner
	Evaluere sannsynlighet for ulike typer hendelser	Regjeringen, kommuner og fylker, DSB, nødetater og frivillige organisasjoner
	Ta raske og effektive beslutninger i nødsituasjoner	Regjeringen, kommuner og fylker, DSB, nødetater og frivillige organisasjoner
	Prioritering av tilsyn	DSB og brannvesenet
	Identifisere svakheter i eksisterende beredskapsplaner og implementere tiltak	Regjeringen, kommuner og fylker, nødetater, DSB og frivillige organisasjoner
	Predikere konsekvenser av hendelser	Regjeringen, kommuner og fylker, nødetater, DSB og frivillige organisasjoner

Overvåkning	Digital overvåkning for å oppdage og forebygge cyberangrep	Politiet
	Sensornettverk for å overvåke miljøforhold	Kommuner og fylker, regjeringen og DSB
	Informasjon om faktorer som påvirker samhandling mellom ulike aktører	Regjeringen, nødetater, DSB, kommuner og fylker og frivillige organisasjoner
Nevrale nettverk og veiledet læring	Identifikasjon av områder hvor ytterligere opplæring eller forbedring er nødvendig	Regjeringen, nødetater, kommuner og fylker, DSB og frivillige organisasjoner
	Identifisere hvilke tiltak som har vært mest effektiv og optimalisere fremtidige ressursallokeringer	Regjeringen, nødetater, kommuner og fylker, DSB og frivillige organisasjoner

3.2.1. Utfordringer og behov i litteraturen

3.2.1.1. ROS-analyser

I del 3.1 ble det identifisert ulike utfordringer og behov i litteraturen, basert på teori-delen i 2.1. I del 3.2 så man på hvilke muligheter KI kan ha for disse utfordringene og behovene. Her vil fokuset være på hvordan KI kan påvirke metoder for risikostyring og samfunnssikkerhet, med utgangspunkt i teori-delen 2.1.1, som tar for seg ulike former for ROS-analyser.

ROS-analyser

Hvis man først ser på ROS-analyser på generell basis, er det enkelt å identifisere hvordan KI kan påvirke slike analyser. Først og fremst innebærer ROS-analyser en systematisk identifisering og kategorisering av risiko. Som nevnt i 3.2.2.1 må enkeltindivider i stor grad identifisere områder som trenger forbedring på egenhånd, for eksempel gjennom ROS-analyser. Ved hjelp av mønstergjenkjenning kan virksomheter identifisere og analysere mønster med

tanke på risikofaktorer og hendelser, som en automatisert prosess. Basert på dette kan man tilpasse risikostyringsstrategier og beredskapsplaner til virksomheten. ROS-analyser brukes også til å identifisere faremomenter og sårbarhet for virksomheter som skal planlegge fremtidige løsninger og tiltak. Ved å benytte seg av prediktiv analyse og automatisert beslutningsstøtte kan man styrke og effektivisere virksomheters ROS-analyser ved å både planlegge og tilpasse seg i tråd med fremtidige behov og utfordringer, samt identifisere svakheter i eksisterende beredskapsplaner og implementere tiltak basert på disse. Resultatene av slike analyser kan integreres i virksomheters generelle beredskaps- og planarbeid, samt etablere risikoreduserende tiltak.

Risikomatrise

Risikomatriser baserer seg på kategoriseringer av enten sannsynlighet eller frekvens, og konsekvens, alvorlighet eller innvirkning. Dette presenteres i en tabell, slik at man enkelt kan identifisere hvilke risikoer som akseptabel og uakseptabel, og dermed hvor man må iverksette tiltak for å minimere risikoen. Prediktiv analyse kan brukes til å evaluere sannsynlighet for ulike typer hendelser, samt predikere konsekvenser av hendelser. Ved å bruke slike KI-løsninger, kan man lage risikomatriser hvor man kan fremstille tabeller for både sannsynlighet og konsekvens, med utgangspunkt i for eksempel historisk data. Ved å vite sannsynlighet for at en hendelse oppstår/hvilke hendelser som er mest sannsynlig og hvilke konsekvenser de kan ha, vil det kunne styrke arbeidet med risikostyring og samfunnssikkerhet.

Sløyfemodell

Sløyfemodellen er en annen form for risikoanalyse, som sett i 2.1.1.2. Her forsøker man på den ene siden å finne medvirkende faktorer som kan føre til den initierende hendelsen og barrierer som forsøker å forhindre den, mens på den andre siden finner man de mulige konsekvensene dersom den initierende hendelsen oppstår og barrierer som har som mål å forhindre at den medfører alvorlige konsekvenser. Formålet til risikoanalysen er å identifisere de initierende hendelsene og utvikle sannsynlighets- og konsekvensbildet (Aven, 2015).

Ved å kombinere flere av KI-teknologier kan også sløyfemodellen effektiviseres og muligens forbedres. Både mønstergjenkjenning, prediktiv analyse og automatisert beslutningsstøtte, samt nevrale nettverk og veiledet læring kan være av nytte for denne metoden. For å konkretisere hvordan sløyemodellen kan forbedres ved hjelp av de ulike teknologiene, kan man for eksempel se på risikostyring av flom.

La oss si at den initierende hendelsen er en kraftig regnperiode som fører til flom i et bestemt område. Her kan medvirkende faktorer for eksempel være ekstreme værforhold, utilstrekkelig drenering og bebyggelse i flomutsatte områder, mens barrierer for å forhindre hendelsen kan være værvarsling, forbedret dreneringssystem og regulering av byggeaktivitet i flomutsatte områder. De potensielle konsekvensene som kan oppstå er skade på eiendom og infrastruktur, og skade eller tap for mennesker, økonomi og miljø. Barrierer for å minimere at disse konsekvensene oppstår er eksempelvis gode evakueringsplaner, redningsoperasjoner og god flomberedskap. Her kan mønstergjenkjenning analysere historisk data fra flom, vær og drenering, og bruke maskinlæringsalgoritmer til å identifisere mønster i dataen, og dermed forutse og forsøke å forebygge flom i disse områdene. Prediktiv modellering kan bruke sanntidsdata fra vær, vann, innsjøer og drenering for å forutsi når og hvor det er mest sannsynlig for at flom kan skje, og dermed varsle relevante myndigheter og befolkningen. Nevrale nettverk kan analysere data fra tidligere flomhendelser, beredskapsinnsats og deres effektivitet, til å identifisere hvilke evakuerings- og redningstiltak som var mest effektive for å minimere skade og tap av liv, og dermed hjelpe til med å optimalisere beredskapsplaner.

3.2.1.2. Generelle utfordringer og behov

Som sett i del 3.1.1 er det en generell utfordring å forberede seg på de «uunngåelige krisene». Det er altså et behov for å få tilgang til verktøy som kan bidra til å minimere både krisen og dens konsekvenser. Som Laskowski & Tucci (2023) viser til så fungerer KI-systemer ved at de tar inn mengder merkede treningsdata, analyserer dataen for korrelasjoner og mønstre, samt bruker disse mønstrene til å forutse fremtidige tilstander. Ved å benytte seg av eksempelvis

mønstergjenkjenning, kan man kanskje være bedre beredt når disse krisene først oppstår.

Når det gjelder kontinuerlig oppdatering av beredskapsplaner så kan for eksempel automatisert beslutningsstøtte og prediktiv analyse bidra til å effektivisere prosessene med automatisert oppdatering, eller i det minste som et verktøy som foreslår oppdateringer av planer basert på tilgjengelige data og ny informasjon. Et eksempel på dette kan være at dersom værdata viser en økt risiko for flom, så kan systemet foreslå proaktive tiltak, slik som tilleggsprosedyrer eller ressursallokeringer for å håndtere et slikt scenario. Det at man bruker prediktiv modellering til å kontinuerlig oppdatere beredskapsplaner, sikrer at man kontinuerlig vil kunne få ny data, noe som gjør at planene vil være basert på den nyeste og mest nøyaktige informasjonen, som igjen vil sikre relevante og effektive planer til tross for endringer i forholdene.

For å løse utfordringen med manglende kunnskap om fremtidige risikoer og deres implikasjoner, kan stordata muligens brukes til å få bedre innsikt i potensielle trusler og redusere usikkerheten, og dermed styrke arbeidet med risikostyring. Maskinlæring gjør det mulig for programvareapplikasjoner å bli mer nøyaktige til å forutse utfall uten å være eksplisitt programmert til å gjøre det (Laskowski & Tucci, 2023). Integreringen av stordata og maskinlæring i risikovurderingsprosesser og beredskapsplanlegging kan derfor være en verdifull forbedring for å håndtere komplekse risikoer og usikkerheter mer effektivt. Hvis man også bruker flom-eksempelet her, men tar utgangspunkt i at tradisjonell risikostyring ikke er tilstrekkelig grunnet klimaendringer som skaper nye og mer komplekse risikoer, kan flere av eksemplene i tabell 1 være nyttig. Eksempelvis kan man bruke mønstergjenkjenning for å indikere sannsynligheten for fremtidige flomhendelser, prediktive modeller for å forutsi når og hvor en flom sannsynligvis vil oppstå, og benytte seg av overvåkning og sensorteknologi for å få informasjon i sanntid om potensielle flomrisikoer.

Til tross for at KI kan føre til utfordringer når det gjelder det komplekse samspillet mellom teknologiske, organisatoriske og menneskelig faktorer, som sett i 3.1.1, kan det også bidra til å identifisere og forutse trusler ved å analysere historiske

data og mønstre. Dette kan potensielt bidra til å fylle gapet mellom menneskelige begrensninger og komplekse risikofaktorer.

