MAY-LENE GABRIELSEN
VEILEDER: MARJA KATARIINA YLÖNEN

Cybersikkerhet i den utviklende digital tiden

En undersøkelse på hvordan man kan forebygge trusler mot cybersikkerheten

[Bacheloroppgave] [2024]

[Toll, vareførsel og grensekontroll]

[Institutt for sikkerhet, økonomi og planlegging]

[Det teknisk-naturvitenskapelige fakultetet]

Sammendrag

Formålet med denne oppgaven var å undersøke om det finnes løsninger på hvordan man kan forebygge cybertrusler og sårbarheter mot cybersikkerheten i en utviklende digital tid. Oppgavens teoretiske rammeverk inkluderte beredskap og cyber-risikostyring. Data og metode som ble brukt i denne oppgaven var litteraturstudie og tematisk analyse. Resultatet fra analysen viste at det finnes en del trusler og sårbarheter ved digitalisering og digital transformasjon. De mest vanlige truslene var cyberangrep der kriminelle fikk tilgang til sensitiv informasjon, for å forandre, ødelegge eller utpresse penger fra organisasjoner. Det ble også funnet at ny teknologi som kunstig intelligens, maskin læring og blockchains er både en sårbarhet og en løsning for cybersikkerheten, og man burde fokusere på god beredskap og cyber-risikostyring for å kontinuerlig forbedre cybersikkerheten.

Abstract

The purpose of this bachelor`s thesis was to investigate if there are solutions on how one can prevent cyber threats and cybersecurity vulnerabilities in a evolving digital age. The theoretical framework includes emergency preparedness and cyber-risk-management. The data and the methods used were literature study and thematic analysis. The results of the analysis showed that there are several threats and vulnerabilities in digitalization and digital transformation. The most common threats were cyber-attacks where cyber-criminals gained access to sensitive information, to change, destroy or extort money from organizations. It was also found that new technology such as Artificial Intelligence, Machine Learning and Blockchains are both a vulnerability and solution for cybersecurity, and one should focus on good emergency preparedness and cyber-risk-management to continuously improve cybersecurity.

Innhold

Begreper

Cybersikkerhet (Cybersecurity)

Cybersikkerhet er beskyttelse av cyberspace mot cybertrusler. Når man definerer cybersikkerhet leter man ikke etter hva man skal beskytte, men heller hva man skal beskytte mot. Cybersikkerhet handler i hovedsak om å beskytte cyberspace (Haugom, et al., 2019), men de fleste organisasjoner er mer opptatt i hvordan cybersikkerhet kan beskytte deres egne cybersystems mot cyberangrep (Refsdal, et al., 2015, s. 29).

Cyberspace og cybersystems

Cyberspace er en samling av sammenkoblede datastyrte nettverk, dette inkluderer datasystemer, kontrollere, informasjonslagring og servere. Det mest populære cyberspace er internett (Refsdal, et al., 2015, s. 25). Systemene som bruker cyberspace kalles cybersystemer, og er en del av organisasjonsstrukturen til de fleste organisasjoner. På grunn av at cybersystemer kan inneholde informasjonsinfrastrukturer som er involvert i organisatoriske prosesser. (Refsdal, et al., 2015, s. 26).

Cybertrusler (Cyber-threats)

Cybertrusler er trusler via cyberspace. Disse kan være ondsinnet eller ikke ondsinnet. Eksempel på ondsinnet angrep er tjenestenektangrep «denial of service attacks», der angrepet er gjort med intensjon for å overbelaste systemer slik at de bryter sammen (Kumar, 2016). Ikke ondsinnet trusler kan være dersom det oppstår systemkrasj på grunn av dårlig internett eller slitasje på ledninger (Refsdal, et al., 2015, ss. 29-30).

Cyberrisiko (cyber-risk)

Cyberrisiko er risiko som oppstår på grunn cybertrusler. Cyberrisiko er ikke lik vanlig risiko, på grunn av at cyberrisiko oppstår ved cybertrusler på et cybersystem. Dette betyr at det ikke er en cyberrisiko med mindre det er trusler innen cyberspace (Refsdal, et al, 2015, 33).

Digitalisering

Digitalisering er en digital prosess, en prosess der noe blir digitalt, som for eksempel et digitalt samfunn eller en digital organisasjon (Andersen & Ragnvald, 2017, s. 1). IT går fra å være et støtteverk til å være en del av organisasjons-DNA. Det handler om å forandre på

forretningsprosess og -modeller med å ta nytte av digitisering (digitizing), med å forandre noe fra analog til digital (Andersen & Sannes, 2018, s. 1).

Digital transformering

Digital transformasjon handler om å adoptere digitale løsninger for forretningsprosesser i organisasjoner. Man transformerer organisasjonsprosesser til teknologiske løsninger, som kan endre flere aspekter av en organisasjon. IT blir en større del av organisasjonsprosessene (Saeed, et al., 2023, s. 1).

Risiko

Risiko kan defineres på mange måter, det kan være muligheten for uønskede hendelser eller potensialet for at uønskede hendelser skjer. Enkelt sagt er risiko, der en hendelse eller aktivitet kan føre til en uønsket hendelse eller negativ konsekvens. Her ser man på tre punkter; hendelse, konsekvens og usikkerhet, hvor dersom en hendelse skjer hva vil konsekvensen bli, og hvilke usikkerheter er det rundt dette (Aven, et al., 2018, s. 4).

Internet of Things

The Internet of Things (IoT), har laget en ny standard med et nettverk av maskiner og teknologiske enheter som er koblet til hverandre. Dette gjør at de lett kan kommunisere og samarbeide med hverandre, for å lage en ny og bedre prosess hos bedrifter (Lee, 2020, s. 1).

Kunstig intelligens (Artificial Intelligence)

Kunstig intelligens er ofte omtalt som en ny teknologi. Den ble laget for å erstatte manuelt arbeid som mennesker utfører. Hvor intelligente maskiner og dataprogrammer blir laget for å utføre oppgaver som er mer krevende for mennesker, men som likevel krever en menneskelig intelligens. Kunstig intelligens bruker ytre data for opptre bedre på oppgavene den gjør, i tillegg til å etterligne menneskelig intelligens (Anjila P K, 2021, s. 65).

Maskin læring (Maskin learning)

Maskin læring gjøres ved at det lages en oppskrift i form av algoritmer for å vise hvordan noe skal gjøres, som igjen blir instruksene for maskinen. Datamaskiner er i stand til å lære mange ting, fra sammenhenger i data, regler og strategier. Dette læres av data fra omverdenen. Dette gjør at maskiner tilpasser seg data kontinuerlig og jo mer data den får

tilgang til, jo mer lærer den og kan bruke for å presisere oppgavene den utfører. Det man kan bruke maskin læring til er å lage prediksjoner for å fylle ut manglende informasjon om et område (Fosse, et al., 2018, ss. 7-9).

Blockchain

Blockchains hovedoppgave er å registrere og lagre informasjon og data i en blokk på tvers av mange dataenheter. Disse blokkene knyttes sammen i en lang kjede eller «chain». Her er det mange enheter som har tilgang og de må alle bli enige dersom en endring i kjeden skal bli gjort. Blockchain er en distribuert database hvor mange enheter/parter kan lese og lage transaksjoner til databasen. Kjeden har en innebygd konsensusmekanisme, slik at det er selve kjeden som sjekker alle transaksjonene og ikke en tredjepart (Alman & Hirsh, 2019, s. 11).

1 Innledning

Tiden vi lever i dag kalles den digitale tid. Denne tiden startet i 1980 med mer avansert teknologi, som datamaskiner og internetteknologi. Dette ga mennesker muligheten med å spre informasjon fritt og raskt (Haugom, et al., 2019, s. 24). Teknologien blir forbedret og mer avansert, og man begynner å leve i en mer digitalisert verden, hvor man tar inn ny teknologi for å tilpasse seg verden rundt. Det at verden blir mer digital kan være en positiv ting, med at driften i samfunnet blir mer effektivt, man får flere muligheter og man kobler verden sammen på en effektiv måte (Petersons, 2024, s. 1). Det sagt, betyr også digitalisering at man blir mer avhengig av teknologi enn det man har noen gang vært. De fleste bedrifter er drevet av teknologi. All personlig og drifts informasjon ligger i dag på nettet, for å ha lettere tilgang til dem. Digital teknologi er en del av alle aspekter av livet i dag, som gjør det enda viktigere å integrere god cybersikkerhet (Haugom, et al., ss. 24-26). Sårbarheten som oppstår i den digitale tid er sårbar mot det som kalles cyberangrep. Dette er angrep som kommer via cyberspace som har intensjon til å skade (Refsdal, et al., 2015, s. 29). Et slikt angrep på en person kan få konsekvens ved at man mister tilgang til brukere eller at man blir utsatt for identitetstyveri. Dette er mer personlig skader, men trenger ikke å ha store konsekvenser på samfunnet. Et cyberangrep på en organisasjon eller bedrift kan ha større konsekvenser. Eksempler på slike konsekvenser kan være med angrep som stenger organisasjoner ute av egne datasystemer, eller at personlig og sensitiv informasjon blir lest av uautoriserte parter, som kan føre til økonomiske tap, skade på omdømmet eller stopp på prosesser innen organisasjoner (Saeed, et al., 2023, ss. 4-5).

Dersom man ønsker et annet eksempel kan man se på meldingen fra regjeringen i 2022, som viste at det var mange alvorlige cyberangrep mot norske bedrifter, og rundt 80% av dem kunne ha vært unngått med grunnleggende sikkerhetstiltak (Regjeringen, 2022). Risikobildet til Nasjonalsikkerhetsmyndighet så i 2023 at det var gjort avanserte cyberangrep mot 12 departementer, dette er seksdoblet siden 2022 (Nasjonal-Sikkerhetsmyndighet, 2023). Dersom man ser på stortinget i Norge har de blitt utsatt for cyberangrep flere ganger i tiden mellom 2020-2022 (Stortinget, 2022). Ved faren for cyberangrep og sårbarhetene med den digitale verden er det viktig å ha gode sikkerhetsmarginer, for privatpersoner og spesielt for organisasjoner og bedrifter. Denne typen sikkerhet kalles for cybersikkerhet, som er beskyttelsen av cyberspace mot cybertrusler og -angrep (Refsdal, et al., 2015, s. 29). Selv med god cybersikkerhet kan man

være sårbare mot angrep, på grunn av at det kan oppstå sårbarheten innenfor cybersikkerhet. Derfor er det viktig at man er klar over sårbarhetene slik at man kan forebygge dem og styrke sikkerheten.

