GÖTEBORGS UNIVERSITET

FÖRVALTNINGSHÖGSKOLAN

Cybersäkerhet i kommunala korridorer

En studie om cybersäkerhet på lokal nivå

Anna Isaksson

Marcus Ragnarsson

Program:	Kandidatprogrammet i offentlig förvaltning, 180 hp
Kurs (kurskod):	Kandidatuppsats i offentlig förvaltning, 15 hp (FH1504)
Nivå:	Grundnivå
Termin/år:	HT2023
Handledare:	Emma Ek Österberg och Johanna Thalenius
Examinator:	Mikael Löfström

Sammanfattning

Program:	Kandidatprogrammet i offentlig förvaltning, 180 hp
Kurs (kurskod):	Kandidatuppsats i offentlig förvaltning, 15 hp
Nivå:	(FH1504) Grundnivå
Titel (svensk):	Cybersäkerhet i kommunala korridorer
Titel (engelsk):	Cybersecurity in corridors of municipalitys
Termin/år:	HT2023
Handledare:	Emma Ek Österberg och Johanna Thalenius
Examinator:	Mikael Löfström
Nyckelord:	Cybersäkerhet, cyberattack, AI, digitalisering

Syfte: Studiens syfte är att få förståelse för existerande uppfattningar, strategier och hantering av cyberhot som den kommunala förvaltningen utsätts för i samband med den accelererande digitaliseringen samt utvecklingen av artificiell intelligens.

Teori: Den teoretiska referensramen utgår ifrån fem teman: AI, trög förvaltning i accelererande omvärld, arbetsmetoder kopplat till cybersäkerhet, medvetenhet och förberedelse/kapacitet.

Metod: Studien genomfördes med en kvalitativ intervjustudie, där totalt sju chefer i tre olika kommuner intervjuades med semi-strukturerade intervjuer.

Resultat: Studiens resultat visat att anställda inom den kommunala verksamheten är medvetna om de cyberhotet som finns samt att hotet har ökat i takt med den accelererande digitaliseringen. Vidare kan det konstateras att det både finns risker och möjligheter med användning av AI-teknik som både kan försvara och utsätta en verksamhet. Det förekommer arbetsmetoder kopplat till cybersäkerhet i de olika förvaltningarna men en variation i utbredhet. Det finns tydligt utrymme för förbättring och en önskan om stöd från andra aktörer.

Förord

Efter tre års studier på kandidatprogrammet i offentlig förvaltning kan vi med stor glädje och stolthet presentera vår kandidatuppsats!

Vi vill ge ett stort tack till våra handledare Emma Ek Österberg och Johanna Thalenius som under uppsatsskrivandet bidragit med ett stort engagemang, kunskap och vägledning som gett oss värdefullt stöd och stor inspiration.

Alla intervjupersoner får självklart ett tack för att ni ställt upp och deltagit i vår studie, vi har sett stort värde i era perspektiv och erfarenheter.

Vi vill även tacka familj och vänner som bidragit med mycket glädje och ovärderligt stöd under våra universitetsstudier, inte minst under höstens utmanande tid med uppsatsskrivande.

Stort tack för allt!

Anna Isaksson,

Marcus Ragnarsson

Förvaltningshögskolan, Göteborgs universitet, 2024

Innehållsförteckning

1. Inledning

Under de senaste decennierna har digitaliseringen snabbt växt fram och påverkat samhället på många plan. Enligt Statens offentliga utredning (2016:89) menar digitaliseringskommissionen att digitalisering inom den offentliga förvaltningen innebär nya tjänster och lösningar av bättre kvalitet som möjliggör en bred användning till låg kostnad. Med digitaliseringen kommer en ökning av individualisering då tillgången till data möjliggör en fördjupad förståelse av individuella behov och preferenser, till följd av detta finns det möjlighet att utforma individanpassade varor och tjänster inom den offentliga förvaltningen (SOU 2016:89).