En annen utfordring som ble nevnt i del 3.1.1, var utfordringen med å ta de «riktige» beslutningene, da konsekvensene kan være vanskelig å forutsi. Automatiserte beslutningsstøttesystemer kan presentere beslutningstakere med et mer omfattende bilde av de ulike beslutningsalternativene og de potensielle konsekvensene de kan medføre, basert på analyse av data og modellering av risiko. Dette kan hjelpe til med å ta mer informerte og effektive beslutninger i kritiske situasjoner. Boletsis & Nilsson (2021) ga et godt eksempel på dette. I nødsituasjoner kan sensorteknologi analysere og tildele en risikoklasse, i dette eksempelet til hvert kjøretøy i tunnelen. Dersom risikoklassen blir ansett som for høy, vil man ved hjelp av automatisert beslutningsstøtte kunne sende forslag til handling og forklaring på dette, noe som vil hjelpe tunneloperatøren med å ta en informert beslutning for å forhindre ulykker og informere trafikantene.

Med utgangspunkt i teori om KI og eksisterende bruk av KI som har blitt presentert så langt, er det tydelig at KI kan ha et betydelig forbedringspotensial med tanke på utfordringer i samfunnssikkerhet og risikostyring. KI kan analysere store mengder data fra ulike kilder, som kan være med på å identifisere mønster og trender knyttet til ulike risikoer, som igjen kan hjelpe til med å forutse potensielle trusler og hendelser før de oppstår - noe som gir muligheten til å iverksette proaktive tiltak (Laskowski & Tucci, 2023). KI kan også brukes til å utvikle avanserte risikovurderingsverktøy som tar hensyn til komplekse sammenhenger og usikkerheter. Ved å integrere ulike datakilder og simuleringsmodeller, som sett i Riddel et al. (2019) sin case-studie, kan KI bidra til å gi bedre innsikt i potensielle konsekvenser av ulike risikoscenarioer og støtte beslutningstakere i å velge de mest hensiktsmessige risikoreduserende tiltakene. Også her kan man trekke frem eksempelet fra Boletsis & Nilsson (2021) hvor beslutningsstøttesystemer kunne gi tunneloperatøren forslag til handling, som videre ga muligheten til å ta en informert beslutning. Ved å benytte seg av maskinlæring kan man også automatisere mange av de rutinemessige oppgavene som er knyttet til risikostyring, som for eksempel datainnsamling, analyse av

rapporter og varsling om avvik (Laskowski & Tucci, 2023). Ved å benytte slike automatiserte prosesser vil det frigjøre tid og ressurser som kan brukes til andre oppgaver i stedet. Man kan også benytte KI til å kontinuerlig overvåke og analysere endringer i risikobildet, og dermed tilpasse risikostyringsstrategiene samtidig. Ettersom KI kan lære av tidligere erfaringer og tilpasse seg nye utfordringer, vil det bidra til å øke robustheten og effektiviteten i risikostyringssystemer (Laskowski & Tucci, 2023). KI og maskinlæring kan potensielt også være viktige verktøy i å forutse og håndtere kriser mer effektivt, og ved å integrere disse teknologiene i risiko- og samfunnssikkerhetsstrategier, kan man forbedre evnen til å identifisere og reagere på risikoer i sanntid, samt forutse og minimere konsekvensene av uforutsette hendelser.

3.2.2. Utfordringer og behov i praksis

3.2.2.1. Mønstergjenkjenning

Mønstergjenkjenning kan brukes til å løse oppgaver innen risikostyring og samfunnssikkerhet på flere ulike områder. Her vil fokuset være på hvordan mønstergjenkjenning kan optimalisere kommunikasjonsprosesser, gi innsikt i hvilke områder som trenger forbedring og hva som har fungert godt tidligere, identifisere og analysere mønster i ulike kommuner og fylker med tanke på risikofaktorer og hendelser, og analysere, forutsi og advare om naturkatastrofer.

Optimalisere kommunikasjonsprosesser

Mønstergjenkjenning kan brukes til å identifisere mønster i kommunikasjonen mellom aktører, noe som kan gi innsikt i hvordan informasjon deles og behandles, og dermed optimalisere kommunikasjonsprosessene. Alle aktørene er avhengig av effektiv kommunikasjon, særlig under hendelser. Som sett så bruker de ulike beredskapsaktørene nødnett for å kommunisere i dag. Det er derimot flere utfordringer ved nødnett, noe mønstergjenkjenning kanskje kunne løst eller vært med på å forbedre.

Innsikt i hvilke områder som trenger forbedring og hva som har fungert godt tidligere

Ved å benytte seg av mønstergjenkjenning kan man identifisere hvilke områder som trenger forbedring og hva som har fungert godt tidligere. I dag må enkeltindivider identifisere områder som trenger forbedring selv, blant annet gjennom undersøkelser, risikoanalyser og vurderinger. Dersom man tar i bruk mønstergjenkjenning, vil man kunne få innsikt i forbedringspotensial basert på tidligere hendelser eller områder hvor det tidligere har vært utfordringer. Det å vite hva som har fungert godt tidligere er også et anerkjent problem, da man ikke nødvendigvis vet hva det er som fungerte av alt man har gjort. Ved å bruke mønstergjenkjenning kan man kanskje få hjelp til å forstå spesifikt hva som fungerer eller ikke.

Dette vil også være noe alle aktørene kan ta nytte av. Eksempelvis så vil en kommune benytte seg av ROS-analyser for å finne hvilke risikoer man står overfor og må planlegge for, mens hvis man hadde brukt mønstergjenkjenning ville det kanskje identifisert disse risikoene og pekt på hvilke områder som trenger forbedring - litt som en automatisert prosess, basert på foreliggende data/tidligere mønster om risikoer og sårbarheter. Nødetater, som for eksempel brannvesenet, kunne også brukt mønstergjenkjenning til å se hvilke deler av deres arbeid som har fungert godt, og hva som trenger å forbedres, slik at man kan forbedre effektiviteten og sikkerheten, basert på mønstergjenkjenning av tidligere hendelser. Det finnes flere eksempler på hvordan brannvesenet kan bruke mønstergjenkjenning i sitt arbeid. Et eksempel kan være å bruke mønstergjenkjenning i sitt forebyggende arbeid, ved å for eksempel se på hva slags områder og bygningstyper som oftest blir rammet av brann, og hva slags forebyggende tiltak som har vært mest effektive. Et annet eksempel kan være å bruke mønstergjenkjenning når det gjelder responstid, ved å identifisere mønster i responstid, som kan være avhengig av ulike faktorer slik som tid på døgnet, værforhold og trafikkmønster.

Identifisere og analysere mønster i ulike kommuner og fylker med tanke på risikofaktorer og hendelser

Mønstergjenkjenning kan også brukes til å identifisere og analysere mønster i ulike kommuner med tanke på risikofaktorer og hendelser. Dette kan blant annet

hjelpe til med å tilpasse risikostyringsstrategier og beredskapsplaner til lokale behov og utfordringer. Som sett tidligere så vil ulike kommuner og fylker ha store forskjeller og dermed også ulike utfordringer og behov, og mønstergjenkjenning kan dermed være helt essensielt i kommuner og fylkers arbeid med blant annet identifisering av risikoer og planlegging rettet mot disse risikoene. Dette vil gjøre at de er bedre beredt dersom en hendelse skulle oppstå. Ettersom DSB skal sørge for god beredskap og har veiledere for kommuners ROS-arbeid så vil det kanskje også være relevant for dem.

Analysere, forutsi og advare om naturhendelser

Som sett tidligere så kom det frem i DSB (2023) sin kommuneundersøkelse at det forekommer naturhendelser oftere og som er mer alvorlig enn før, samt at over halvparten av kommunene i Norge har blitt rammet av alvorlige naturhendelser de siste to årene. Ved bruk av mønstergjenkjenning kan man analysere historisk data og andre faktorer knyttet til naturhendelser, slik som sannsynlighet, hyppighet og årsaker, noe som igjen kan brukes til å utvikle modeller for å forutsi og advare om mulige naturhendelser. Dette kan være verdifullt for kommuners og fylkers arbeid med risikostyring og samfunnssikkerhet. Ved å bruke mønstergjenkjenning kan man være bedre forberedt på disse naturhendelsene, ved å tidlig planlegge for de og respondere på en annen måte enn man kanskje ville gjort dersom man ikke var godt nok forberedt. Det kan også være relevant for nødetater og frivillige organisasjoner, da disse ofte bistår i slike hendelser. De får da mulighet til å skaffe nødvendig mannskap og ressurser, og se hvor behovet for disse er størst. Dette vil ikke bare gjøre at man er bedre forberedt, men også effektivisere flere prosesser, som kanskje kan gjøre at færre liv går tapt og at skadepotensialet blir mindre.

3.2.2.2. Prediktiv analyse og automatisert beslutningsstøtte

Prediktiv analyse og automatisert beslutningsstøtte er også viktig for flere oppgaver innen risikostyring og samfunnssikkerhet. Her er fokuset på å analysere kriminalitet, planlegging og tilpassing i tråd med fremtidige behov og utfordringer, evaluere sannsynlighet for ulike typer hendelser, prioritering av tilsyn, identifisere

svakheter i eksisterende beredskapsplaner og implementere tiltak, og predikere konsekvenser av hendelser.

Analysere kriminalitet

Prediktiv analyse kan brukes til å analysere historisk data om blant annet kriminalitetsmønster, noe som kan brukes til å optimalisere ressurser og prioritere forebyggende tiltak for å redusere kriminalitet og dermed øke sikkerheten. Dette vil ikke bare være nyttig for politiet, men også samfunnet på generell basis.