Tema i denne bacheloren er IKT og sikkerhet, med spesifisering på cybersikkerhet og teknologisk utvikling. Dette er på grunn av den økene teknologien og det økende trusselbilde. Det skal bli sett på de ulike cybertruslene og sårbarheter som kan oppstå, og metoder for å forebygge slike trusler og sårbarheter. Grunnen til at dette virker viktig å studere er på grunn av at verden blir mer teknologisk og mer avhengig av nyere teknologi, og med det oppstår det nye trusler hele tiden. Derfor er det viktig at man ser på hvordan man skal forebygge disse truslene i takt med utviklingen av teknologier, for å beskytte samfunnet best mulig.

Studielinjen denne oppgaven er fra, er «Toll, vareførsel og grensekontroll». Derfor er det naturlig å diskutere hvordan problemstillingen påvirker Tolletaten. Hovedtema i oppgaven er cybersikkerhet og det vil derfor ikke fokuseres på Tolletaten gjennom data, analyse og hovedsakelig diskusjonsdelen. Det sagt vil det avslutningsvis i diskusjonen, diskuteres hvordan dette tema kan påvirke Tolletaten. Tolletatens har et samfunnskritisk oppdrag, og skal sikre at lover og regler blir etterlevet for grensekryssende vareførsel. Dette for å holde samfunnet trygt, bærekraftig og rettferdiggjøre næringslivet (Tolletaten, 2022, s. 2). Tolletaten startet en omorganisering 01. oktober 2020, der de endret organisasjonsstruktur. Her fokuserte de på en rask overgang til nye teknologi-systemer for raskere oppgaveløsninger (Tolletaten, 2020). Denne omorganiseringen kom som et oppdrag fra Finansdepartementet i 2016, og sa at Tolletaten måtte prioritere arbeidet med digitalisering, for å gjøre det lettere for reisende og bedrifter ved grenseoverganger (Finansdepartementet, 2021). Den nye teknologien det var fokus på var et nytt system, Digitoll. Her blir prosessene som før var gjort manuelt, digitalt, for å fjerne tidskrevende prosess ved innføring av varer til næringslivet (Tolletaten, 2024). På grunn av denne digitaliseringen og digitale transformasjonen på etaten er det også interessant å bruke Tolletaten som et mer konkret eksempel på hva cybertrusler, sårbarheter og løsninger kan bety for en organisasjon.

1.1 Hensikten med oppgaven

Hensikten med dette systematiske litteraturstudiet og tematisk analysen er å se på hvordan tidligere studier ser på problemet med cybersikkerhet i den utviklende digitale tiden. I tillegg til å legger frem en ny løsning for å bygge videre på de tidligere studiene.

1.2 Problemstilling

Problemstillingen i denne oppgaven blir dermed «Hvordan kan man forebygge de ulike sårbarhetene og truslene som oppstår mot cybersikkerheten i en utviklende digital tid?» For å svare på denne problemstillingen deler jeg det inn i to spørsmål, «hvilke sårbarheter og trusler kan oppstå?», og «hvordan kan man forebygge de eventuelle sårbarhetene og truslene?» Når oppgaven nevner den digitale tid, innebærer dette både digitalisering og digital transformasjon.

2 Teoretisk rammeverk

Denne oppgaven bruker to teoretiske rammeverk som et perspektiv på problemstillingen, når artiklene blir analysert. Disse teoriene er beredskap og cyber-risikostyring.

2.1 Beredskap

Beredskap handler om å være forberedt på å håndtere utfordrende, uønskede, eller alvorlige hendelser. Beredskap er dermed de tiltakene man gjør for å forebygge og håndtere uønskede hendelser i tillegg til å redusere konsekvensene som kan oppstå (Engen, et al., 2021, s. 321). Man er beredt med å kunne forutse og håndtere mulige trusler som kan oppstå på en effektiv måte. Dette kan beskrives med fire ord; prosess, produkt, aktivitet og tilstand. Beredskap er en prosess som aldri tar slutt, og er et produkt i form av beredskapsplan. Aktiviteten i beredskap er trening og øvelser, og å bruke beredskap er en tilstand på grunn av at man er beredt (Engen, et al., 2021, s. 321). God kunnskap om beredskapssituasjoner er noe man alltid burde ha, på grunn av at neste hendelse man møter vil aldri være helt identisk til den forrige. Beredskap handler derfor ikke om å håndtere situasjonene man trener på, men å ha en generell kunnskap ved å lære seg karakteriserte trekk ved treningssituasjonen. Man gir personer kunnskap og ferdigheter for å håndtere beredskapssituasjoner ved å lære hvordan man kobler en situasjon med kjennetegn og atferd til situasjonene. (Sommer, et al., 2020, s. 39). Den beredskapen oppgaven fokuserer på er beredskapshjulet.

Beredskap sees ofte som et hjul som beskriver faser i beredskapsarbeid. Første fase i hjulet er «risikoanalyse» her utfører man en risikovurdering for å etablere akseptabel risiko med basis på hvor mye kunnskap om eventuelle trusler man har, for å kartlegge og beskrive den risikoen som eksisterer. Risikoanalysen skal lage et «risikobilde» av de farene og truslene man identifiserer. Den neste fasen i hjulet blir dermed «beredskapsanalyse», her tar man truslene fra risikoanalysen for å finne de uønskede hendelsene man ønsker at beredskapen skal håndtere. Her identifiseres to forhold, ambisjon for god beredskap og ressurser man har for å svare på uønskede hendelser. De første fasene jobber med hverandre og sammen skal de kartlegge de aktuelle farene man skal være forberedt på, og kunnskap om den nødvendige beredskapen. Ved å finne ressursbehovet ved ressurskartleggingen fra de første fasene går man over til den tredje fasen «beredskapsplan». Her ser man på hvem som har ansvaret, hvor, når og hvordan beslutningene skal tas. Her viser planen hvilke typer beredskap man trenger for å håndtere de aktuelle uønskede hendelsene. Etter fasene om analyse og planlegging kommer fasen hvor man «etablerer» beredskapsstrukturen og ressursene ved øvelser og trening. De forrige fasene skal sikre at neste fase «responsene» til en uønsket hendelse er planlagt, effektiv, forutsigbar og koordinert. Den siste fasen handler om «evaluering» hvor man tar lærdom av de virkelige hendelsene som man trener og øver til. Denne lærdommen er dermed grunnlaget for en ny forbedret beredskap, for det er en kontinuerlig prosess eller et hjul som aldri tar slutt, man oppdaterer analysene, planene og øvelsene hele tiden (Engen, et al., 2021, s. 326).

2.2 Cyber-risikostyring (Cyber-Risk-Management)

Dersom man ser på trusler og sårbarheter innen cybersystemer kan det hjelpe å se på det fra cyber-risikostyrings perspektivet. Det første man kan se på er hva vanlig risikostyring er for å så se hvordan dette overføres til cyberspace. Risikostyring er prosessen for å identifisere risiko, vurdere risiko og lage løsninger for å redusere risikoen. Det er tre prosesser innen risikostyring, (i) risikovurdering, (ii) risikoreduksjon og (iii) evaluering og vurdering (Stoneburner, et al., 2002, ss. 1, 4). Kort sagt handler risikostyring om hvordan man styrer og vurderer risiko (Aven, et al., 2018, s. 8). For å overføre denne styringen over til cyberspace kan man først se på hvilken risiko man ser på i cyberspace. Det er ikke vanlig risiko man ser etter, men cyberrisiko som oppstår på grunn av cybertrusler mot cybersystemer (Refsdal, et al., 2015, s. 33). Videre kan man tenke at det finnes to typer

cyberrisiko. Det er ondsinnede og ikke-ondsinnede cyberrisiko, der ondsinnede cyberrisiko oppstår av cybertrusler og ikke-ondsinnede cyberrisiko er i de fleste tilfeller uhell. Cyberrisiko oppstår i de fleste tilfeller når det er en blanding av både ondsinnede og ikke-ondsinnede cyberrisiko (Refsdal, et al., 2015, s. 34). Måten man håndterer risiko er avhengig av hvilken type det er, om det er ondsinnet eller ikke-ondsinnet. Et godt startpunkt er å identifisere cyberrisiko ved å identifisere mulige trussel-kilder (Refsdal, et al., 2015, ss. 35-36). For å identifisere cyberrisiko kan man skille mellom de data typer som kan skape cyberrisikoer, høyrisikodata og lavrisikodata. Det er høyrisikodata som er viktig å beskytte, og det er viktig at organisasjoner vet hvor deres høyrisikodata ligger for å kunne beskytte disse mot uautorisert tilgang. Da kan bedrifter begynne med å kartlegge områder i bedriften hvor det kan samles høyrisikodata. Dette kan være menneskelige ressursene, økonomi områder og kunderelasjoner (Freedman, 2023). Her finner man de mulige trussel-kildene, og kan gå videre på cyber-risikostyringen.

Videre kan man se på hvordan man skal vurdere risiko, det er forskjellige måter det kan gjøres og er avhengig av om det er ondsinnet eller ikke-ondsinnet risiko. Ondsinnet har menneskelig intensjoner og motiv, og kan være vanskelig å forutse. Derfor kan det hjelpe dersom man lager sikkerhetstestinger, systemtesting og sårbarhetstesting. Dette kan hjelpe med å finne ut hvor sårbar disse risikoene er for angrep og manipulasjon. Man analyserer derfor årsaken og bakgrunnen til cyberrisiko som er cybertrusler og sårbarheter. Her begynner man å se på teknikker for trussel-modeller for å beskrive angripers teknikker, evner, motiv og kunnskap, likt kan man lage modeller for sårbarhetene. Med hjelp av disse modellene kan man se hvor sannsynlig risikoen for trusler og sårbarheter er. Her fokuserer man på kunnskapen om hvem og hva trussel-kildene er og hvordan de oppstår, for å estimere hva konsekvensene av en uønsket hendelse er (Refsdal, et al., 2015, ss. 42-43).