År 2018 inrättades Myndigheten för digital förvaltning då det fanns ett behov av att analysera och främja digitaliseringen i den offentliga sektorn (Myndigheten för digital förvaltning et al., 2023). Myndigheten samarbetade med andra myndigheter i *Det nationella AI-uppdraget* med syfte att driva på den offentliga förvaltningens möjlighet att främja användningen av artificiell intelligens (AI). Uppdraget visade att AI kan innebära en stor nytta inom den offentliga förvaltningen och år 2020 uppskattades det sammanlagda värdet av en fullständig implementering av dåvarande AI-teknik att uppgå till en besparing på 140 miljarder kronor, det antogs även finnas andra indirekta ekonomiska och sociala värden som inte inkluderades i beräkningen (Myndigheten för digital förvaltning et al., 2023). I uppdraget framgick det att mindre och medelstora aktörer inte har resurser till att delta i utvecklingen av användandet av AI, vilket medför stora risker för säkerhetsintrång och cyberattacker (Myndigheten för digital förvaltning et al., 2023).

I takt med digitaliseringens framfart ställs den offentliga förvaltningen inför nya risker då frågor kring trygghet och säkerhet i den digitala världen blir aktuella. Medborgare ska känna tillit till att deras personliga data som den offentliga förvaltningen förvarar inte hamnar i fel händer eller används till något annat än vad den är avsedd till (Myndigheten för digital förvaltning, 2023). Samtidigt är kommuner då de bedriver samhällsviktiga funktioner måltavlor för cyberattacker, vilket kan efter en lyckad cyberattack resultera i negativa effekter på samhället och dess invånare (Advencia, 2023). Ett exempel där detta hänt är när en databas tillhörande en organisation i Indien blev utsatta för en cyberattack där 815 miljoner indiska invånares personuppgifter läcktes och såldes på dark web i oktober 2023 (Ford, 2023). Även Kalix kommun utsattes år 2022 för en IT-attack där hackare låste kommunens IT-system och krävde

en lösensumma för upplåsning (Stahle, 2022). Flertalet delar av kommunens verksamhet påverkades negativt av attacken då flertalet system var otillgängliga och hantering av attacken uppskattas ha kostat kommunen miljonbelopp (Stahle, 2022).

Säkerheten kring digitala lösningar hänger inte med i den takt digitaliseringen utvecklas, vilket gör organisationer sårbara för cyberhot (Myndigheten för samhällsskydd och beredskap, u.å). Safitra et al. (2023) förklarar att man behöver implementera säkerhetsåtgärder för att förutse, mildra, svara på och återhämta sig från cyberattacker. Larsson (2023) skriver i en intervju med Mari Paananen, docent i företagsekonomi på Handelshögskolan i Göteborg, att det är viktigt att det finns regler innan man går för fort fram med AI-system, bland annat regler som hanterar kundinformationen som matas in i AI-system.

I kommittédirektivet om en kommission för den digitala agendan (Dir 2012:61) presenteras målet att ‘’*Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter*’’ (Dir 2012:16, sida 1). Målet övergriper it- och digitaliseringspolitiken genom de kommande åren (Regeringskansliet, 2017; SOU 2016:89). I Statens offentliga utredning (2016:89) skriver digitaliseringskommissionen att organisationer inom den offentliga sektorn både inhämtar och producerar stora kvantiteter data, på grund av den ökade digitaliseringen tillkommer utmaningar kring integritets- och konsumentskydd. Det tydliggörs att det måste finnas kompetens kring hur man inom den offentliga verksamheten säkerställer informationssäkerhet för att undvika att främmande makter eller kriminella nätverk kommer åt datan. (SOU 2016:89).