Ettersom det i størst grad er politiet som har ansvar for «vanlig» kriminalitet, vil det også gi størst nytte for dem. Politiet har ofte begrensede ressurser og det kan derfor være vanskelig å prioritere hvor man skal sette disse eller hvilke områder som krever mest. Prediktiv analyse kan derfor være av stor betydning for å optimalisere disse ressursene. En av politiets hovedoppgaver er også kriminalitetsforebygging, og prediktiv analyse kan gjøre dette arbeidet enklere og mer effektivt ved å prioritere de forebyggende tiltakene som er av størst betydning, og dermed redusere kriminaliteten og øke sikkerheten.

Planlegging og tilpassing i tråd med fremtidige behov og utfordringer

Ved å bruke prediktiv analyse kan man potensielt forutsi fremtidige hendelser, noe som er både fordelaktig og veldig nyttig innenfor mange områder, derav særlig planlegging og forebygging av uønskede hendelser. Dette er også noe de fleste aktører kan dra nytte av.

Kommuner og fylker vil kunne bruke prediktiv analyse i arbeidet med risikostyring og samfunnssikkerhet. Hvis man vet hva slags hendelser som potensielt kan oppstå, vil man kunne implementere disse i planer, som for eksempel å implementere forebyggende tiltak for å forsøke å forhindre at hendelser oppstår, eller vite hvordan man best kan respondere på dem, og dermed minimere konsekvensene. Det å forutsi fremtidige hendelser gjør også at man kan gjennomføre øvelser rettet spesifikt mot disse hendelsene, noe som igjen gjør at de ulike beredskapsaktørene er bedre beredt og kan respondere mer effektivt når hendelsene inntreffer. Det er derimot ikke kun kommuner og fylker som kan ha nytte av prediktiv analyse. Regjeringen kan for eksempel bruke prediktiv analyse

når det gjelder å forutsi fremtidige hendelser for å vite hvor de bør prioritere økonomiske midler og ressurser. Dette vil også være nyttig for nødetatene, da de kan bruke de spesifikke planene og øvelsene i sitt forebyggende arbeid, samt hvor de bør prioritere sine ressurser. Dette vil også være viktig for frivillige organisasjoner, slik at de også er forberedt på å hjelpe til dersom det kreves. Ettersom DSB har det overordnede ansvaret for beredskap, risiko og sårbarhet i samfunnet, vil det å kunne planlegge og tilpasse i tråd med fremtidige behov og utfordringer, også være en viktig ressurs for dem.

Evaluere sannsynlighet for ulike typer hendelser

Prediktiv analyse og automatisert beslutningsstøtte kan brukes til å evaluere sannsynligheten for ulike typer hendelser basert på historisk data, og kan dermed identifisere hvilke scenarioer som er mest sannsynlig, samt hvilke hendelser man bør planlegge for i beredskapsplanleggingen. Dette punktet vil generelt sett ha de samme funksjonene, og være til hjelp for de samme oppgavene som sett over. Det å vite sannsynligheten for ulike typer hendelser vil derimot gjøre at man vet hvilke av de fremtidige hendelsene som har størst sjanse for å inntreffe, og at man dermed kan prioritere arbeidet mot de hendelsene som har størst sannsynlighet. Kanskje man kunne brukt denne evalueringen av sannsynlighet til å se på sannsynlighet for ulike utfall av hendelsene også, eller sannsynlighet for at ulike tiltak fungerer eller ikke fungerer – noe som igjen vil gjøre at man vet hva slags respons som vil være mest effektiv og hensiktsmessig.

Ta raske og effektive beslutninger i kritiske situasjoner

Som sett tidligere, så kan automatisert beslutningsstøtte hjelpe beslutningstakere med å håndtere informasjonsstrømmen raskere og mer effektivt – noe som kan være spesielt viktig under kritiske situasjoner. Ettersom man ofte er utsatt for tidspress i nødssituasjoner, vil man måtte ta raske avgjørelser, noe som understreker viktigheten av å ha tilgjengelig beslutningsstøtte.

Dette vil være nyttig for alle beredskapsaktører. Eksempler på dette er regjeringens håndtering av covid-19, hvor de flere ganger måtte ta raske beslutninger, uten å nødvendigvis vite hva som var det beste alternativet. Når

nødetatene må ta raske avgjørelser, for eksempel ved brann eller trafikkulykker, vil automatisert beslutningsstøtte kunne gi de forslag til hvordan de bør respondere, noe som vil gi de muligheten til å raskt ta en informert beslutning.

Prioritering av tilsyn

Som sett tidligere så er DSB ansvarlig for å føre tilsyn innenfor flere områder. Disse tilsynene skal i utgangspunktet prioriteres etter risiko og vesentlighet, men som Riksrevisjonen (2023) viste til, så har disse tilsynene blitt prioritert på feil grunnlag. Ved å benytte seg av prediktiv modellering vil man kunne få nøytrale prioriteringer av tilsyn, som baserer seg på de faktorene som man faktisk skal basere tilsynene på, slik som risiko og vesentlighet. Dette vil bidra til at man prioriterer og fører tilsyn på de områdene det er mest nødvendig, i stedet for der det for eksempel er mest økonomisk lønnsomt. Å bruke prediktiv modellering til å prioritere tilsyn vil også kunne være nyttig for brannvesenet.

Identifisere svakheter i eksisterende beredskapsplaner og implementere tiltak

Prediktiv modellering kan brukes til å analysere potensielle utfordringer knyttet til for eksempel risiko og sårbarhet, og dermed identifisere svakheter i eksisterende planer. Dette gjør at man kan få informasjon om hvilke deler av de eksisterende planene som trenger endring, og man kan dermed implementere tiltak med sikte på å forbedre disse områdene, som igjen vil styrke arbeidet med beredskapsplanlegging.

Det har tidligere blitt poengtert at kontinuerlig oppdatering og utvikling av beredskapsplaner kan være en utfordring. Prediktiv modellering kan derfor kanskje delvis være med på å dekke dette behovet. Dersom man også benytter seg av automatisert beslutningsstøtte i tillegg, vil dette kunne gjøre arbeidet enda enklere og mer effektivt, ved at man får forslag til hvilke tiltak og endringer man kan gjøre. Dette vil være nyttig for alle aktører som jobber med beredskapsplaner. Hvis man tar kommuner og fylker som eksempel, kan disse bruke prediktiv modellering til å analysere historisk data, slik som tidligere naturkatastrofer, for å identifisere områder som har høy risiko. Deretter kan de identifisere svakheter, slik som områder som mangler tilstrekkelig infrastruktur for

å håndtere slike hendelser. Ved hjelp av automatisert beslutningsstøtte kan de få forslag til hvordan de kan forbedre denne infrastrukturen.

Predikere konsekvenser av hendelser

Prediktiv modellering kan også brukes til å predikere konsekvenser av hendelser. Det kan gi et innblikk i hvilke konsekvenser ulike hendelser vil ha, noe som gir oss mulighet til å implementere tiltak for å minimere disse konsekvensene. Dersom man kan planlegge for hvilke tiltak man bør gjøre og hvilke ressurser man bør bruke når det gjelder ulike hendelser, vil dette gjøre arbeidet med risikostyring og samfunnssikkerhet, og derav særlig beredskapsplanlegging og krisehåndtering, enklere, bedre og mer effektivt. Alle aktører som arbeider med beredskapsplaner og krisehåndtering kan dra nytte av denne tilnærmingen for å være bedre forberedt på potensielle hendelser. Et eksempel på å predikere konsekvenser av hendelser kan demonstreres med utgangspunkt i naturkatastrofer, og derunder jordskjelv. Her vil man kunne bruke prediktiv modellering til å blant annet analysere historiske jordskjelv for å forutsi utsatte områder og styrken på skjelvene. Ut ifra dette kan man predikere konsekvensene av en slik hendelse, som kan bestå av å vurdere potensielle skader på bygninger, infrastruktur og potensielle tap av liv i de utsatte områdene.

3.2.2.3. Overvåkning

Overvåkning kan brukes til å løse oppgaver innen risikostyring og samfunnssikkerhet på flere ulike områder. Her vil fokuset være på hvordan overvåkning kan benyttes til digital overvåkning for å oppdage og forebygge cyberangrep, bruke sensornettverk for å overvåke miljøforhold, og gi informasjon om faktorer som påvirker samhandling mellom ulike aktører.

Digital overvåkning for å oppdage og forebygge cyberangrep

Digital overvåkning kan brukes til å oppdage og forebygge cyberangrep og digitale sikkerhetstrusler. Man har tidligere sett hvor alvorlige utfall cyberangrep kan ha, slik som cyberangrepet av Helse Sør-Øst i 2018, hvor de kunne fått adgang til å stjele eller kompromittere pasientopplysninger. Dagens samfunn blir bare mer og mer digitalisert, og mange tar i bruk teknologiske løsninger så langt

det er mulig. Dette gjenspeiler viktigheten av å ha gode sikkerhetssystemer og være beredt på digitale angrep.

Ettersom de aller fleste aktører benytter seg av digitale løsninger i mindre eller større grad, vil også alle aktørene være utsatt for slike angrep og bør derfor være beredt på dette. Dersom ulike beredskapsaktører hadde blitt utsatt for spionasje, eller fått data stjålet, endret eller påvirket, kunne det i verste fall fått fatale konsekvenser. Digital overvåkning er dermed noe alle aktører bør ta sikte for i sitt arbeid med risikostyring og samfunnssikkerhet. Det er nok likevel kanskje politiet som i størst grad jobber med digital overvåkning for å oppdage og forebygge slike cyberangrep.