Dersom man skal finne løsninger for å redusere risiko kan man se på kommunikasjon og trening. God cyber-risikostyring implementeres med god og effektiv kommunikasjon av cyberrisiko. Her lager organisasjoner klassifiseringer og kategoriseringer av informasjon, for å representere og forstå relevant informasjon. Målet her er å oppbevare relevant informasjon som er stadig oppdatert om cybertrusler, sårbarheter, hendelser, strategier for cyberrisiko. I tillegg til skadebegrensninger og profiler av aktører som kan gjøre skade (Refsdal, et al., 2015, s. 35). Her kan man også se på risikomodellene nevnt over for å vurdere nye løsninger og strategier. En annen løsning på cyberrisiko er ved å skape en

bevissthet når det kommer til cyberrisiko, dette er ved trening, sikkerhetsprinsipper og gode sikkerhetsrutiner (Refsdal, et al., 2015, s. 44).

3 Data og Metode

I dette kapittelet blir det gjort rede for hvilke søkeprosess og datainnsamling som ble brukt i oppgaven. Her blir det nevnt systematisk litteraturstudie, tematisk analyse, kvalitativ metode, avgrensinger og kildekritikk. Litteraturstudie ble brukt for å samle inn data, mens tematisk analyse ble brukt for å analysere dataen.

3.1 Systematisk litteraturstudie og datainnsamling

Systematisk litteratursøk fokuserer på eksplisitte søkekriterier slik at man kan forske videre ved at man replikerer søkeprosessen. Her definerer man først begreper man ønsker å søke med, etter finner man hvilke søkekilder man skal bruke. Deretter lages det eksklusjons- og inklusjonskriterier for å finne studier man kan ta med eller utelukke. Etter det gjennomføres søket, ved å bruke søkeordene og avgrensningene på valgte søkeområder. Det vurderes så om litteraturen er relevant, ved å lese sammendraget, av hver artikkel som virker relevant (Jacobsen, 2022, ss. 81-84).

3.1.1 Søkeprosess

Søkeprosessen jeg brukte var et systematisk litteratursøk, der jeg brukte forskjellige begreper innen cybersikkerhet og den digitale verden for å finne relevante artikler. Artiklene som ble valgt er av, Petersons (2024), Mosteanu (2020), Saeed et al., (2023), AlSalem et al., (2023) og Lee (2020). De blir presentert dypere senere i oppgaven, og det er disse artiklene litteraturstudie skal analysere. Jeg valgte å bruke ulike databaser som Google Scholar og Oria i søkeprosessen for å finne relevante artikler. Noen av artiklene ble funnet på begge databasene, men jeg nevner kun den første jeg fant de i. Tabellen under viser den systematiske søkeprosessen.

Tabell 1. Søkeprosess

Database	Søkeord	Treff	Avgrensninger	Treff etter avgrensning	Leste abstrakter	Inkludert i oppgaven
Google Scholar	Cybersecurity challenges and digitalization	69 000			5	1
Google Scholar	Digitalization and cybersecurity	84 300	Etter 2020	16 600	10	2
Oria	IoT and cybersecurity	2658	Fra 2020-2024	1 919	5	1
Google Scholar	Cybersecurity risk and IoT	107 000			3	1

3.1.2 Avgrensninger

Jeg brukte forskjellige søkeord på grunn at jeg ville se om det var forskjellige syn dersom søkeordene var forskjellige. Uten avgrensninger fikk jeg et treff på mellom 2658 og 107 000. Derfor valgte jeg å bruke en del avgrensninger på søkene ved å bruke ulike kriterier for å redusere treffene jeg fikk. Disse kriteriene var en tidsbegrensning på når artiklene var skrevet, fra 2020-2024. Noen ganger valgte jeg ikke å legge inn avgrensninger i google, på grunn av at jeg allerede hadde funnet den relevante artikkelen uten avgrensningene, men artiklene lå fortsatt under kriteriene å være skrevet mellom 2020 og 2024. Et av de andre kriteriene var at artiklene måtte inneholde to konsepter «cybersikkerhet» og noe innen «den digital tid».

3.1.3 Utvalg av data og kildekritikk

Det første jeg så etter når jeg søkte på data var gyldighet og relevans, at kildene faktisk er relevante, riktige, og kan stoles på (Jacobsen, 2022, s. 17). Grunnet at det er en systematisk litteraturstudie kan andre som ønsker å forske videre på dette tema, bruke min søkeprosess for å finne de artiklene som er brukt. Det er viktig å være kildekritisk når man skriver en oppgave og søker etter data. Derfor valgte jeg artikler som er skrevet på fagfellevurderte

databaser som leser igjennom og vurderer all litteratur og ser på at den er pålitelig. Artiklene er også relevante på grunn av de kriteriene jeg satt da jeg søkte etter data. Da ser jeg spesielt på det første kriteriet, dato. Alle artiklene jeg valgte er laget mellom 2020 og 2024, som viser at dataen i dem er oppdatert, som er viktig i forhold til dette tema. Cybersikkerhet er et tema som endrer seg på grunn av teknologiendringer og det er derfor viktig å bruke data som er oppdatert slik at man får den mest relevante og korrekte data ut av dem.

Jeg valgte 5 artikler som studerer samme tema som jeg har valgt i problemstillingen. Det som gjør de relevante, er at de alle har en forskjellig vinkel de studerer dette på. Noen av artiklene ser direkte på hvordan digitalisering skaper sårbarheter og løsninger innen cybersikkerhet, mens andre ser mer på digital transformering i stedet for digitalisering. To av artiklene fokuserer mer på IoT enn digitalisering. Grunnen til at alle er like relevante er på grunn av at de nevner sårbarheter som kan oppstå i den digitale tid, og ser på cybersikkerhet. Etter dette skal jeg presentere artiklene og utføre en litteraturgjennomgang av hovedtemaet til hver av artiklene før jeg analyserer dem.

3.2 Data og litteraturgjennomgang

Data som ble samlet, er fem teoretiske artikler; (i) “Cybersecurity challenges in the era of digitalization” av Edgard Petersons (2024) publisert av SSRN Electronic Journal. (ii) “Challenges for organizational structure and design as a result of digitalization and cybersecurity” av Narcisa Roxana Mosteanu (2020) publisert av The business and Management review (Volum 11, Utgave 1). (iii) “Digital transformation and cybersecurity challenges for business resilience: Issues and Recommendations” av Saqib Saeed, Salha A. Altamimi, Norah A. Alkayyal, Ebtisam Alshehri og Dina A. Alabbad (2023) publisert av Sensors (Volum 23, Utgave 15). (iv) “Cybersecurity risk analysis in the IoT: A systematic review” av Thanaa Saad AlSalem, Mohammed Amin Almaiah og Abdalwali Lutfi (2023) publisert av Electronics (Volum 12, Utgave 18). (v) “Internet of things (IoT) cybersecurity: Literature review and IoT cyber risk management av In Lee (2020) publisert av Future Internet (Volum 12, Utgave 9).

Det var viktig for meg at alle artiklene nevnte cybersikkerheten i en av formene for digital tid, mer spesifikt er det snakk om digitalisering, digital transformering og systemer i digitalisering som for eksempel IoT. Det var også interessant å se hvordan hver av artiklene

ser på den digitale tid om det var med et negativt eller positivt syn. Dersom man ser på det som positivt først kan man se at mange av artiklene ser først på den digitale tid som noe positivt. Petersons artikkel ser på digitalisering som noe positivt, som kan gi samfunnet nye muligheter for mer effektivitet i jobb og samhandling (Petersons, 2024, s. 1). Artikkelen til Mosteanu, ser på digitalisering som en mulighet for bedrifter, på grunn av at det kan endre organisasjonsstrukturen til å bli mer effektiv for å overkomme utfordringer som ikke kunne blitt håndtert tidligere (Mosteanu, 2020, s. 278). Saeed, et al., fokuserer på digital transformasjon, der man omgjør organisasjonsstrukturen til å bli mer digitalisert, ved å implementere IT til flere av organisasjonsprosessene, som skaper mange muligheter for en organisasjon (Saeed, et al., 2023, s. 1). Artikkelen til AlSalem, et al., i tillegg til artikkelen til Lee ser på cybersikkerheten innenfor et spesifikt digitalt system, IoT. Artikkelen til Lee ser på IoT som noe positivt, som kan hjelpe drive nye prosesser i bedriften (Lee, 2020, s. 1), mens AlSalem, et al., ser mer på truslene ved IoT (AlSalem, et al., 2023).

Videre var det interessant å se hvilke problemer de så innen de forskjellige digitale enhetene. Selv om de ser på at den digitale tid som noe som gir mange muligheter, ser de videre på sårbarheter og trusler de også kan bringe. Petersons viser til at selv med alle mulighetene som digitalisering gir, kommer det også mange cybertrusler (Petersons, 2024, s. 1). Det samme gjør artikkelen til Mosteanu, digitalisering gir muligheter, men utsetter også bedrifter for farer innen cyberspace (Mosteanu, 2020, s. 278). Artikkelen til Lee og AlSalem, et al., ser på trusler mot IoT, på grunn naturen til systemet, der det er mange systemer som er koblet mot hverandre og dersom ett system blir utsatt for cybertrusler, kan de andre systemene også bli utsatt for samme cybertrusler (Lee, 2020, s. 1). Artikkelen til Saeed, et al., ser på hvordan digital transformasjon skaper sårbarheter for cybersikkerheten, på grunn av de nye teknologiene som blir implementert i prosessen (Saeed, et al., 2023). Etter denne litteraturgjennomgangen kan man gå videre til å analysere artiklene dypere med å en tematisk analyse hvor man setter artiklenes tema og budskap inn i en tabell, for så å se på konkrete problemer og løsninger.