1.1 Definition cybersäkerhet och digitalisering

Cybersäkerhet innefattar den digitala säkerheten och hur verksamheter arbetar för att skydda digital information. Konfidentialitet, integritet och åtkomst är tre viktiga begrepp inom cybersäkerhet som uppmanar till att säkerställa att endast behöriga har tillgång till digital information, att informationen inte ändras samt att det ska vara möjligt att komma åt den digitala informationen även vid en cyberattack (Microsoft, u.å). Policys, verktyg, tekniker och riktlinjer är exempel på åtgärder för att skydda mot att känsliga uppgifter blir röjda av cyberattacker (Schatz et al., 2017). Digitalisering innebär att använda sig av teknikens möjligheter till att förbättra, utveckla och förändra saker (Cadeo, u.å).

I denna uppsats kommer begreppen digitalisering, cybersäkerhet, cyberattacker och AI att inkluderas i diskussionen kring kommunala verksamheters cybersäkerhet då de på olika sätt har en inverkan på cybersäkerhet.

1.2 Problembeskrivning

Samtidigt som ny digital teknik träder fram i samhället förändras delar av den offentliga förvaltningens tjänster, bland annat automatiserat beslutsfattande, chatbotar och tjänster online. I samband med en digitaliserad offentlig förvaltning tillkommer risker och utmaningar kring cybersäkerhet (Henman, 2020). Cyberkriminella har i stor utsträckning offentliga verksamheter som måltavla i cyberattacker då den sorts verksamhet lagrar känslig information om medborgare, vilket är intressant och värdefull information för cyberkriminella att få tag på (Norris et al., 2019). Khisamova et al. (2019) varnar för att det finns problem med att säkerställa sekretessen av konfidentiell information med anledning av hotet om cyberattacker.

Norris et al. (2021) såg i sin studie att det var tydligt att offentliga verksamheter hanterar cybersäkerhet på olika sätt samt besitter olika nivåer av kunskap inom området. Riksrevisionen (2023) kom i en skrivelse till Regeringskansliet fram till att det saknas en effektivt utformad och utförd strategi för information- och cybersäkerhet. Det fanns brister i strategiska avvägningar och prioriteringar i arbetet. Problemet grundade sig i att Regeringskansliet saknade tillräckligt bra arbetsmetoder, resursanvändning och organisering för ett effektivt arbete.

Ett annat sätt att förstå cybersäkerhet som kan beskriva problembilden är vad IoT har för effekt i samhället. IoT beskrivs av IoT Sverige (u.å.) som sakernas internet, ett nyfenomen som innebär att flertalet föremål, inte bara smartphones, blir uppkopplade till internet. Butun et al. (2020) menar att den ökade användningen av IoT kommer leda till brister i cybersäkerheten, vilket kan bli problem för alla individer som är uppkopplade till internet. Riskerna med IoT är högst relevanta då det påverkar en stor del av befolkningen då mängden enheter uppkopplade till internet innehållandes känslig information är stor. Konsekvenserna för samhället kan bli stora, exempelvis då självkörande bilar är uppkopplade. Skulle cybersäkerheten vara låg i detta fall skulle det kunna innebära att trafikdödligheten ökar, när samhällsmålet är noll (Transportstyrelsen, u.å.). En ökad digitalisering leder alltså till en ökning av IoT vilket innebär att större mängder data behöver skyddas.

Wirtz et al. (2019) menar att det är problematiskt att AI-system är självlärande eftersom det är utmanande för människor att förutse AI-systemets framtida beteende. En ansvarslucka uppstår då det är svårt att avgöra om det är människan eller AI-systemets fel om saker inte går som planerat.