Sensornettverk for å overvåke miljøforhold

Sensornettverk for å overvåke miljøforhold kan bidra til å identifisere potensielle risikoer, med tanke på miljøforhold slik som luftkvalitet, værforhold, forurensning og naturkatastrofer. Ved å benytte sensornettverk vil man kunne ta nødvendige tiltak for å redusere skader.

Dette er mest aktuelt for de aktørene som jobber med miljø og ressursforvaltning, og planer rundt dette - slik som regjeringen, kommuner og fylker, og DSB. Dersom man kan identifisere risikoer knyttet til miljøforhold som for eksempel forurensning, kan man iverksette tiltak for å begrense eller minimere de ulike formene for forurensning. Det å kunne overvåke potensielle naturkatastrofer vil også være både veldig viktig og nyttig i arbeidet med risikostyring og samfunnssikkerhet. Ovenfor så man at man kunne benytte prediktiv analyse og automatisert beslutningsstøtte til å for eksempel forutsi fremtidige hendelser og evaluere sannsynligheten av hendelsene. Dersom man også kan overvåke disse hendelsene, vil man i større grad vite når en hendelsene vil inntreffe, og kanskje gjøre tiltak underveis basert på dataen fra overvåkningen, slik at det er mindre sannsynlighet for at hendelsen inntreffer - eller i det minste minimere konsekvensene. Hvis man tar utgangspunkt i jordskjelv-eksempelet overfor, kunne man overvåket de utsatte områdene, og kanskje evakuert menneskene i disse områdene før jordskjelvet inntreffer.

Informasjon om faktorer som påvirker samhandling mellom ulike aktører

Overvåking kan også gi informasjon i sanntid om situasjoner og statusen til ulike faktorer som påvirker samhandling mellom aktører. Dette kan bidra til å oppdage endringer og behov raskere, slik at aktørene har mulighet til å tilpasse seg og samarbeide mer effektivt.

I DSB (2023) sin brukerevaluering av nødnettet ble det trukket frem av mange brukere at det er mange områder hvor det er dårlig dekning. Dersom ikke alle aktørene kan benytte seg av nødnett kan dette være en stor utfordring, og gjøre samarbeidet vanskeligere. Dersom man gjennom overvåkning kan få informasjon i sanntid om at spesifikke aktører ikke får kommunikasjonen som deles på nødnettet, vil de andre aktørene kunne tilpasse seg dette og finne andre løsninger for å sikre effektiv kommunikasjon, og at alle får med seg viktige beskjeder.

3.2.2.4. Nevrale nettverk og veiledet læring

Nevrale nettverk og veiledet læring er også nyttig når det kommer til å løse oppgaver innen risikostyring og samfunnssikkerhet på flere ulike områder. Det kan blant annet være nyttig for å identifisere komplekse sammenhenger mellom ulike faktorer som påvirker risiko og sikkerhet, for å identifisere effektive tiltak som har blitt gjort tidligere og dermed optimalisere og justere ressursallokeringer, analysere datasett effektivt, og automatisere oppgaver. Her vil fokuset være på identifikasjon av områder hvor ytterlige opplæring eller forbedring er nødvendig, og identifisere hvilke tiltak som har vært mest effektiv og optimalisere fremtidige ressursallokeringer.

Identifikasjon av områder hvor ytterlige opplæring eller forbedring er nødvendig

Nevrale nettverk og veiledet læring kan identifisere områder hvor ytterlige opplæring eller forbedring er nødvendig, og dermed bidra til å tilpasse, for eksempel, fremtidige øvelser for å adressere spesifikke læringsbehov og mål. Som nevnt tidligere kan man argumentere for at man aldri får øvd nok, og at det å gjennomføre øvelser som sikrer læring for alle involverte parter kan være utfordrende. Ved å få tilpassede øvelser for å adressere spesifikke læringsbehov

og mål kan man kanskje i større grad sikre læring, og fokusere på de områdene som trenger det mest. Dette vil være relevant for alle aktører som øver og responderer på hendelser. Særlig nødetater og frivillige organisasjoner vil kunne ta nytte av dette. Det kan kanskje også brukes som en indikasjon for regjeringen, DSB, og kommuner og fylker, hvor man trenger å prioritere midler og ressurser.

Identifisere hvilke tiltak som har vært mest effektiv og optimalisere fremtidige ressursallokeringer

Nevrale nettverk og veiledet læring kan analysere og lære av data om tidligere innsats og resultater, eksempelvis fra frivillige organisasjoner, noe som kan bidra til å identifisere hvilke tiltak som har vært mest effektiv, og lære av disse erfaringene for å optimalisere fremtidige ressursallokeringer.

Ved å få en oversikt over hvilke tiltak som har vært mest effektiv og optimalisere fremtidige ressursallokeringer, kan de ulike aktørene prioritere tiltak og ressurser enklere og mer effektivt, der det er mest nødvendig. Dette vil være til stor hjelp for frivillige organisasjoner da de ofte har dårlig økonomi og er basert på at frivillige bidrar. Ved å ha oversikt vil de kunne sikre at økonomiske midler og menneskelige ressurser prioriteres der det er viktigst. Det vil også være like viktig for regjeringen, nødetater, DSB, og kommuner og fylker.

4. Diskusjon

Dette kapittelet vil se på hvordan aktører kan ta KI-løsninger videre i praksis, utfordringer med KI, etiske og juridiske dilemmaer med KI, og begrensninger for oppgaven.

Her vil fokuset være på hvordan aktørene kan ta funnene og implementere dem i praksis, ved hjelp av ni-steg for implementering av KI i virksomheter. Det tredje punktet tar for seg ulike utfordringer med KI, slik som personvern, beslutninger, skadelig påvirkning, høyt strømforbruk og datakvalitet. Etter dette vil fokuset være på ulike problemstillinger knyttet til bruken av KI, slik som personvern og juridiske problemstillinger. Til slutt vil begrensninger for oppgaven presenteres, hvor fokuset vil være på hvordan disse begrensningene kan ha påvirket oppgaven og forslag til videre forskning basert på dette.

4.1. Hvordan kan aktørene ta det videre i praksis?

Så langt har fokuset vært på utfordringer og behov, og de mulighetene KI har for å dekke disse - men ikke hvordan man faktisk kan implementere KI i praksis. Derfor vil denne delen av diskusjonen ta sikte på hvordan aktørene som har blitt nevnt så langt kan ta i bruk forslagene som har blitt presentert.

Bray (u.å.) foreslår ni enkle skritt for å effektivt implementere KI i virksomheter. Steg en er å identifisere områder i virksomheten som kan ha nytte av å implementere KI, andre steg er å evaluere ulike KI løsninger og tilbydere, tredje steg er å lage en plan for implementering, fjerde steg er å vurdere datakvalitet og tilgjengelighet for implementering av KI, femte steg er å bygge et sterkt lag til å støtte og administrere implementeringen av KI, sjette steg er å implementere et pilotprosjekt for å teste effektiviteten av KI i virksomheten, syvende steg er å etablere klare retningslinjer og protokoller for å bruke KI, åttende steg er å lage en plan for å måle suksessen og innvirkningen som implementering av KI vil ha for virksomhetens mål, og det niende steget er å investere i kontinuerlig læring og utvikling for å holde følge med KI sine fremskritt.

Steg 1: Identifisere områder i virksomheten som kan ha nytte av KI-implementering

En naturlig start vil være å identifisere hvilke områder i virksomheten som kan ha nytte av å implementere KI. Eksempler på dette kan være oppgaver som er repeterende eller tidkrevende (Bray, u.å.).

I Tabell 1 så man eksempler på ulike oppgaver innen risikostyring og samfunnssikkerhet som kunne ha nytte av konkrete teknologier. For at aktører skal kunne identifisere områder/oppgaver i virksomheten som kan ha nytte av KI, vil en slik tabell også kunne være god start for dem. Først vil det være naturlig å kartlegge hvilke arbeidsprosesser de driver med den dag i dag, som er knyttet til risiko og sikkerhet. Deretter se på hvilke av disse som, for eksempel, er tidkrevende, repeterende, dyre, utfordrende og/eller manglende - oppgaver som trenger, eller hvor det vil være nyttig, med forbedringer. Når man har identifisert disse arbeidsprosessene, kan se på konkrete teknologier innenfor KI for å finne ut av hvilken konkret teknologi som kan ha for eksempel de beste, mest effektive og/eller mest lønnsomme løsningene. Dersom aktørene føler at det er bedre å starte med konkret teknologi og deretter se på arbeidsprosesser, så kan tabellen, som nevnt tidligere, leses begge veier.

Steg 2: Evaluere ulike KI-løsninger og tilbydere

Det finnes ulike KI-løsninger og tilbydere. Derfor er det viktig å finne løsninger som er best egnet for sin virksomhet, og tilbydere som har erfaring innenfor deres felt. Andre faktorer som er viktig å se på er budsjett, fleksibilitet og tilpasning av KI-løsningene, tilbyderne sine sikkerhetstiltak og overholdelse av regelverk (Bray, u.å.).