3.3 Tematisk analyse og kvalitativ metode

Tematisk analyse er en metode for å analysere kvalitativ data. Her søker man etter den samme ideen eller tema i de forskjellige dataene man samler, og det sies at det er en type kvalitativ metode (Riger & Sigurvinsdottir, 2016, s. 33). Kvalitativ metode er relevant

dersom man har en eksplorerende problemstilling som trenger en metode som får frem mye nyanser, med konsentrasjon om noen få enheter (Jacobsen, 2022, ss. 66-67). Måten oppgaven tar for seg en tematisk analyse er i form av en tabell for å vise tema og budskap fra litteraturstudie.

4 Analyse og resultat

Analysen av artikkelen blir gjennomført som en tematisk analyse for å vise til tema og budskap i artiklene, ved hjelp av sitater tatt direkte fra artiklene. Først ble alle artiklene lest, deretter ble tema valgt ut ifra alle artiklene. Disse temaene er trusler og utfordringer, cybertrusler og løsninger. Temaene ble valgt ut ifra problemstillingen, hvordan man kan forebygge cybertrusler. For å vise til tema ble det tatt ut flere sitater, og deretter funnet budskapet i disse sitatene. Etter å ha lest alle artiklene, funnet tema, relevante sitater og budskap, ble dette satt opp i en tabell, se tabell 2.

Tabell 2: Analyse tabell

Artikler	Tema	Sitat	Budskap
[1] (Petersons, 2024)	**Trusler og utfordringer.**	"Emerging technologies such as artificial intelligence (AI) and machine learning (ML), blockchain… have the potential to both enhance and challenge cybersecurity" (Petersons, 2024, s. 3) "blockchains systems are not immune to security vulnerabilities…" (Petersons, 2024, s. 3) "ransomware incidents have also become increasingly prevalent, with	Ny teknologi som egentlig skal hjelpe organisasjoner med å oppdage og forebygge cybertrusler og -angrep, er selv sårbare for angrep, og kan bli lurt og manipulert av angripere for at de skal unngå oppdagelse. Viser til to spesifikke cybertrusler som har blitt mer relevant med økningen til digitalisering, «ransomware incidents» og «supply chain attacks»

		cybercriminals… extort money…" (Petersons, 2024, s. 2) "Supply chain attacks have emerged as a particularly concerning trend…" (Petersons, 2024, s. 2)	
	Løsninger	"AI and ML technologies offer powerful tools for detecting and mitigating cyber threats… Blockchain… hold promise for enhancing cybersecurity… immutable record-keeping… improve data integrity, authentication, and access control." (Petersons, 2024, s. 3) "Human factors play a crucial role in cybersecurity, as individuals' knowledge, attitudes, and behavior can either enhance or undermine security measures" (Petersons, 2024, s. 4)	Løsningene kan være med nyere teknologi slik som kunstig intelligens, maskin læring og Blockchains på grunn av at disse kan oppdage og forebygge angrep i tillegg til å forbedre cybersikkerheten med bedre teknikker. Ser på hvordan risikovurderinger og trussel intelligens kan hjelpe med å identifisere og prioritere cybersikkerhets risikoer. Viser til hvordan menneskelig holdning og oppførsel har mye å si for cybersikkerheten, og det er derfor viktig å trene denne holdningen for å styrke sikkerheten.
[2] (Mosteanu, 2020)	**Trusler og utfordringer**	"Cyberattacks are usually aimed at accessing, changing, or destroying sensitive information;	Artikkelen viser til hva som motiverer et cyberangrep, å få tilgang, ødelegge, endre eller utpresse enheter.

		extorting money from users; or interrupting normal business processes" (Mosteanu, 2020, s. 279). "… a cyberattack can have many faces: phishing, … man in the middle…" (Mosteanu, 2020, ss. 280-281)	Cyberangrep kan komme på mange måter, «phishing» og «man in the middle» er to eksempler hvor kriminelle kan lure enheter og få tilgang til informasjon de ikke skal ha, slik at de ødelegger eller utpresser enhetene.
	Løsninger	"…the importance of redesigning the organizational structure for any business, giving more attention to cyber-security, and to employ specialized personal, able to identify and develop a solution for data security and cyber transformation" (Mosteanu, 2020, s. 284)	Kan løse dette ved en omorganisering på organisasjonsstrukturen, som fokuserer mer på cybersikkerhet. Her er det også viktig med ansatte som er i stand til å oppdage trusler og som kan løse dem dersom de oppstår.
[3] (AlSalem, Almaiah, & Lutfi, 2023)	**Cybertrusler**	"Cybersecurity attacks can threaten the power grid and water supply… concerns about eavesdropping… created concerns regarding the impacts and consequences on the economy… health sector has suffered from cyberattacks…	IoT er sårbar for angrep mot forskjellige enheter som for eksempel, smarthjem, finanssektor og helsesektoren. Med forskjellige konsekvenser som kan oppstå dersom de blir utsatt for angrep.

		include data loss…" (AlSalem, et al., 2023, s. 11) «… IoT devices and systems face a wide range of cyber threats, with privacy issues and cybercrimes standing out as the most significant concerns…" (AlSalem, et al., 2023, s. 13). "top two issues concerning the cybersecurity of IoT… denial-of-access attacks… man-in-the-middle attacks" (AlSalem, et al., 2023, s. 13)	IoT har mange trusler, med hovedfokus på trusler mot personvern og cyberkriminalitet. To eksempler på cyberangrep på IoT er «denial of access» og «man-in-the-middle», hvor kriminelle enten overbelaster systemer eller får tilgang eller manipulerer sensitiv informasjon.
	Løsninger	"Integration of artificial intelligence (AI)… has emerged as a promising technique in addressing the challenges of IoT cybersecurity… particularly machine learning algorithms, in detecting and mitigating cybersecurity threats in IoT environments… Blockchain technology for enhanced security… be providing decentralized and tamper-resistant data storage and communication… reduce the risk of data manipulation and	Ny teknologi som kunstig intelligens og blockchains kan styrke cybersikkerheten til organisasjoner. På grunn av muligheten kunstig intelligens har for å lære seg mønster til cybertrusler, og blockchains mulighet til å redusere risikoen for manipulasjon og uautorisert tilgang.

		unauthorized access" (AlSalem, et al., 2023, s. 13)	
[4] (Saeed, Altamimi, Alkayyal, Alshehri, & Alabbad, 2023)	**Cybertrusler**	"Cybercriminals may take advantage of vulnerabilities in digital technologies…" (Saeed, et al., 2023, s. 2) "attacks usually aim to assess, change, org destroy sensitive information; extort monetary benefits from users…" (Saeed, et al., 2023, s. 2) "financial sector… are exposed to online identity theft, computer system damage, and hacking attempts… health sector… cybersecurity… deals with patient data privacy and the security of medical devices" (Saeed, et al., 2023, ss. 4-5).	Cyberkriminelle kan utnytte mangelen på cybersikkerhet, organisasjoner har når de er under den digitale transformasjonen, ved at de angriper de nye teknologiene før cybersikkerheten har blitt etablert. Cyberangrep har som regel bakgrunn ved å få tilgang, ødelegge, endre eller utpresse enheter og bedrifter. Det er forskjellige sektorer som kan være sårbare for cyberangrep, disse er finans og helse sektorene.
	Løsninger	"machine learning approaches can help identify malicious traffic in network which can help identifying cyber threats proactively." (Saeed, et al., 2023, s. 14).	Viser til hvordan ny teknologi som maskin læring kan identifisere ondsinnede mønster innen enheter og data, slik at de også kan oppdage sårbarheter og cybertrusler.

		"organizations need a well-planned organizational cybersecurity strategy documenting the processes for cybersecurity…" (Saeed, et al., 2023, s. 15). "… it is essential for organizations undergoing DT to consider the human factor in cybersecurity… providing regular training and awareness programs…" (Saeed, et al., 2023, s. 15).	Organisasjoner trenger også en god plan for cybersikkerheten, hvor de dokumenterer og lager strategier for god cybersikkerhet. Dette ved å lage en plan om forberedelser, utplassering og overvåking. Det er også viktig med å tenke på den menneskelige faktoren innen cybersikkerhet. Derfor er det også viktig å utføre trenging og bevisthetstrening for ansatte i organisasjoner for å forbedre cybersikkerheten.
[5] (Lee, 2020)	**Cybertrusler** **Løsninger**	"rapid increase of cyberattacks is in part due to phenomenal growth of IoT devices… security management of the IoT is challenging due to the dynamic… nature of the connection between devices" (Lee, 2020, s. 1) "The four-layer IoT cyber risk management framework is proposed to help IoT security managers develop a cost-effective cybersecurity risk management plan… IoT	IoT kobler mange elektroniske systemer til hverandre som skaper muligheter for cybertrusler og -angrep. I tillegg lager den store økningen av enheter i IoT større sårbarheter og gjør det vanskeligere for cybersikkerheten. Cybersikkerhet-risikostyring er en måte å forebygge sårbarheter innen cybersikkerheten til IoT, for å stoppe angrep og trusler som kan oppstå. Artikkelen deler

		cyber ecosystem layer, an IoT cyber infrastructure layer, an IoT cyber risk assessment layer, and an IoT cyber performance layer" (Lee, 2020, ss. 6-7).	det opp i fire faser: the IoT cyber ecosystem layer, the IoT cyber-risk infrastructure layer, the IoT cyber-risk assessment layer, og the IoT cyber performance layer

4.1 Resultat

Da tema, sitat og budskap er satt inn i tabellen, kan det her bli satt opp i en mer utfyllende tekst for å vise hvilke resultater som ble funnet etter litteraturgjennomgangen og den tematiske analysen. Her vil de mest nevnte truslene, sårbarhetene og løsningene bli presentert.