Den accelererande digitaliseringen har inneburit en ökad användning av informationsteknologi och informationssystem inom offentliga verksamheter, tillit och beroende av dessa system innebär även fler risker och sårbarheter, däribland hot om cyberattacker. Trots de risker offentliga verksamheter står inför i takt med digitaliseringen så brister forskningen inom ämnet cybersäkerhet inom offentlig sektor (Writz & Weyerer, 2017). På grund av att fler tjänster inom offentliga sektorn erbjuds digitalt finns det ett tydligt behov av att förstå hur verksamheterna arbetar med att skydda sin data (Hatcher et al., 2020). Writz och Weyerer (2017) samt Norris et al. (2021) genomförde sina studier med anledning av den bristande forskningen på området. Att det inte finns tillräckligt med forskning inom fältet återfinns i flertalet vetenskapliga artiklar där forskare menar gång på gång att det krävs mer forskning inom fältet (Writz & Weyerer, 2017; Norris et al., 2021; Preis & Susskind, 2022; Choodakowska et al., 2022; Hatcher et al., 2020; Caruson et al., 2012). Det finns således en tydlig inomvetenskaplig relevans för ämnet som studien ska behandla.

Denna studie ska uppmärksamma forskningsfältet cybersäkerhet i offentlig sektor och bidra till den bristande forskning som forskare tidigare har rapporterat om. Det finns ett behov att förstå hur den offentliga förvaltningen arbetar med cybersäkerhet då en felaktig hantering kan innebära stora negativa konsekvenser (Norris et al., 2019).

1.3 Syfte och frågeställningar

Studiens syfte är att få förståelse för existerande uppfattningar, strategier och hantering av cyberhot som den kommunala förvaltningen utsätts för i samband med den accelererande digitaliseringen samt utvecklingen av artificiell intelligens.

Syftet uppnås genom en kvalitativ intervjustudie om cybersäkerhet där följande frågeställningar besvaras:

- *Hur uppfattas hotet mot cybersäkerheten i accelerationen av digitaliseringen/AI?*

- *Vilka arbetsmetoder använder kommunen för att säkerställa cybersäkerheten för verksamheten?*

1.4 Tidigare forskning

Writz och Weyerer (2017) beskriver att information- och kommunikationstekniker har utvecklats drastiskt under de senaste decennierna samtidigt som det har integrerats väl in i olika samhällsfunktioner. Offentliga infrastrukturer är direkt kopplade till informationsteknologi, samtidigt som den accelererande digitaliseringen innebär möjligheter tillkommer även risker och svagheter kopplat till cybersäkerhet vilket orsakar en oro hos offentliga verksamheter. Offentliga verksamheter är en vanlig måltavla för cyberattacker och det sker en ökning i antalet anmälda cyberattacker mot offentliga verksamheters digitala infrastruktur (Writz & Weyerer, 2017). Det är en utmaning för offentliga verksamheter att använda digitaliseringens möjligheter samtidigt som de säkerställer att deras data skyddas eftersom de digitala tjänster som introduceras för att effektivisera och förbättra arbetet även innebär en ökad risk för cybersäkerheten (Frandell & Feeney, 2022). Samtidigt förekommer en oro över att anställda inom offentliga verksamheter underskattar den mängd av cybersäkerhetsöverträdelser som genomförs med brottsliga avsikter (Caruson et al., 2012). Lyckade cyberattacker mot offentliga IT nätverk kan påverka både verksamheten och individer, samtidigt som den offentliga säkerheten riskerar att påverkas (Writz & Weyerer, 2017).

Då antalet rapporterade cyberattacker mot offentliga verksamheter växer anses det vara en av de främsta socio-tekniska utmaningarna som offentliga verksamheter ställs inför i nuläget. Det är nödvändigt för offentliga verksamheter att ha en mjukvara som kan skydda mot cyberattacker, vidare bör det även finnas anställda som ansvarar för att säkerställa att verksamheten följer existerande cybersäkerhetspolicys (Choodaowska et al., 2022). Offentliga verksamheter har ett stort ansvar i att försäkra att verksamhetens digitala plattformar och databaser är skyddade från cyberattacker, samtidigt syns en kunskapsbrist inom verksamheter huruvida det skett försök till cyberattacker eller inte (Norris et al., 2021).