Som nevnt ovenfor, vil det være naturlig å se på hvilken konkret teknologi som presenterer blant annet de beste, mest effektive og/eller lønnsomme løsningene, etter at man har kartlagt virksomhetens arbeidsprosesser innen risiko og sikkerhet. Hvilken KI-løsning som er best, vil være avhengig av aktørenes og virksomhetenes oppgaver, utfordringer, behov og mangler. Som sett i Tabell 1 så vil stort sett alle aktører dra nytte av de konkrete teknologiene i større eller

mindre grad, og det å velge riktig løsning kan derfor være vanskelig. Ved å for eksempel lage en egen tabell eller en liste, og skrive ned de ulike arbeidsprosessene/oppgavene innenfor risiko og sikkerhet, vil man kunne se hvordan hver enkelt oppgave kan ha nytte av de ulike konkrete teknologiene. Ofte vil en spesifikk oppgave kunne løses med hjelp av flere teknologier. Når dette er tilfellet må aktørene/virksomhetene tenke over hvilken av de ulike løsningene som vil være mest nyttig for deres formål, eller se hvilken konkret teknologi som skiller seg ut/stiller sterkest i helheten av tabellen. Hvis for eksempel prediktiv analyse og automatisert beslutningsstøtte kan være nyttig for nesten alle oppgavene, mens mønstergjenkjenning bare er nyttig for tre av oppgavene vil det kanskje være ganske åpenbart hvilken løsning som er best egnet for deres formål. Dersom disse tre oppgavene derimot er de aller viktigste i virksomheten, vil det derimot kanskje være best å velge mønstergjenkjenning. Det kan også være nyttig å se på om de ulike teknologiene kan ha noen spesielle svakheter som man må ta i betraktning.

Videre vil det være ulike tilbydere for disse KI-løsningene. Som Bray (u.å.) sier, så er det mange faktorer man må se på når man skal velge tilbyder. Aktørene må derfor bestemme seg for hvilke faktorer som er viktigst for dem, enten det er tilbydere med erfaring, som er mest lønnsomme, har mest fleksible og tilpasningsdyktige KI-løsninger, eller sikkerhetstiltak og overholdelse av regelverk. Til tross for at det mest ideelle hadde vært og funnet en tilbyder som oppfyller alle disse faktorene, vil det nok realistisk sett ikke være så enkelt å finne det. Ettersom aktørene i dette tilfellet jobber med risiko og sikkerhet i mindre eller større grad, så vil eller bør, sikkerhetstiltak og overholdelse av regelverk være en viktig faktor. For virksomheter som selger produkter vil de måtte overveie forholdet mellom produksjon og sikkerhet. Ulike aktører har ofte ulike verdier som er svært viktig innad i organisasjonen, og det å finne tilbydere som deler disse verdiene bør være i fokus.

Steg 3: Lage en plan for implementering

Dersom man skal implementere KI i virksomheten, må man lage en plan for hvordan dette skal gjøres. Eksempelvis må man sette realistiske mål og tidslinjer,

delegere ansvar og roller, og identifisere potensielle risikoer og utfordringer som man må ta sikte for (Bray, u.å.).

Det å ha en plan for hvordan man skal implementere KI i virksomheten er helt essensielt. Det å sette realistiske mål og tidslinjer er viktig for å forsikre seg om at man har den tiden man trenger, for å unngå at man utelater viktige detaljer eller at det oppstår feil under implementeringen - da dette kan føre til kritiske og tidkrevende problemer senere. Når man skal delegere ansvar og roller er det viktig å sikre at de ansatte innehar den nødvendige kunnskapen som man trenger for å implementere slike løsninger. Aktørene må også identifisere potensielle risikoer og utfordringer, slik som for eksempel datasikkerhet og personvern.

Steg 4: Vurdere datakvalitet og tilgjengelighet

Kvaliteten og kvantiteten av data vil være av stor betydning for hvorvidt KI-systemer fungerer godt. Virksomheter bør derfor finne ut om de har nok data tilgjengelig for å trene KI-modellene (dersom de ikke har det må de lage en plan for å innhente mer data eller forbedre den eksisterende dataen), sikre at dataen er nøyaktig og konsekvent, og jobbe med IT- eller maskinlæringseksperter for å identifisere potensielle problemer med dataen og løsningene, samt å maksimere effektiviteten av KI-løsningen og oppnå bedre resultater (Bray, u.å.).

Aktørene må altså her tenke over hva slags data de har tilgjengelig, hvilken data de kan skaffe og hvor de eventuelt kan få tak i denne dataen dersom det trengs, samt om dataen er god nok. Dette er viktig for å sikre at systemene er egnet til å gjøre det de skal/utføre spesifikke oppgaver.

Steg 5: Bygge et sterkt lag til å støtte og administrere implementeringen

Når man ønsker å implementere KI i virksomheten så må man ansette IT-eksperter, ingeniører og prosjektledere for å overse prosessen, og trene de ansatte man har il hvordan man kan bruke KI-løsninger og løse problemer (Bray, u.å.).

Som sett i steg 3 så bør man lage en plan for å implementere KI-løsninger, basert på de ressursene man har i virksomheten. Man trenger derimot også å ansette

personer med kunnskap om og erfaring med KI, som kan støtte og administrere implementeringen. Dette innebærer å overse at alt går som det skal, og sikre at de ansatte får den nødvendige kunnskapen til å både bruke disse nye løsningene og vite hvordan de kan løse problemer som kan oppstå underveis.

Steg 6: Implementere et pilotprosjekt

Før man implementerer KI helt i virksomheten, bør man teste og evaluere hvordan KI vil påvirke virksomheten og eventuelle problemer som kan oppstå. Ved å ha et pilotprosjekt vil man kunne samle tilbakemelding fra både kunder og kunder for å sikre at KI-løsninger møter deres behov og forventninger (Bray, u.å.).

Til tross for at KI-løsninger kan være av stor nytte innenfor mange områder og oppgaver, kan nye systemer medføre nye og andre problemer enn det man er vant til. Å implementere et pilotprosjekt kan være med på å avdekke flere slike utfordringer. En utfordring kan være overgangen til et nytt system, noe som kan gjøre at oppgavene blant annet blir vanskeligere og mer tidkrevende, i stedet for enklere og effektive. En annen utfordring kan være at systemene ikke fungerer ordentlig, for eksempel fordi datakvaliteten ikke er god nok. Dersom løsningene ikke fungerer som tenkt for å løse de ulike arbeidsprosessene kan dette også være en utfordring. Når virksomheter benytter stadig flere teknologiske løsninger, vil det også oppstå flere utfordringer rundt personvern og sikkerhet. Selv om KI-løsninger fungerer godt i et pilotprosjekt kan det også oppstå utfordringer når løsningen skal skaleres/implementeres i hele virksomheten, og dette er noe man bør ta sikte for, før man tar steget videre.

Et pilotprosjekt kan imidlertid også identifisere nye muligheter og gode løsninger. Selv om overgangen til et nytt system kan være vanskelig og tidskrevende, er det viktig å huske at dette kan løses ved hjelp av god opplæring og kontinuerlig bruk av disse systemene, noe som gjør det lønnsomt i lengden/dersom man implementerer løsningene i virksomheten. Det at systemene ikke fungerer ordentlig eller at datakvaliteten ikke er god nok er en ofte en naturlig del av implementeringen av nye systemer, og noe man kan løse langsiktig, for eksempel ved å trene systemene og innhente god nok data. Det å implementere KI-

løsninger i virksomheter kan gjøre arbeidsprosessene mer effektiv og lønnsom på mange måter. Et eksempel på dette er at prosesser i stor grad kan bli automatisert, noe som gjør at man slipper repetert og tidkrevende arbeid, og dermed har mer tid til andre oppgaver. KI har også flere løsninger som mennesker ikke greier å gjøre på egenhånd, som for eksempel å bruke store mengder historisk data til å forutse hendelser.

Steg 7: Etablere klare retningslinjer og protokoller

Dersom man skal implementere KI i virksomheten, må man etablere klare retningslinjer og protokoller. Dette er for å sikre hvordan beslutninger blir gjort og evaluert, og for å etablere datasikkerhet og personvernsprotokoller - og dette må kontinuerlig gjennomgås og oppdateres (Bray, u.å.).

Når virksomheter skal ta i bruk nye løsninger, trenger de naturligvis også retningslinjer og protokoller for hvordan disse løsningene skal brukes, og hvordan de *ikke* skal brukes. For eksempel så vil KI-løsninger kunne gi forslag til beslutninger, og det å danne et grunnlag for hvordan man tar visse beslutninger eller evaluerer disse er essensielt for å skape en felles forståelse og «oppskrift» på hvordan man skal forholde seg til KI. Som nevnt flere ganger tidligere, så vil også det å benytte seg av nye teknologiske løsninger presentere datasikkerhet- og personvernsproblemer - og dette er noe man må ha gode retningslinjer og protokoller for.

Steg 8: Lage en plan for å måle suksess og innvirkning

Ved å lage en plan for å måle suksess og innvirkning vil man få mest mulig ut av investeringen av KI. Man bør etablere beregninger og indikatorer for å måle effektiviteten av KI, og dette inkluderer å måle ulike faktorer slik som kostnadsbesparelser, økt effektivitet, forbedret kundetilfredshet og samlet forretningsvekst (Bray, u.å.).

Det å ha en plan for å måle suksess og innvirkning i virksomheter, vil samlet sett maksimere verdien av investeringene, sikre kontinuerlig forbedring, opprettholde høy kvalitet og sikkerhet, og oppnå både operasjonelle og strategiske mål.

Steg 9: Investere i kontinuerlig læring og utvikling

Virksomhetene må gi de ansatte trening og opplæring, og følge med på nye utviklinger innenfor KI. Ved å prioritere læring og utvikling vil virksomheten blant annet kunne forbli konkurransedyktig og få en kultur for innovasjon og samarbeid (Bayer, u.å.).

Det er altså ikke nok med å bare investere i KI-løsninger. Virksomheter må også investere i kontinuerlig læring og utvikling, både for at ansatte får den treningen og kunnskapen de trenger, og for å sikre at man holder følge med nye utviklinger og trender. Det gjøres stadig nye fremskritt i teknologi, og KI-løsninger vil derfor måtte oppdateres kontinuerlig dersom man ønsker de beste og nyeste utgavene, og ikke bli hengende etter andre virksomheter.