4.1.1 Trusler og sårbarheter

For å kunne vite hvordan man skal forebygge trusler og sårbarheter innen cybersikkerheten må man først vite hvilke trusler og sårbarheter det er. Cybertrusler er utviklende og det kan trekkes en kobling mellom utviklingen til truslene og utviklingen av teknologi (Petersons, 2024, s. 2). Cybertruslene og sårbarhetene som ble vist til i de fleste artiklene var de digitale systemene og teknologiske enhetene som er koblet til internett og andre enheter. Disse enhetene ble vist til å være det som kalles for ny teknologi (Mosteanu, 2020, s. 278), som kunstig intelligens og maskin læring. Disse enhetene er laget for å oppdage og forebygge cybertrusler, men de er også sårbare for de samme cyberangrepene de skal oppdage. De kan bli manipulert eller påvirket av cyberangrep som bruker bedre og mer avansert teknologi enn det kunstig intelligens og maskin læting bruker. Det vises også til hvordan blockchain, et annet system som er laget for å redusere risikoen for cyberangrep er selv også sårbar for angrep (Petersons, 2024, s. 3). Det ble også oppdaget at cyberkriminelle vil utnytte sårbarhetene til organisasjoner når de er midt i den digitale transformasjonen (Saeed, et al., 2023, s. 2). Her er det et par sektorer som er spesielt sårbare for angrep. Finans-sektoren som er sårbar mot trusler for identitetstyveri, datasystem skader, og forsøk på hacking, og helse-sektoren hvor de er sårbare mot trusler på personvern og sikkerhet, og flere sektorer med lignende sårbarheter (Saeed, et al., 2023, ss. 4-5).

Cyberangrep er gjort for å få tilgang til, forandre eller ødelegge sensitiv informasjon, utpresse penger eller forstyrre vanlig produktivitet (Mosteanu, 2020, s. 279). Eksempler på cyberangrep som organisasjoner kan bli utsatt for kan være «ransomware» hendelser, hvor cyberkriminelle utpresser penger fra personer og organisasjoner ved å kryptere viktig data til de får pengene. «Supply chain attacks», hvor de angriper tredjeparter til organisasjoner for å få tilgang til selve organisasjonens systemer og data (Petersons, 2024, s. 2). «Phishing» hvor man etterligner brukernavn, passord og mailadresse som legitimt, og kan inneholde linker som fører til virus (Bhavsar, et al., 2018, s. 27). «Man in the middle» angrep hvor cyberkriminelle lytter på nettverkstrafikken til to enheter uten at enhetene vet om det, dette kan gi den kriminelle tilgang til sensitiv data og muligheten til å manipulere datastrømmen til enhetene (Jain, et al., 2016, s. 277). «Denial-of-access» angrep, hvor man sender meldinger med sensitiv data for å utpresse svakheter og sårbarheter, eller sender mange meldinger til systemet, for å overbelaste systemet slik at det bryter sammen (Kumar, 2016).

Det ble også sett på cyberangrep innen IoT. Her ses det at personvernssikkerhet og cybersikkerhetsutfordringer er et av hovedproblemene ved IoT. Cyberangrep kan påvirke både smarthjem, smart-byer, økonomi og helsetjeneste, ved strømforsynings angrep og tjuvlytting (AlSalem, et al., 2023, s. 11). Dersom bedrifter blir utsatt for cyberangrep kan dette føre til problemer for bedriftens omdømme, økonomien og bedrifts operasjonen. Det kan kobles til de økende antall enheter som kobler seg til IoT og den dynamiske naturen til alle enhetene gjør det vanskelig for cybersikkerheten i IoT (Lee, 2020, s. 1).

4.1.2 Løsninger til bedre cybersikkerhet

Videre kan man se på hvilke løsninger artiklene kommer med for å forebygge cybertrusler og sårbarheter.

De nye teknologiene bringer med seg mange trusler og sårbarheter, men de kan også være et godt verktøy for å oppdage cybertrusler (Petersons, 2024, s. 3). Kunstig intelligens og maskin læring kan oppdage cybertrusler på grunn av at de kan lese store mengder data, og lete etter mønster innen cybertrusler og -angrep. Maskin læring kan være en løsning på å identifisere cybertrusler ved å se på ondsinnede mønstre ved store mengder data (Saeed, et al., 2023, s. 14). Blockchains kan forbedre autentifisering, adgangskontroll, i tillegg til at den lagrer store mengder data som kan brukes for bedre cybersikkerhet (Petersons, 2024, s.

3). Den kan også redusere risikoen for data-manipulasjon og uautorisert tilgang (AlSalem, et al., 2023, ss. 13-14).

Omorganisering kan ha betydning for cybersikkerheten, ved at det blir fokusert på å implementere IT-team som kan fokusere på cybersikkerheten til organisasjoner (Mosteanu, 2020, s. 281). I tillegg er det også viktig med god opplæring av ansatte for å ha god cybersikkerhet. Dette er fordi menneskelig holdning til sikkerheten og hvordan man utøver sikkerheten kan påvirke om man har god eller dårlig cybersikkerhet (Petersons, 2024, s. 4). Med god opplæring og bevissthetstrening for ansatte i organisasjoner (Saeed, et al., 2023, s. 15), i tillegg til trening i programmer som kan oppdage cybertrusler, sterke passord, og å alltid forbedre og oppdatere sikkerheten kan man utvikle en god cybersikkerhet som er minst mulig sårbar for cyberangrep (Petersons, 2024, s. 4).

Det er viktig å lage en god cybersikkerhets strategi, hvor man dokumenterer prosesser ved sikkerheten. Det kan her fokuseres på tre faser, forberedelser, utplassering og overvåking, i overvåkningsfasen ser man hele tiden etter sårbarheter som kan oppstå (Saeed, et al., 2023, s. 15). Organisasjoner burde også fokusere på cyber-risikostyring og trussel-intelligens for å kunne identifisere og prioritere cybersikkerhets-risikoer. Dette ved å overvåke trussel landskapet og analysere disse for mulige trusler og sårbarheter, slik at man har kunnskap om cybertrusler i forkant av cyberangrep (Petersons, 2024, s. 4). Dette er en prosess for å redusere cybersikkerhets-risiko, også kalt for cyber-risikostyring. En av artiklene i tabell 2 viser også til fire lag ved cyber-risikostyring i forhold til IoT; IoT cyberrisiko økosystem (the IoT cyber ecosystem layer), IoT cyberrisiko-infrastruktur (the IoT cyber-risk infrastructure layer), IoT cyberrisiko-vurdering (the IoT cyber-risk assessment layer), og IoT cyberrisiko-ytelse (the IoT cyber preformance layer). Hvor spesielt IoT cyberrisiko vurderingsprosessen identifiserer, kvantifiserer og prioriterer IoT-cyberrisiko (Lee, 2020, ss. 6-7).

4.1.3 Konklusjon

Etter en gjennomgang og analyse av artiklene, viser de alle til trusler, sårbarheter og løsninger for cybersikkerheten i en rask utviklende digital tid. De fleste artiklene så på ny teknologi som en stor grunn til sårbarheter innen cybersikkerheten, kunstig intelligens, maskin læring, blockchains og IoT. Grunnen til denne sårbarheten var på grunn av

sammenkoblingen mellom flere teknologier og enheter, i tillegg til muligheten for å manipulere eller lure teknologien til å ikke oppdage cybertrusler eller -angrep. Selv med sårbarhetene som kom med de nye teknologiene, var de også for mange av artiklene en løsning på cybersikkerhet. Kunstig intelligens og maskin læring kan brukes for å oppdage og begrense skadene til cybertrusler og -angrep. Blockchains kan redusere risikoen for at datasystemer blir manipulert. Menneskelige holdninger kan også påvirke cybersikkerhet, og det er viktig med god opplæring innen cybersikkerhet. Det kan også lages gode planer for cybersikkerheten der man fokuserer på cybersikkerhets-risikoer, hvor man finner relevante risikoer og deretter løsninger på dem.

5 Diskusjon

I denne delen skal det fokuseres på hvordan resultatene til den tematiske analysen kan sees i sammenheng med de teoretiske perspektivene. Dette blir gjort for å se hvordan resultatene og perspektivene kan kobles til problemstillingen. I tillegg sees det om de kan svare på spørsmålet, hvordan kan man forebygge de ulike sårbarhetene og truslene som oppstår mot cybersikkerheten i den utviklende digitale tiden?

5.1 Trusler og sårbarheter

Gjennom litteraturgjennomgangen ble det vist til viktigheten for god cybersikkerhet i en utviklende digital tid, hvor truslene blir stadig mer alvorlig og avansert. De tidligere studiene viser til forskjellige trusler og sårbarheter for cybersikkerheten. De mest nevnte truslene er angrep og hendelser der cyberkriminelle får tilgang til sensitiv informasjon. Artiklene nevnte også at den største grunnen til cyberangrep er for å få tilgang, ødelegge eller endre sensitiv informasjon, slik at de kan utpresse penger eller forstyrre vanlig produktivitet. Deretter viste artiklene hvordan angrepene kunne få konsekvenser for mange ulike sektorer, noen av sektorene som ble nevnt var finans- og helsesektoren. Disse truslene og sårbarhetene blir vist for å vise viktigheten med god cybersikkerhet, slik at det skal oppfordre bedrifter og organisasjoner med å implementere gode prosedyrer og planer for cybersikkerheten. Videre kan man se på hvordan man kan bygge på løsningene til de tidligere studiene. Dette kan gjøres ved å koble resultatene med de to teoretiske perspektivene som ble nevnt tidligere i oppgaven.

5.2 Beredskapsløsninger

Resultatet på analysen viser til hvordan man kan dokumentere cybersikkerhetsprosesser for å lage en bedre cybersikkerhetsstrategi. Hvor man også fokuserer på å overvåke sårbarhetene som kan oppstå for å kunne implementere bedre sikkerhet for de nye oppdagede sårbarhetene (Saeed, et al., 2023, s. 15). Disse prosessene blir nærmere forklart i det siste avsnittet til 5.2, her i dette avsnittet fokuseres det på hvordan selve dokumentasjonen kobles til beredskap. Fasene kan først kobles til beredskapshjulet ved at man er i den tredje fasen, «beredskapsplan». Den kommer etter at man har laget to analyser, risikoanalyse og beredskapsanalyse. Dokumentasjonen man skriver skal forklare hvem som har ansvaret og hvilke beslutninger man skal ta dersom en uønsket hendelse skjer (Engen, et al., 2021, s. 326). Her lager man en plan over hva som må gjøres ved å bestemme hvilken type beredskap som må brukes. Man etablerer også en beredskapsstruktur sammen med analysene for å se hva man burde øve og trene på for å være klare, slik at responsene som er neste fase er planlagt, koordinerte og effektive (Engen, et al., 2021, s. 326).