Khisamova et al. (2019) skriver att i takt med användning av AI kommer ett behov att beakta etiska och rättsliga problem, och de ställer frågan ‘’*How to use maximum data with minimum risks?*’’(Khisamova et al., 2019, sida. 568). Khisamova et al. (2019) varnar om att det finns

stora möjligheter för cyberkriminella att utnyttja AI-teknik för att bedriva brottslig verksamhet. Det kommer alltså inte alltid vara möjligt att garantera cybersäkerheten då ny AI-teknik har kapacitet att hitta dolda kopplingar i datasystem genom att analysera stora mängder data (Khisamova et al., 2019). Guembe et al. (2022) rapporterar att cybersäkerheten kommer påverkas av den nya varianten av cyberkriminella då cyberkriminella kan utnyttja AI-teknik för att skala upp och öka hastigheten av attackerna, dessutom finns det en risk att cyberattacker kommer vara kapabla till att utföras självständigt genom AI.

Writz et al. (2020) menar att AI för med sig utmaningar in i offentlig sektor. Den alltför snabba utvecklingen av AI leder till att offentlig sektor inte lika lätt kan möjliggöra adekvat styrning. Författarna drar slutsatsen att offentlig sektor borde samarbeta med privata organisationer för att dra nytta av kunskap som finns inom den privata sektorn, detta finns vid tillfället inte inom offentlig sektor. Ett samarbete av detta slag kan leda till implementeringen av nya policys (Writz et al., 2020).

Hatcher et al. (2020) beskriven tyngden av att kommuner har specifikt utformade policys för cybersäkerhet då det observerats att de kommuner som har en formell cybersäkerhetspolicy är mer troliga att testa sin kapacitet att försvara sig mot attacker, specificera åtkomsten till känslig data och utbilda anställda om policys och arbetssätt kopplat till cybersäkerhet. Hatcher et al. (2020) kom i sin studie fram till att kommuner har i många fall har policys som adresserar cybersäkerhet, dock behövs det fortfarande en förbättring. Endast 37% av kommunerna som deltog i studien sparade uppgifter om tidigare cyberintrång, författarna menar att kommuner bör spara dessa uppgifter. Vidare bör kommuner ta hjälp av utomstående aktörer och kunniga i utvecklingen av IT-policys samt bidra med löpande utbildning i cybersäkerhet för chefer och ledare. Otillräckliga finansiella resurser hindrar kommuner från att arbeta med cybersäkerhet på olika vis, därmed menar författarna att staten behöver bidra med stöd för att kommuner ska ha råd att implementera åtgärder för cybersäkerhet (Hatcher et al., 2020).

Barcik et al. (2023) studerar möjligheter och utmaningar i digitaliseringsarbetet i städer. Det beskriver tyngden av att ledning inom städer har ansvarsperspektivet i åtanke. I den allt mer accelererande digitaliseringen krävs stort fokus på cybersäkerhet, då det är viktigt att motverka cyberhot. För att integriteten ska säkras behövs det bestämmelser om vem eller vilka som är ansvarig för datan för att skapa tillit mellan olika parter (Barcik et al., 2023).

2. Teoretisk referensram

I följande kapitel presenteras begrepp från tidigare forskning som ligger till grund för att besvara studiens frågeställningar och för att analysera empirin. Inledningsvis presenteras AI som aspekt och därefter introduceras påståendet om den tröga förvaltningen, arbetsmetoder kopplat till cybersäkerhet, medvetenhet om cybersäkerhet och till sist förberedelse och kapacitet att hantera en cyberattack. Kapitlet avslutas med en sammanfattning av den teoretiska referensramen.