4.2. Utfordringer med KI

Selv om KI kan være med på å løse utfordringer og behov for ulike aktører, vil disse teknologiene også medføre andre utfordringer. Øye & Normann (2021) trekker frem utfordringer med personvern, beslutninger, skadelig påvirkning og strømforbruk.

Til tross for at Norge er langt fremme når det gjelder digitalisering, så er mangel på personvern en utfordring når man skal ta i bruk KI. For eksempel så kan det være mulig å finne ut hvem som har vært med å lage datasettet til en algoritme, uten at man har tilgang til data - selv om dette i utgangspunktet er informasjon som skulle vært fortrolig (Øye & Normann, 2021).

Videre så argumenterer de for at det kan være vanskelig å forklare beslutninger, at beslutningene er usikre, og konsekvensene av gale beslutninger. Algoritmene til KI fungerer som en svart boks, hvor mennesker ikke forstår hvordan maskinen kommer frem til beslutninger som tas. Ofte vil man trenge en forklaring på prosessen når man skal ta en beslutning, og det vil derfor være problematisk dersom dette ikke er tilgjengelig. Forklarbarhet anses derfor som et stort problem innen KI (Øye & Normann, 2021). Videre så må man også ta høyde for vurdering av usikkerheten i beslutningene. Ifølge Øye & Normann (2021) vil KI aldri gi en

beslutning som er 100 prosent sikker. Små endringer kan også forandre beslutningene som tas av KI. Algoritmene i KI er sårbare for små endringer i et bilde eller annen input, noe som kan gi helt forskjellige resultater, og feiltolker det som mennesket kan forstå - noe som kan være farlig (Øye & Normann, 2021). Når det kommer til beslutninger i kriser, hvor man må ta riktige beslutninger, og hvor feil i beslutninger kan medføre negative konsekvenser, er det viktig å ta riktige beslutninger der og da. KI kan med andre ord ende opp med å gjøre skade på liv, miljø og helse basert på feil beslutninger.

En annen svakhet med KI er bærekraft grunnet høyt strømforbruk. KI-algoritmer krever mye elektrisitet, og det å trene opp slike modeller kan kreve like mye energi, og slippe ut like mye karbondioksid som flere biler gjør i løpet av hele sin levetid (Øye & Normann, 2021). Ettersom man trenger å gjennomgå data over mange dager eller måneder, vil CO2-utslippene kunne utgjøre livstidsutslippene til opptil fem biler.

Et annet spørsmål er hvor langt vi kan gå i å overlate beslutningstaking om risikoproblemer til maskiner. Stødle et al. (2024) har sett på nettopp dette, og konkluderte med at det er utfordrende å se hvordan prinsippet om risikoinformert beslutningstaking er oppnåelig uten menneskelig inngrep. Det er flere utfordringer relatert til ordentlig representasjon av usikkerhet, og med å bruke og tolke output fra KI-modeller. De KI-metodene vi har tilgjengelig i dag gir heller ikke en komplett karakterisering av usikkerhet, og KI-modeller gir av og til misvisende output-data, i tillegg til at output-dataen fra KI-modeller ikke alltid er helt forståelig for beslutningstakere (Stødle et al., 2024).

Det kan også være verdt å nevne at teknologi også kan ha sine egne svakheter. Eksempelvis så kan håndtering av store og komplekse datasett som blir generert av stordata, samt bruken av avanserte analyseteknikker som maskinlæring, være utfordrende. Selv om disse datasettene kan inneholde verdifull informasjon om potensielle risikoer og trusler, kan det til tider være utfordrende å trekke ut meningsfulle innsikter fra de, grunnet omfanget og kompleksiteten. Det kan derfor være behov for å utvikle avanserte analysemetoder og dataverktøy som

kan hjelpe til med å forstå og håndtere disse dataene mer effektivt (Bigelow & Botelho, 2022).

En annen svakhet med KI er tilknyttet treningsdata. Ifølge Datatilsynet (2018) krever datamaskiner, da særlig innenfor maskinlæring, langt mer data for opplæring enn det mennesker trenger for å lære det samme. Kvaliteten og egenskapene på denne dataen vil ofte være viktigere enn kvantitet, til tross for det typiske mantraet om at «desto mer treningsdata vi kan fôre modellen med, jo bedre» (Datatilsynet, 2018). For at veiledet læring skal være optimal, er også riktig kategorisering veldig viktig - da data som er feilklassifisert vil kunne påvirke treningsresultatet negativt. Det er også verdt å nevne «black box» problemet, eller heller «den svarte boksen», som handler om at man ikke alltid vet hvordan resultater blir produsert, og dermed ikke kan forklare grunnlaget for beslutningstaking (Datatilsynet, 2018).

4.3. Etiske og juridiske dilemmaer

I tillegg til at KI har enkelte svakheter, medfører KI også flere problemstillinger. Her vil fokuset være på prinsipper for personvern ved bruk av KI og juridiske problemstillinger.

4.3.1. Prinsipper for personvern og KI

KI vil by på enda flere dilemmaer og forhold mellom frihet og sikkerhet enn tidligere. Ifølge Datatilsynet (2018) er det vanlig å skille mellom når KI utvikles ved hjelp av personopplysninger, og når KI brukes for å analysere eller ta avgjørelser om enkeltpersoner. De trekker videre frem fire prinsipper som de anser som mest relevant for KI, og disse prinsippene handler om rettferdighet, formålsbegrensning, dataminimering og gjennomsiktighet.

Når det er snakk om rettferdighet tenker man kanskje at KI vil kunne utføre mer objektive analyser og dermed ta bedre avgjørelser. Algoritmer og modeller vil imidlertid ikke være mer objektiv enn de menneskene som lagde dem eller

personopplysningene som benyttes i opplæringen (Datatilsynet, 2018). Dersom treningsdataen gir et skjevt bilde av virkeligheten eller ikke er relevant for området modeller skal virke på, kan resultatene bli uriktig eller diskriminerende.

Mange av modellene som utvikles med KI skal brukes til gode formål. Formålsbegrensning innebærer at formålet for behandling av personopplysninger må være tydelig angitt og fastsatt når personopplysninger samles inn (Datatilsynet, 2018). Utvikling og bruk av KI krever derimot ofte mange forskjellige typer personopplysninger, og disse er ofte i utgangspunktet samlet inn for andre formål. Selv om slike opplysninger kan være nyttig og gi mer nøyaktige analyser, kan det også være i strid med prinsippet om formålsbegrensning (Datatilsynet, 2018).

Når man skal utvikle KI vil man ofte være avhengig av store mengder personopplysninger. Prinsippet om dataminimering stiller krav om at opplysningene som brukes skal være adekvate, relevant og begrenset til det som er strengt tatt nødvendig for å oppnå det formålet de behandles for (Datatilsynet, 2018). En utfordring her vil være å definere formålet med bruken, ettersom man ikke kan forutse hva algoritmen vil lære. Siden formålet kan endres etter hvert som maskinlæring lærer mer, vil også dette prinsippet bli utfordret, da det kan være vanskelig å definere akkurat hva slags opplysninger som er nødvendige (Datatilsynet, 2018).

Det siste prinsippet handler om gjennomsiktig (transparent) behandling av personvern. Personvern handler i stor grad om å ivareta den enkeltes rett til å bestemme over egne opplysninger. Derfor er det nødvendig at de som behandler personopplysninger er åpne om at de bruker de (Datatilsynet, 2018). Det kan derimot være utfordrende å oppfylle prinsippet om gjennomsiktighet når KI utvikles og brukes, da avanserte former for KI er vanskelig å både forstå og forklare, noe som kan gjøre det nærmest umulig å forklare hvordan opplysninger blir koblet og vektlagt i en spesifikk behandling (Datatilsynet, 2018).

Til tross for at KI trosser personvern på flere ulike områder, og utfordrer de ulike prinsippene for KI, vil det likevel være flere løsninger, verktøy og metoder som kan hjelpe de som behandler personvernsopplysninger med å etterleve

regelverket. Dersom man skal implementere/utvikle KI i sin virksomhet, er det viktig å sette seg godt inn i regelverket og ta i bruk disse løsningene, verktøyene og metodene for å sikre at personvern blir ivaretatt.

4.3.2. Juridiske problemstillinger

Selv om KI skaper mange muligheter og kan effektivisere en rekke prosesser i en virksomhet, reiser det også en rekke rettslige problemer. Werring et al. (2023) har sett på noen juridiske problemstillinger knyttet til bruken av generativ KI. Maskinlæring vil her være den metodikken som gjør det mulig å utvikle generative modeller, og stordata gir den nødvendige mengden data for å trene disse modellene effektivt. Generativ KI er altså et resultat av å bruke maskinlæringsteknikker på store datasett for å genere nye og realistiske dataeksempler.

En problemstilling er erstatningsansvar for feil bruk og misbruk av KI. Dette handler om hvem som er ansvarlig for skade påført som følge av feil og misbruk av KI-systemer. I det fleste tilfeller vil det være produsenten eller tilbyderen av KI-systemene som blir holdt ansvarlig (Werring et al., 2023). KI-systemer som trener på brukeres input vil derimot, kunne utvikle seg selv og genere output som leverandøren ikke har kontroll over.