Resultatet viser også hvordan menneskelig holdning kan påvirke cybersikkerheten til organisasjoner, for eksempel kan det vises til at menneskelig holdning enten kan styrke eller såre cybersikkerheten. (Petersons, 2024, s. 4). Det er derfor viktig å tenke over den menneskelige faktoren ved cybersikkerheten, og dermed viktigheten med god opplæring og bevissthetstrening (Saeed, et al., 2023, s. 15). Dersom man ser dette med et beredskapssyn, er dette del av aktiviteten til beredskap (Engen, et al., 2021, s. 321). Det er viktig å øve på krisesituasjoner og det å kjenne igjen en trussel eller sårbarhet, på grunn av med øvelse blir man mer bevist og klare når en uønsket hendelse skjer. Det er også viktig å vite at beredskap er ikke noe man kan være utlært i, de situasjoner man trener på trenger ikke være de situasjonene man faktisk møter på. Det sagt trenger man treningen for å være forberedt på lignende situasjoner (Sommer, et al., 2020, s. 39).

Videre kan det vises til de fire fasene ved cybersikkerhetsprosessen, overvåkning, strategi, forberedelser og utplassering (Saeed, et al., 2023, s. 15). Dette kan også kobles til de forskjellige fasene ved beredskap, hvor man lager en strategi ved å overvåke den trusselen man har. Dette kalles at man utfører en risikovurdering for å kartlegge risikoen som eksisterer og med det skape et risikobilde. Etter dette lager man en strategi med en beredskapsanalyse, hvor man tar truslene fra risikoanalysen og finner de uønskede

hendelsene man ønsker at beredskapen skal stoppe. De to analysene skal sammen kartlegge farene som man må være forberedt på. Videre er det å lage en beredskapsplan en del av forberedelsen der man bestemmer hvor, når, hvem og hvordan beredskapen skal bli utført. I planleggingsfasen bestemmes også utplasseringen for beredskapen som skal utføres som en respons til den uønskede hendelsen (Engen, et al., 2021, s. 321). Dette kan videre kobles til det neste teoretiske perspektivet som oppgaven skal bruke, cyber-risikostyring.

5.3 Cyber-risikostyring løsninger

Risikostyring blir inkludert for det kan bygge videre på punktene ved risikovurdering og risikoanalyse, som er viktige deler av beredskap.

Resultatet av analysen viser til at det burde fokuseres på cyber-risikostyring for å kunne identifisere og prioritere cybersikkerhetsrisiko. Dette innebærer å overvåke og analysere trussel landskapet for å kunne oppdage mulige cybertrusler eller sårbarheter (Petersons, 2024, s. 4). Det kan fokuseres på fire lag innen cyber-risikostyring; (i) cyberrisiko-økosystem, hvor man overvåker og evaluerer cyberlandskapet. Man ser hvilke trusler og sårbarheter som er innen cyberspace, for å deretter kommuniseres resultatene til de andre lagene. (ii) Cyberrisiko-infrastruktur, hvor organisasjoner analyserer hvordan den nåværende cybersikkerhetens infrastruktur er, ved å analysere cybersikkerhets teknologien, personers ansvar og organisasjonenes retningslinjer. (iii) Cyber-risikovurdering, hvor man identifiserer cybertrusler og sårbarheter, bestemmer hvordan man skal prioritere cybertrusler og hvordan man skal fordele ressursene til cybersikkerheten. (iv) Cyberrisiko-ytelse, hvor teknikker for cybersikkerheten er laget, overvåket og kontrollert, og hvor man stadig forbedrer aktivitetene for god cybersikkerhet (Lee, 2020, ss. 6-7). Fasene kan kobles likt til cyber-risikostyring, her handler det om å identifisere risiko lignende det man gjør i cyberrisiko-økosystemet. Neste steg er å vurdere cyberrisikoen slik man gjør i cyber-risikovurderingen. Det siste er å lage løsninger for å redusere risikoen, lignende det man gjør i cyberrisiko-ytelses fasen.

Det man også kan gjøre dersom man skal bruke cyber-risikostyring er å identifisere hvilken cyberrisiko som kan oppstå (Refsdal, et al., 2015, ss. 42-43), og med dette kan man finne ut hvilken data type man skal beskytte. De eksemplene som har blitt vist igjennom artiklene er at finans- og helsesektoren er sårbare mot cyberangrep, og det kan derfor tenkes at det er

snakke om høyrisikodata man ønsker å beskytte. (i) Da kartlegger man først hvor i organisasjonen høyrisikodataen ligger, og med det kan man forutse hvor cyberrisikoen kan oppstå. (ii) Etter dette vurderes risikoen (Refsdal, et al., 2015, ss. 42-43), om den er ondsinnet eller ikke ondsinnet. Igjen er de fleste eksemplene nevnt i artikkelen angrep hvor cyberkriminelle ønsker tilgang til sensitiv informasjon eller utpresser penger fra organisasjoner. Det kan derfor tenkes at risikoen de fleste har er ondsinnet cyberrisiko. (iii) Med kunnskapen om hvor og hvilken cyberrisiko man skal håndtere kan man lage sårbarhets- og trussel modeller for å se sannsynligheten for cybertrusler og sårbarhetene. (iv) Deretter kan man implementere kommunikasjon og trening for å få en god og effektiv cybersikkerhet, (v) i tillegg kan man dokumentere prosessen, truslene og sårbarhetene for å hele tiden fornye modellene og cyber-risikostyrings prosessen.

Prosessene nevnt i cyber-risikostyrings løsningene, kan settes i lignende figurer som beredskapshjulet, som kan vise hvordan man kan knytte sammen prosessene både fra beredskap og cyber-risikostyring for å utvikle den beste cybersikkerheten. Figurene som er referert til her ligger under vedlegg, der Figur 1 er Engen, et al., sitt beredskapsperspektiv, Figur 2 er Lee sin cyber-risikostyrings lag og Figur 3 er Refsdal, et al., sine cyber-risikostyringsprosesser.

Fase 1 i figuren til Lee handler om å overvåke og evaluere cyberlandskapet. Dette er likt fase 1 i figuren til Refsdal, et al., om å kartlegge hvor og hvilke risikoer som oppstår. Fase 2 i Lee sin figur viser videre hvordan man burde analysere nåværende cybersikkerhets infrastruktur, noe de andre figurene ikke nevner. Første fase i Engen, et al., sin figur om risikoanalyse er lik fase 3 i Lee sin figur om risikovurdering og fase 2 i Refsdal, et al., sin figur om å vurdere risiko. Engen, et al., kartlegger den risikoen som allerede eksisterer, Lee identifiserer cybertrusler og prioriterer truslene, Refsdal, et al., ser om det er ondsinnet eller ikke-ondsinnet cyberrisiko. Engen, et al., lager i fase 2 en beredskapsanalyse og beredskapsplan, noe de andre figurene ikke gjør, men Refsdal, et al., lager i stedet sårbarhetsmodeller for å se sannsynligheten til risiko i sin fase 3. Deretter etablerer Engen, et al., i fase 3 beredskapsstruktur og ressurser ved øvelser og trening, noe også Refsdal, et al., gjør i fase 4 ved implementering av kommunikasjon og trening. Engen, et al., ser i fase 5 på respons ved beredskap, og i fase 6 evalueres beredskapen som blir grunnlaget til ny og forbedret beredskap. Lee ser også i fase 4 på cybersikkerhets-ytelse, hvor sikkerhets teknikkene blir overvåket for å bli forbedret. Refsdal, et al., ser i fase 5 på hvordan man

burde dokumentere prosessen for å kontinuerlig forbedre sikkerheten. Figurene er forskjellige ved at de har ulike faser, men det er en del likheter i noen av fasene. Det som er ulikt er at de fokuserer på forskjellige ting i like faser, eller at de har faser de andre figurene ikke har. Det er derfor viktig å ha en blanding av både beredskap og cyber-risikostyring for å utvikle best cybersikkerhet.

5.4 Cybertrusler mot Tolletaten

Nevnt innledningsvis i oppgaven er det interessant å se hvordan resultatene fra analysen kan påvirke en organisasjon. Resultatet viser hvordan cybersikkerheten påvirkes av en omorganisering for å gjøre organisasjoner mer digitaliserte. Det vises til hvordan organisasjoner burde prioritere å implementere gode IT-team som skal fokusere på cybersikkerheten (Mosteanu, 2020, s. 281). Det vises også til muligheten cyberkriminelle har for å angripe teknologien og systemene før de får implementert god cybersikkerhet for de nye systemene (Saeed et al., 2023, s. 2). En relevant organisasjon å se på for å forklare dette ytterligere er Tolletaten. Det ble nevnt innledningsvis at Tolletaten har et samfunnskritisk oppdrag, og at de i 2016 fikk et oppdrag om å utføre en omorganisering for å fokusere på digitalisering. Denne digitaliseringen inneholdt implementering av et nytt teknologisk system Digitoll. På grunn av denne omorganiseringen og implementering av ny teknologi, er det viktig å se på hva dette kan bety for cybersikkerheten hos etaten. Det kan bli gjort ved å se på sårbarhetene og truslene beskrevet i forrige kapittel, for så å se på relevante løsninger etaten burde fokusere på under denne omorganiseringen.