2.1 AI som aspekt - möjlighet eller hot?

Nya former av teknik har genom tiderna kommit med både möjligheter och svårigheter, detta gäller även framfarten av AI (Henman, 2020). Guembe et al. (2022) skriver att det utvecklas en ny generation av cyberkriminella där AI används för att skala upp och effektivisera cyberattacker. Det kommer i framtiden förekomma cyberattacker som sker självständigt genom AI, AI-tekniken kommer kunna ta egna beslut och anpassa attacken baserat på det specifika målets förutsättningar och miljö. Redan idag genomförs välorganiserade cyberattacker med hjälp av AI, utvecklingen kommer inte avta och det kan komma stora utmaningar i att hantera attackerna då dagens metoder inom cybersäkerhet inte kommer kunna upptäcka framtidens avancerade AI drivna attacker då de redan nu brister i motståndskraften mot dagens cyberattacker som tar hjälp av AI. Framtidens cyberattacker kommer ha kapacitet att utnyttja ett systems svagheter och även maskera sig som ett pålitligt system. Verksamheter bör svara på denna utveckling genom att själva investera i cybersäkerhetsinfrastruktur som drivs av AI-teknik (Guembe et al., 2022).

Norris et al. (2021) menar att det finns en okunskap hos offentliga verksamheter kring förekomsten av cyberhot mot den enskilda verksamheten, vilket tyder på att offentliga verksamheter inte hänger med i den digitala utvecklingen. Samtidigt utvecklas AI snabbt, Tegmark (2023) menar att arbetet med avancerade AI-system bör pausas då det är okänt om dess effekter är positiva eller negativa, det är även oklart om det finns kapacitet att hantera de risker som tillkommer med välutvecklad AI. Wirtz et al. (2020) menar samtidigt att om AI utvecklas för snabbt inom offentlig sektor så minskar möjligheterna för kommunen att utföra adekvat, eller lämplig styrning, som behövs inom offentlig sektor.

Samtidigt som AI kan utgöra ett hot möjliggör det även förbättringar både i offentliga tjänster och offentliga verksamheters cybersäkerhet (Henman, 2020). AI kan komplettera existerande arbetsmetoder vilket kan innebära besparingar och ökad produktivitet (Wirtz et al., 2019). Offentliga verksamheter kan använda AI som ett komplement till sina tjänster genom virtuella assistenter och automatiserat beslutsfattande, utöver detta kan välutvecklade AI-system i ett tidigt skede uttrycka varningar för bedrägeri samt upptäcka skattefusk (Mergel et al., 2023).

Hoten som uppenbarar sig i framfarten av AI kan påverka professionerna, Susskind och Susskind (2017) menar att framtiden är oviss gällande digitaliseringen. Det är oklart exakt vad som är nästa steg. Förändringar som med hjälp av AI effektiviserar verksamheter kan få stora effekter på hur professioner fungerar. Susskind och Susskind (2017) tror att övergången till ett postprofessionellt samhälle, där maskiner tar över uppgifter tillhörande professionerna, kommer ske genom en inkrementell omdaning, där det genom steg för steg snarare än omedelbar revolution kommer leda till stor radikal effekt.

På grund av att implementeringen av AI-tjänster och system växer inom offentlig sektor (Henman, 2020) samtidigt som studier rapporterar om både möjligheter och risker kopplat till AI:s påverkan på cybersäkerhet (Guembe et al., 2022) så är det relevant att se offentligt anställdas attityd till AI.

2.2 En trög förvaltning i accelererande omvärld

Den offentliga förvaltningen står inför stora utmaningar sett till den allt mer accelererande omvärlden. Andréasson (2015) menar att den e-förvaltning som idag används i offentlig sektor behöver vara i samklang med demokratiska värderingar, lagstiftning och byråkratiska regelverk sett till det digitaliserade samhälle som utvecklas. Även Melin (2018) menar på att den offentliga sektorn inte hänger med och att digitaliseringen av offentlig sektor tar för lång tid. Digitaliseringen är otillräckligt samordnad och det finns en alldeles för stor variation i kvalitet i samhället sett till genomkraft (Melin, 2018).

I arbetet med digitalisering i den offentliga sektorn har det observerats som mest utmaningar i stadiet av implementering av AI-system. Offentliga verksamheter är i ett tidigt

utvecklingsskede gällande AI-system, vilket pekar på att innovation inom offentliga verksamheter sker långsamt trots att verksamheterna visar intresse och vilja för användning av AI (Campion et al., 2020).