En annen problemstilling er knyttet til konfidensialitetforpliktelser. Eksempelvis vil bruken av generativ KI som benytter seg av fritekstfelt utgjøre en fare for at konfidensiell informasjon kommer på avveie (Werring et al., 2023). ChatGPT er et eksempel på en modell med et slikt fritekstfelt, og deres personvernserklæring viser til at både ansatte i OpenAI og tredjeparter potensielt kan se opplysningene som skrives der. Hvis brukeren ikke har slått av funksjonen om å bruke input som treningsdata, vil den konfidensielle informasjonen potensielt også kunne bli avslørt til andre brukere (Werring et al., 2023). Risikoen for lekkasje og innsamling av konfidensiell informasjon er derfor en mulighet, og flere ansatte blir forbydd å bruke ulike KI-verktøy grunnet dette. Dersom virksomheter ønsker å bruke generativ KI bør de ha gode interne rutiner og retningslinjer som sikrer at

de ansatte er informert om at konfidensiell informasjon ikke skal lekkes til chatboter (Werring et al., 2023).

En tredje problemstilling er knyttet til cybersikkerhet. EU har foreslått en KI-forordning, som setter cybersikkerhet på agendaen og stiller konkrete krav til høyrisiko KI-systemer (Werring et al., 2023). Denne delen av forordningen handler om viktigheten av at KI-systemer er motstandsdyktig, hvordan cyberangrep mot KI-systemer kan utnytte KI-spesifikke eiendeler slik som treningsdatasett og trente modeller, og at leverandører bør ta passende tiltak for å sikre et cybersikkerhetsnivå som er passende for risikoen. I tillegg til disse foreslåtte kravene, kan en mulig rettslig konsekvens av at for eksempel ChatGPT blir brukt til cyberkriminalitet, være erstatningansvar – og dermed hvem som er ansvarlig for skader som er forvoldt i slike tilfeller (Werring et al., 2023).

Krenkelse av immaterielle rettigheter ved bruk av KI er en annen juridisk problemstilling, og her er opphavsrett et særlig relevant tema. Bruken av generative KI-systemer, som chatboter og tekst-til-bilde-modeller reiser flere problemstillinger (Werring et al., 2023). Opphavsrett gir rettighetshaver enerett til å fremstille digitale kopier av eget verk og laste det opp på internett, ved bruke nav KI-systemer så utfordres imidlertid denne eneretten på flere måter, både i forbindelse med trening av KI og ved bruk av resultater som genereres av KI (Werring et al., 2023). En annen problemstilling som ligger nært, er om resultater skapt av KI kan være beskyttet av immaterielle rettigheter og hvem som i så fall blir innehaver av rettigheten. Werring et al. (2023) viser til at dersom et verk, en tekst, sang eller bilde skal være beskyttet av opphavsretten så ligger det et krav om at åndsverket må være menneskeskapt. Derfor vil den klare oppfatningen være at KI-systemer i seg selv ikke kan være opphaver til et åndsverk, selv om resultatet som genereres er kreativt og originalt. Et annet spørsmål vil dermed være om brukeren kan få opphavsrett til verk som de skaper ved hjelp av KI-verktøy. Den rådende oppfatningen i Europa virker å være at verk som blir skapt ved hjelp av KI-systemer kan være beskyttet av opphavsretten så lenge produktet er et resultat av «brukerens egen intellektuelle frembringelse» (Werring et al., 2023). Et spørsmål vil da her igjen være hvor grensen går for hvor mye

menneskelig input som er nødvendig for at verket skal være opphavsrettslig beskyttet, noe som er uklart.

4.4. Begrensninger med oppgaven

I denne delen av diskusjonen vil det reflekteres over hva man ikke har funnet ut av, og identifisere begrensninger med det nåværende arbeidet, samt forslag til videre forskning. Dette er viktig for å gi en helhetlig forståelse av oppgaven og vise til områder som krever ytterligere utforskning.

Ingen konkret «oppskrift»

Oppgaven har tatt sikte på å identifisere en rekke ideer og potensielle tilnærminger for bruk av KI, tilknyttet spesifikke oppgaver for spesifikke aktører. Det har imidlertid ikke blitt utviklet en konkret «oppskrift» for hvordan disse ideene kan tas videre og implementeres i praksis, kun forslag på hvordan det kan gjøres. Ettersom en konkret plan er nødvendig for å kunne operasjonalisere funnene og gi praktisk veiledning til implementering, kan dette anses som en begrensning. Videre forskning bør derfor fokusere på å utvikle detaljerte retningslinjer for hvordan KI-løsninger kan integreres hos de ulike aktørene.

Begrensning av metode

Denne oppgaven har utelukkende fokusert på eksisterende litteratur og egne antakelser. Ved å inkludere andre metoder, som for eksempel intervjuer av de relevante aktørene, kunne man fått et mer konkret og realistisk bilde av hvilke spesifikke oppgaver de har utfordringer med den dag i dag, samt behov.

Begrensning av teori

Oppgaven har vært begrenset til noen utvalgte teorier innenfor risikostyring, samfunnssikkerhet og KI. Dette kan ha ført til at viktige perspektiver kan ha blitt oversett. Andre teorier kan potensielt ha styrket oppgaven eller vært mer relevant med tanke på resultatene man har kommet frem til. Det er mange ulike arbeidsprosesser som krever ulik risikostyring og bruk av ulik teknologi, og ved å begrense til enkelte teorier vil man ikke dekke alle de ulike prosessene og

områdene. For å få en mer helhetlig tilnærming til hvordan KI kan påvirke risikostyring og samfunnssikkerhet, bør fremtidig forskning utforske og inkludere flere teoretiske rammeverk som kan være av relevans.

Begrensning av oppgaver

Som nevnt tidligere har oppgaven kun sett på spesifikke oppgaver innenfor risikostyring og samfunnssikkerhet som spesifikke aktører innehar, ikke en uttømmende liste - og oppgaven har dermed ikke dekket alle mulige anvendelser av KI. Det gir derfor ikke et fullt innblikk i KI sitt potensial, da det er mange andre oppgaver som også kan dra nytte av KI. Fremtidige studier bør derfor inkludere et bredere utvalg av oppgaver slik at man kan få en mer omfattende forståelse av KI, og hvordan KI kan brukes i flere ulike kontekster. Dette vil gi et mer helhetlig bilde og bidra til å identifisere enda flere muligheter og utfordringer.

Begrensning av konkret teknologi

Oppgaven har videre vært begrenset til noen konkrete teknologier innenfor KI. Det finnes mange andre teknologier som kunne vært vel så interessant og relevant å ta for seg, men som ikke har gjort rede for i denne oppgaven. Videre forskning bør derfor ta sikte på å fortsette å fylle ut Tabell 1, og se på hvordan andre konkrete teknologier kunne vært viktig for andre oppgaver innenfor risikostyring og samfunnssikkerhet, eller om andre konkrete teknologier kunne vært enda bedre enn de som har blitt valgt i denne omgang, for de gitte oppgavene.

Relativt positivt syn på KI

Så langt har oppgaven hatt et relativt positivt syn på KI, og har ikke i tilstrekkelig grad diskutert begrensninger eller utfordringer knyttet til bruken av KI. Det er viktig å erkjenne at KI har en rekke problemstillinger og utfordringer som bør adresseres. For å få et mer realistisk bilde av hvordan KI faktisk kan påvirke risikostyring og samfunnssikkerhet, bør det legges mer vekt på disse utfordringene.

Egen kunnskap om KI

Et annet nevneverdig punkt er at min egen kunnskap om KI er begrenset, noe som kan ha påvirket dybden og bredden av analysen. En grundigere gjennomgang av eksisterende litteratur, eller eventuelt et samarbeid med eksperter på dette områder vil kunne styrke troverdigheten og nøyaktigheten av funnene.

Teknologisk utvikling

Teknologi er i stadig endring og utvikler seg raskt. Det som har vært mest aktuelt og relevant å fokusere på i denne oppgaven kan bli utdatert på kort tid, og dermed begrense relevansen og anvendeligheten av funnene over tid. Dette bør derfor tas med i beregning dersom man skal forske videre eller implementere KI i sin virksomhet.

5. Konklusjon

I denne oppgaven har jeg hatt som mål å *oppnå ny kunnskap* om hvordan KI kan påvirke arbeidet med risikostyring og samfunnssikkerhet. For å oppnå dette har jeg sett på teorier innenfor risikostyring og samfunnssikkerhet, om KI maskinlæring og stordata, samt om eksisterende bruk av KI. Jeg har også sett på ulike utfordringer og behov som eksisterer i dag, og hvilke muligheter KI kan ha for ulike oppgaver innenfor risikostyring og samfunnssikkerhet for ulike aktører. I tillegg til dette har jeg sett på hvordan ulike aktører kan implementere KI i sin virksomhet, samt utfordringer og etiske og juridiske dilemmaer med KI. Gjennom alle disse punktene har jeg også forsøkt å besvare problemstillingen min:

Hvordan kan kunstig intelligens påvirke arbeidet med risikostyring og samfunnssikkerhet?

Med utgangspunkt i KI og eksisterende bruk av KI, er det tydelig at KI kan presentere betydelig forbedringspotensial med tanke på utfordringer og behov som sett i litteraturen og praksis.

Litteraturen har flere utfordringer og behov knyttet til verktøy for å minimere kriser og konsekvenser, kontinuerlig oppdatering av beredskapsplaner, manglende kunnskap og fremtidige risikoer, identifikasjon av trusler, og å ta riktige beslutninger. Her presenterer KI ulike løsninger som kan være med på å effektivisere prosesser, eller til og med gjøre det mennesker ikke får til - blant annet ved å benytte seg av mønstergjenkjenning, prediktiv modellering og automatiserte beslutningsstøttesystemer. KI kan også brukes til å forbedre ROS-analyser, blant annet ved å automatisere identifisering og kategorisering av risikoer, gjennom mønstergjenkjenning og prediktiv analyse. Dette gir virksomheter muligheten til å tilpasse risikostyringsstrategier mer effektivt, styrke beredskapsplaner, og identifisere svakheter. Ved å bruke KI i risikomatriser kan man evaluere sannsynlighet og konsekvenser av hendelser mer nøyaktig. Sløyfemodellen kan også forbedres ved hjel av KI, ved at man kan forutsi initierende hendelser og optimalisere barrierer for å forhindre alvorlige konsekvenser. Basert på dette er det klart at konkrete teknologier, slik som

mønstergjenkjenning, prediktiv analyse og nevrale nettverk, kan bidra til mer presise og effektive ROS-analyser, og dermed risikostyring.