Dersom Tolletaten blir utsatt for et cyberangrep kan det få store konsekvenser på samfunnet, på grunn av det samfunnskritiske oppdraget. Eksempel på dette kan være dersom de blir utsatt for et «denial of access»-angrep, som kan føre til at de mister tilgang til systemene sine. Konsekvensen til dette kan bli at prosessene innen etaten stopper, og med det kan også hele grenseovergangen stoppe. Et annet angrep de kan bli utsatt for er «man in the middle» angrep, hvor de kan miste sensitiv informasjon som kan få konsekvensen med at omdømmet til etaten blir skadet ved at viktig informasjon blir tapt. I tillegg kan kriminelle få personlig eller bedrifts informasjon ved å ta informasjonen fra Tolletaten, som de kan selge på ulovlige sider eller bruker for å utpresse penger fra bedrifter. Det er derfor viktig at tolletaten har god cybersikkerhet og er klar over cyberrisiko ved å være i en digital transformering. De burde være oppmerksomme på at den nye teknologien kan skape sårbarheter dersom det

ikke er implementert god cybersikkerhet innen teknologien. En av løsningene de kan se på er å i tillegg til Digitoll implementere annen teknologi som kunstig intelligens, maskin læring og blockchains for å oppdage sårbarheter og trusler, så lenge disse også er implementert med god cybersikkerhet. God opplæring og bevissthetstrening om god cybersikkerhet i tillegg til flere ressurser til IT-team, er også viktig å vurdere når de digitaliserer etaten. Det viktigste blir da å tenke beredskap og cyber-risikostyring hvor de stadig leter etter sårbarheter og risiko, og kontinuerlig jobber med å forbedre og teste cybersikkerheten.

5.5 Begrensninger med metoden

Det er svakheter ved en litteraturstudie, den største er at det er krevende på en kort tid. Da man søker etter data får man mange treff, også etter avgrensninger, og man har en tidsbegrensning når man går igjennom treffene. På grunn av at dette er en bacheloroppgave er det liten tid å lese artiklene i dybde og det ble i tillegg laget en grense på hvor mange artikler som skulle være i oppgaven. Dette kan føre til at oppgaven kun får en vinkel, den forfatter selv mener er relevant og der motstridende data kanskje ikke kommer frem i oppgaven. Styrken med denne metoden er at man får forskning fra tidligere studier som er relevant for oppgaven, i tillegg til at det er mange artikler man kan bruke. Denne oppgaven bruker fem artikler, som betyr at det er mye informasjon og data man kan ta ut fra dem og flere synspunkter på samme tema. Det kan vises ved at noen av artiklene mente ny teknologi var en grunn til cybertrusler og sårbarheter, mens andre mente at de var en løsning for å styrke cybersikkerheten.

En annen ting man må se på er at alle artiklene er skrevet på engelsk, mens denne oppgaven er skrevet på norsk. Dette kan bety at det har blitt oversatt feil eller at det er misforståelse i oversettingen slik at ordene mister sin originale mening. Derfor har denne oppgaven først skrevet ordene og de teoretiske begrepene på norsk, for å så sette dem inn på engelsk i parenteser for å vise originalmeningen. I tillegg er alle artiklene referert slik at leser kan selv gå inn å lese dem for å få tema på originalspråket.

Resultats var både forutsigbart og overaskende. Det var overaskende mange studier med samme konsept og tema som denne oppgaven fokuserer på, men ikke mange som ser på det med de teoretiske perspektivene denne oppgaven har. Det var også overaskende at de

samme systemene og teknologien som skaper så mange sårbarheter til organisasjoner også kan være en del av løsningen. Det var derimot ikke overaskende at alle artiklene var enig i at cybersikkerhet er viktig spesielt i en utviklende digital tid hvor man blir mer avhengig av teknologi.

6 Konklusjon

Hensikten til denne oppgaven var å finne måter man kan forebygge cybertrusler og sårbarheter mot cybersikkerhet i en utviklende digital tid. Oppgaven ble løst ved bruk av litteraturstudie og en tematisk analyse av fem artikler. Resultatet som ble funnet var at ny teknologi som kunstig intelligens, maskin læring og blockchains er både en sårbarhet og en løsning, og likt som alt annet digitalt, trenger de god cybersikkerhet for å kunne brukes uten risikoen for cyberangrep. Organisasjoner burde fokusere på beredskap og cyber-risikostyring for å kontinuerlig forbedre cybersikkerheten, og burde fokusere på både opplæring og bevissthetstrening i tillegg til cybersikkerhetsstrategiene for å få den best mulige cybersikkerheten. Det sagt vil alltid cyberrisiko og cyberangrep oppstå på grunn av naturen og utviklingen til teknologien.

6.1 Anbefaling for videre forskning

Cybertrusler og angrep utvikler seg hele tiden og blir mer effektiv og avansert, derfor er det viktig at man fortsetter med slike studier og mer forskning for å finne nye og bedre løsninger for å forsvare organisasjoner mot cyberangrep. Det burde fortsettes å forske på hvordan ny teknologi som kunstig intelligens og maskin læring kan forbedres for å styrke cybersikkerheten. I tillegg burde det videre forskes på hvordan beredskap og cyber-risikostyring kan styrke cybersikkerheten hos organisasjoner for å fortsette å implementere bedre prosesser og systemer innen cybersikkerhet. Cybersikkerhet må derfor være lik cybertrusler, alltid i endring og forbedring for å bli mer effektiv og avansert.

Referanser

Alman, S., & Hirsh, S. (2019). *Blockchain* (10-25 ed.). American Library Association. Retrieved from https://ebookcentral-proquest-com.ezproxy.uis.no/lib/uisbib/detail.action?docID=6202109

AlSalem, T. S., Almaiah, M. A., & Lutfi, A. (2023). Cybersecurity Risk Analysis in the IoT: A Systematic Review. *Electronics, 12*(18), 1-19. doi:https://doi.org/10.3390/electronics12183958

Andersen, E., & Ragnvald, S. (2017). Hva er digitalisering? *Magma - Tidsskrift for økonomi og ledelse, 20*(6), 1-8. Retrieved from http://hdl.handle.net/11250/2569870

Andersen, E., & Sannes, R. (2018). Er du klar for digitalisering? *Praktisk økonomi og finans, 34*(3), 1-13. doi:https://doi.org/10.18261/issn.1504-2871-2018-03-04

Anjila P K, F. (2021). Artificial Intelligence. In J. Karthikeyan, T. S. Hie, & N. Y. Jin, *Learning outcomes of classroom research* (1 ed., p. 65). L Ordine Nuovo Publication.

Aven, T., Ben-Haim, Y., Andersen, H. B., Cox, T., Droguett, E. L., Greenberg, M., . . . Zio, E. (2018). Society for Risk Analysis Glossary. *Society for Risk Analysis (SRA)*, 4-9. Retrieved from https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing attacks. *International Journal of Computer Applications, 182*(22), 27. Retrieved from https://www.researchgate.net/profile/Shabnam-Sharma-2/publication/329716781_Study_on_Phishing_Attacks/links/5ef9867a92851c52d6069bf2/Study-on-Phishing-Attacks.pdf

Engen, O. A., Pettersen, K. A., Kruke, B. I., Lindøe, P. H., Harald, O. K., & Olsen, O. E. (2021). *Perspektiver på samfunnssikkerhet* (2 ed.). Cappelen Damm akademisk.

Finansdepartementet, D. k. (2021). *Statsbudsjett 2022 - Tolletaten - tildelingsbrev.* Regjeringen. Retrieved from https://www.regjeringen.no/contentassets/5bafee03762f4ed8bb97f52472ce60ab/2022-tolletaten-tildelingsbrev.pdf

Fosse, E., Hatlen, S., Madsen, S., Melber, H. O., Nassehi, D., Riegler, M., & Lovett, H. (2018). Kunstig Intelligens - muligheter, utfordringer og en plan for Norge. *Teknologirådet*, 7-19. Retrieved from https://web-backend.simula.no/sites/default/files/publications/files/rapport-kunstig-intelligens-og-maskinlaering.pdf

Freedman, L. F. (2023). Five steps to enhance digital risk management practices. *Trade Journal, 60*(6). Retrieved from http://ezproxy.uis.no/login?url=https://www.proquest.com/trade-journals/five-steps-enhance-digital-risk-management/docview/2826828946/se-2?accountid=136945

Haugom, L., Stenslie, S., & Vaage, B. H. (2019). *Etterretningsanalyse i den digitale tid - en innføring.* Fagbokforlaget.

Jacobsen, D. I. (2022). *Hvordan gjennomføre undersøkelse?* (4 ed.). Cappelen Damm AS.

Jain, K. A., Jain, M. V., & Borade, J. L. (2016). A survey on man in the middle attack. *International Journal of Science Technology & Engineering, 2*(09), 277. Retrieved from https://d1wqtxts1xzle7.cloudfront.net/44716087/IJSTEV2I9103-libre.pdf?1460611574=&response-content-

disposition=inline%3B+filename%3DA_Survey_on_Man_in_the_Middle_Attack.pdf&Expires=1714135633&Signature=WHqK6SYOGQdd5Y1BvzeSdelcvVK0tdci8~Qenav5oyygSeXQ6xGAz

Kumar, G. (2016). Denial of service attecks - an updated perspective. *Systems science & Control Engineering, 4*(1). doi:https://doi.org/10.1080/21642583.2016.1241193

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet, 12*(9), 1-21. doi:https://doi.org/10.3390/fi12090157

Lunde, I. K. (2019). *Praktisk krise- og beredskapsledelse- etablering av beredskap, potensialbasert beredskapsledelse, proaktiv stabsmetodikk* (2 ed.). Universitetsforlaget.

Mosteanu, N. R. (2020). Challenges for organizational structure and design as a result of digitalization and cybersecurity. *The business and Management review, 11*(1), 278-286. Retrieved from https://www.researchgate.net/profile/Hany-Hanna-2/publication/344793035_TOE_Model_Adoption_of_Block_Chain/links/5fecdaf1a6fdccdcb81ad7e3/TOE-Model-Adoption-of-Block-Chain.pdf?origin=journalDetail&_tp=eyJwYWdlIjoiam91cm5hbERldGFpbCJ9#page=288

Nasjonal-Sikkerhetsmyndighet. (2023). *Norge rammes av avanserte målrettede cyberangrep.* NSM.no. Retrieved from Norge rammes av avanserte målrettede cyberangrep - Nasjonal sikkerhetsmyndighet (nsm.no)

Petersons, E. (2024). Cybersecurity challenges in the era of digitalization. *SSRN*, 1-6. doi:https://dx.doi.org/10.2139/ssrn.4723047

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-Risk Management.* Springer International Publishing. doi:https://doi.org/10.1007/978-3-319-23570-7_3

Regjeringen. (2022). *Digitale angrep mot norske kommuner kan få store konsekvenser.* Regjeringen.no. Retrieved from – Digitale angrep mot norske kommuner kan få store konsekvenser - regjeringen.no

Regjeringen. (2023). *Departementer utsatt for dataangrep.* Regjeringen.no. Retrieved from Departementer utsatt for dataangrep - regjeringen.no

Riger, S., & Sigurvinsdottir, R. (2016). Thematic Analysis. In L. A. Jason, & D. S. Glenwick, *Handbook of Methodological approaches to community-based research* (p. 33). Oxford University Press.

Rognsaa, A. (2023). *Bachelor-oppgaven* (2 ed.). Universitetsforlaget.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for businesses Resilience: Issues and Recommendations. *Sensors, 23*(15), 1-20. doi:https://doi.org/10.3390/s23156666

Sommer, M., Pollestad, B., & Steinnes, T. (2020). *Beredskapsøving og -læring.* Fagbokforlaget.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *National Institute of Standards and Technology*, 1-55. Retrieved from https://sites.pitt.edu/~dtipper/2825/NIST_Risk.pdf

Stortinget. (2020). *IT-angrep mot Stortinget.* Stortinget.no. Retrieved from IT-angrep mot Stortinget - stortinget.no

Stortinget. (2021). *Stortinget utsatt for IT-angrep.* Stortinget.no. Retrieved from Stortinget utsatt for IT-angrep - stortinget.no

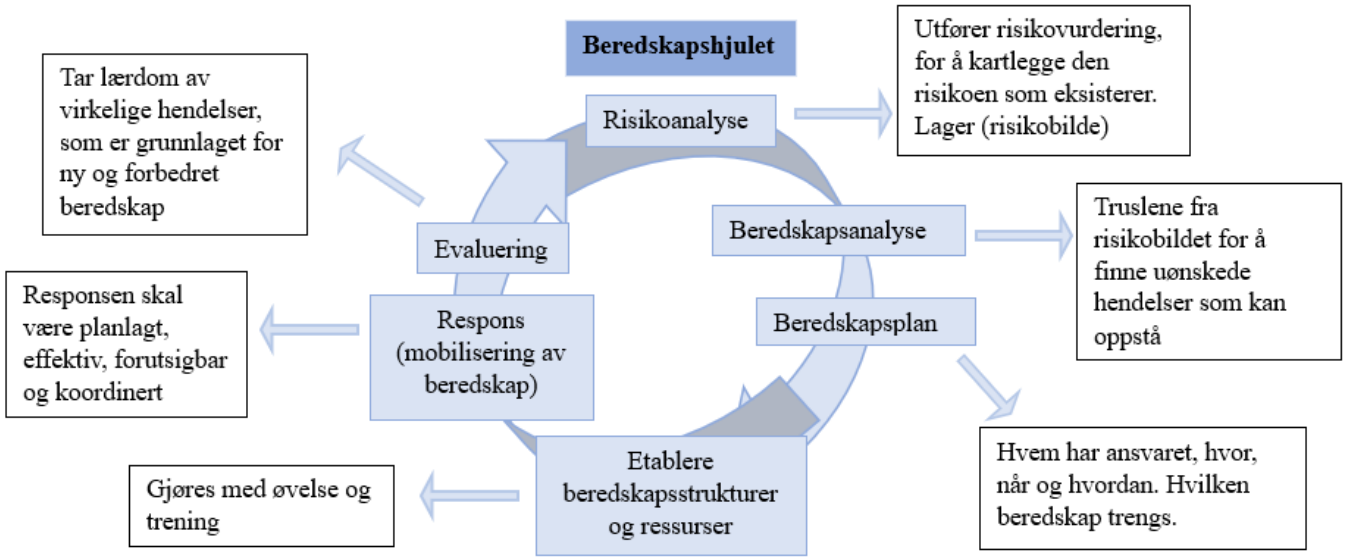
Stortinget. (2022). *Stortinget Administrasjon har mottatt forhåndsvarsel fra Datatilsynet.* Stortinget.no. Retrieved from https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Pressemeldingsarkiv/2021-2022/stortinget-har-mottatt-forhandsvarsel-fra-datatilsynet/

Tolletaten. (2020, Oktober 01). *Tolletaten med ny organisering fra 1.oktober*. Retrieved from Tolletaten.no: https://www.toll.no/no/om-tolletaten/nyheter/arkiv/2020/tolletaten-med-ny-organisering-fra-1.-oktober/

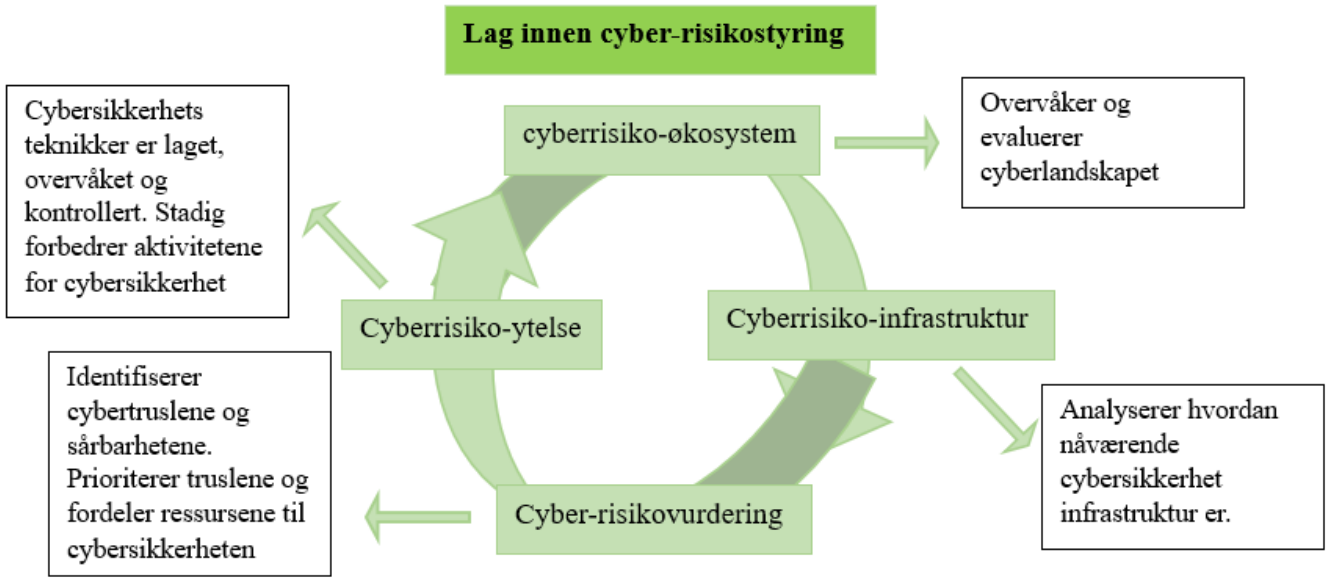
Tolletaten. (2022). *Tolletaten mot 2030.* Tolletaten.no. Retrieved from https://www.toll.no/contentassets/ab1cde2a68b248eeb5b0afa25878579a/tolletatens-virksomhetsstrategi-2022-2030.pdf

Tolletaten. (2024, Mars 06). *Digitoll*. Retrieved from Tolletaten.no: https://www.toll.no/digitoll

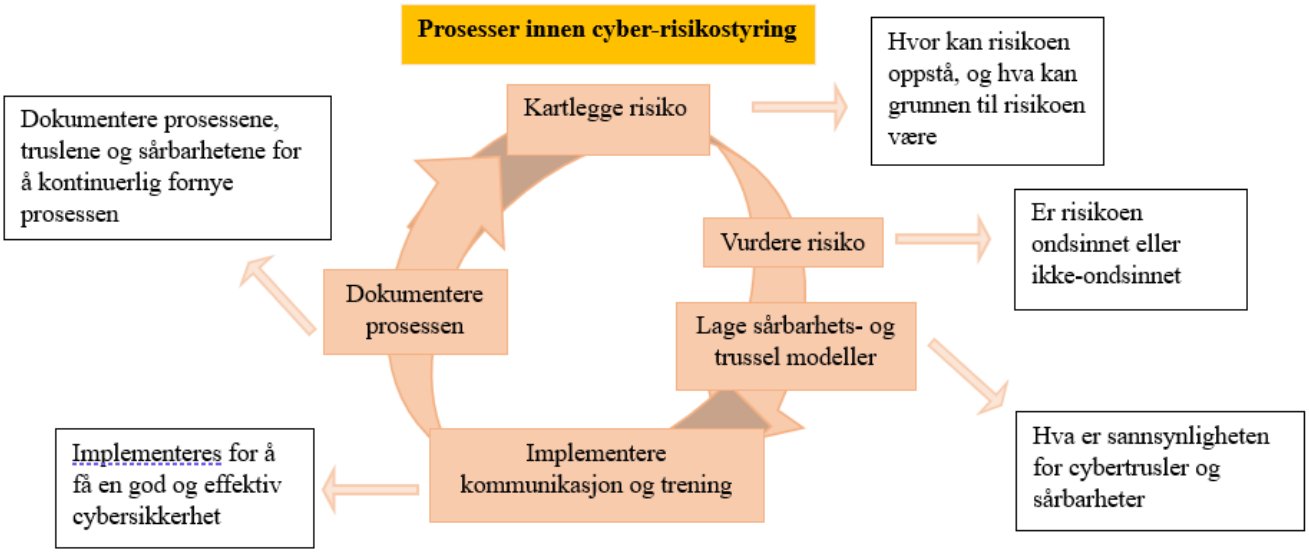
Vedlegg



Figur 1. Beredskapshjulet (basert på Engen, et al., 2021, s.325)



Figur 2. Lag innen cyber-risikostyring (basert på Lee, 2020, s. 6)



Figur 3. Prosesser innen cyber-risikostyring (basert på Refsdal, et al., 2015, ss. 42-46)