Når det kommer til utfordringer og behov i praksis er det også tydelig at KI kan være av stor betydning for risikostyring og samfunnssikkerhet, og kan påvirke disse områdene på mange forskjellige måter. Med utgangspunkt i KI, og derunder maskinlæring og stordata, blir flere konkrete teknologier presentert - slik som mønstergjenkjenning, prediktiv analyse og automatisert beslutningsstøtte, overvåkning, nevrale nettverk og veiledet læring. Som sett så vil mønstergjenkjenning kunne brukes til å optimalisere kommunikasjonsprosesser, gi innsikt i hvilke områder som trenger forbedring og hva som har fungert godt tidligere, identifisere og analysere mønster i ulike kommuner og fylker med tanke på risikofaktorer og hendelser, og analysere, forutsi og advare om naturhendelser. Prediktiv analyse og automatisert beslutningsstøtte kan brukes til å analysere kriminalitet, planlegge og tilpasse i tråd med fremtidige behov og utfordringer, evaluere sannsynlighet for ulike typer hendelser, prioritere tilsyn, identifisere svakheter i eksisterende beredskapsplaner og implementere tiltak, og predikere konsekvenser av hendelser. Overvåkning kan brukes til digital overvåkning for å oppdage og forebygge cyberangrep, bruke sensornettverk for å overvåke miljøforhold, og gi informasjon om faktorer som påvirker samhandling mellom ulike aktører. Nevrale nettverk og veiledet læring kan brukes til å identifisere komplekse sammenhenger mellom ulike faktorer som påvirker risiko og sikkerhet, identifisere effektive tiltak som har blitt gjort tidligere og dermed optimalisere og justere ressursallokeringer, analysere datasett effektivt, og automatisere oppgaver. Til tross for alt dette, er det ikke en uttømmende liste på alle muligheter som KI kan ha for risikostyring og samfunnssikkerhet. Det finnes enda flere konkrete teknologier innenfor KI, som ikke har blitt nevnt i denne oppgaven, samt utallige oppgaver og aktører som kan ha nytte av slike teknologier og de løsningene de gir.

Selv om KI kan påvirke, og mange steder styrke risikostyring og samfunnssikkerhet, er det også viktig å se på utfordringer, og etiske og juridiske dilemmaer ved bruk av KI. Bruken av KI byr på flere dilemmaer knyttet til

personvern og de tilhørende prinsippene om rettferdighet, formålsbegrensning, dataminimering og gjennomsiktighet. KI medfører også en rekke juridiske problemstillinger, knyttet til erstatningsansvar for feil bruk og misbruk av KI, konfidensialitetforpliktelser, cybersikkerhet og krenkelse av immaterielle rettigheter. Disse er alle dilemmaer og problemstillinger som er viktig å være klar over, og ha gode retningslinjer for, dersom man ønsker å implementere KI i sin virksomhet, og som kanskje er lett å glemme litt av når man tenker over alle mulighetene det kan ha.

Referanser

Aven, T. (2015). *Risk analysis* (2nd ed.). Chichester, West Sussex, United Kingdom: John Wiley & Sons.

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

Bigelow, B. & Botelho, S. J. (2022, januar). *Big data*. TechTarget. https://www.techtarget.com/searchdatamanagement/definition/big-data

Bjelland, B. & Nakstad, E. R. (2018). *Beredskap, kriseledelse og praktisk skadestedsarbeid: en lærebok for helse- og beredskapspersonell på strategisk, operasjonelt og taktisk nivå*. Gyldendal.

Boletsis, K., Nilsson, E. G. (2021). *RiskTUN: Risk-aware Decision Support System for Tunnel Safety*. SINTEF. https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2995592/202100140%2b-%2bRapport%2bRiskTUN_%2bRisk-aware%2bDecision%2bSupport%2bSystem%2bfor%2bTunnel%2bSafety%2b-%2bsignert.pdf?sequence=2&isAllowed=y

Bray, K. (u.å.). *9 Simple Steps: How To Effectively Implement AI In Business.* Zesium. https://zesium.com/9-simple-steps-how-to-effectively-implement-ai-in-business/

Casagli, N., Tofani, V., Sassa, K., Bobrowsky, P. T. & Takara, K. (2021). *Understanding and Reducing Landslide Disaster Risk* (3. utg.). Springer.

Cox, L.A. (2008). What's wrong with risk matrices? *Risk Analysis, 28*(2), 497-512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Datatilsynet. (2018). *Kunstig intelligens og personvern*. https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/rapport-om-ki-og-personvern.pdf

DSB. (2023). *Brukerevaluering Nødnett 2023: landsdekkende brukerundersøkelse blant alle brukere i Nødnett.* Nødnett.

https://www.nodnett.no/siteassets/bibliotek/rapporter/brukerevaluering-nodnett-2023.pdf

DSB. (u.å.). *Om DSB*. Hentet 3. mai 2024 fra https://www.dsb.no/menyartikler/om-dsb/

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

Folkehelseinstituttet. (2023). *Erfaringer fra koronapandemien: Lærdommer og anbefalinger for FHI og den nasjonale beredskapen.* https://fhi.brage.unit.no/fhi-xmlui/bitstream/handle/11250/3098111/Erfaringer_2023.pdf?sequence=2

Kruke, B. I., Olsen, O. D. & Hovden, J. (2005). *Samfunnssikkerhet – forsøk på en begrepsfestning*. NORCE. https://norceresearch.brage.unit.no/norceresearch-xmlui/bitstream/handle/11250/2674989/RF%202005-034.pdf?sequence=1

Laskowksi, N. & Tucci, L. (2023, november). *A guide to artificial intelligence in the enterprise*. TechTarget. https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence

Lynggaard, K. (2010), Dokumentanalyse. I S. Brinkmann & L. Tanggaard (Red.), *Kvalitative metoder: Empiri og teoriutvikling*. Gyldendal akademisk.

NORCE. (u.å.). *Radar interferometry og offset tracking*. Hentet 15. april 2024 fra https://www.norceresearch.no/forskningstema/radar-interferometry-and-offset-tracking

Nødnett. (u.å.). *Hva er Nødnett?* Hentet 15. april 2024 https://www.nodnett.no/om-nodnett/hva-er-nodnett/

Regjeringen. (2018, 11. september). Samfunnssikkerhetskjeden. https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/samfunnssikkerhetskjeden/id2340021/

Riddell, G. A., van Delden, H., Maier, H. R., & Zecchin, A. C. (2019). Exploratory scenario analysis for disaster risk reduction: Considering alternative pathways in

disaster risk assessment. *International Journal of Disaster Risk Reduction, 39*, 101230. https://doi.org/10.1016/j.ijdrr.2019.101230

Ringdal, K. (2018). *Enhet og mangfold: Samfunnsvitenskapelig forskning og kvantitativ metode* (4. utg.). Fagbokforlaget.

Røde Kors. (u.å.). *Beredskap*. Hentet 10. april fra https://www.rodekors.no/vart-arbeid/beredskap/

SINTEF. (u.å.). *Kunstig intelligens for bedre helse*. Hentet 5. juni 2024 fra https://www.sintef.no/fagomrader/kunstig-intelligens/kunstig-intelligens-for-bedre-helse/

Song, X.-P., Hu, Z.-H., Du, J.-G., & Sheng, Z.-H. (2014). Application of Machine Learning Methods to Risk Assessment of Financial Statement Fraud: Evidence from China. *Journal of Forecasting, 33*(8), 611–626. https://doi.org/10.1002/for.2294

Stortingsmelding Nr. 17 (2001-2002): *Samfunnssikkerhet: Veien til et mindre sårbart samfunn.* Det kongelige justis- og politidepartement. https://www.regjeringen.no/contentassets/ee63e1dd1a16409fa0bb737bfda9279a/no/pdfa/stm200120020017000dddpdfa.pdf

Stødle, K., Flage, R., Guikema, S., & Aven, T. (2024). Artificial intelligence for risk analysis - A risk characterization perspective on advances, opportunities, and limitations. *Risk Analysis*. https://doi.org/10.1111/risa.14307

Thagaard, T. (2018). *Systematikk og innlevelse: En innføring i kvalitative metoder* (5. utg.). Fagbokforlaget.

Walch, K. (2021, 27. april). *Big data vs. machine learning: How they differ and relate*. TechTarget. https://www.techtarget.com/searchbusinessanalytics/tip/Big-data-vs-machine-learning-How-they-differ-and-relate

Werring, E. A., Sivertsen, E. K., Vislie, C., Bjørgo, H. C., Stabell, A. (2023). *Hvilke juridiske problemstillinger kan oppstå i forbindelse med kunstig intelligens?* Thommessen. https://www.thommessen.no/aktuelt/personvern-og-immaterialrett-hvilke-problemstillinger-kan-oppsta-i-forbindelse-med-bruk-av-kunstig-intelligens

Øye, O. J. & Normann, M. (2021). Dette er utfordringene med kunstig intelligens. *Oslomet*. https://www.oslomet.no/forskning/forskningsnyheter/dette-er-utfordringene-med-kunstig-intelligens