Bilden av att utvecklingen inom offentliga verksamheter sker långsamt är relevant att diskutera i förhållande till cybersäkerhet då digitaliseringen i omvärlden sker snabbt (Writz & Weyerer, 2017), vilket kan innebära att den kommunala verksamheten har svårt att hantera nyutvecklade varianter av cyberattacker och övriga digitala skyddsåtgärder.

2.3 Arbetsmetoder och organisering kopplat till cybersäkerhet

Forskningen brister gällande den offentliga sektorns arbetsmetoder för cybersäkerhet, dock finns forskning om arbetsmetoder inom den privata sektorn. Inom tillverkningsindustrin forskas det om åtgärder för att hantera cyberattacker mot digitala system, Wu et al. (2018) kommer fram till att vid utvecklingen av gamla system behövs ny åtkomstkontroll, kryptering och tekniker för att upptäcka intrång. Författarna kom även fram till att för att förhindra problem skapade av hackers behövs en övervakning av system och processer för att upptäcka eventuella brister. Den offentliga sektorn kan ta vara på denna kunskap och ta vid dess arbete framåt.

Norris et al. (2019) presenterar ett antal rekommendationer som offentliga verksamheter bör implementera i sitt arbete med cybersäkerhet. Det bör skapas ett tänk för cybersäkerhet som genomsyrar hela verksamheten, från botten till toppen då det inte räcker att endast en del av verksamheten värdesätter cybersäkerhet. Vidare bör hinder som sätter stopp för utvecklingen av cybersäkerhet adresseras och de kunskapsluckor som existerar kring cybersäkerhet bör elimineras genom att sprida kunskap. Verksamheter rekommenderas att följa den bästa praxisen för cybersäkerhet. Studier som analyserar offentliga verksamheters hantering av cybersäkerhet bör upprepas enligt författarna minst vart femte år för att belysa de förändringar som konstant sker (Norris et al., 2019).

Demertzi et al. (2023) forskar om digitala smarta städer, de presenterar ett antal arbetssätt att arbeta efter för just städer, istället för kommunala förvaltningar. För att mildra eventuella problem som kan uppstå behövs cybersäkerhetsstrategin integreras med den ordinarie strategin. Det behöver genomföras en grundlig genomgång av processer för att identifiera eventuella

problem samt förhindra framtida problem. Det rekommenderas att en data- och cyberstyrning formaliseras för att utveckla regler och processer. Det krävs en kontakt med experter för att stärka kunskapen och kapaciteten kring cyberrelaterade problem (Demertzi et al, 2023).

Safitra et al. (2023) presenterar ett ramverk som ska stärka organisationers motståndskraft mot cyberhot. Ramverket menar att det är viktigt med organisationellt ledarskap, ansvarstagande och att komma på idéer som ska motstå cyberhot. Att följa praxiserna ska hjälpa organisationer att förutspå, mildra, svara på och återhämta sig från cyberattacker.

Det är viktigt att offentliga verksamheter identifierar verksamhetens svagheter i digitala sammanhang för att stärka skyddet mot yttre hot (Writz & Weyerer, 2017). Vanliga aktiviteter online som kan vara potentiella risker för cybersäkerheten är e-postkommunikation, webbsurfande samt missbruk av trådlöst nätverk. Efter identifieringen av digitala svagheter bör det ske en riskanalys inom verksamheten kopplat till svagheterna som identifierats (Writz & Weyerer, 2017).

En viktig del av cybersäkerhet är att vidta skyddsåtgärder, till exempel utbildningar för anställda, brandväggar, antivirusprogram samt kryptering. I de fall skyddsåtgärderna inte lyckas blockera en cyberattack krävs det att verksamheten har en nödplan där det finns planerade processer och åtgärder för att hantera en krissituation (Writz & Weyerer, 2017). Specifika policys för cybersäkerhet bör utformas då verksamheter som har det är mer benägna att arbeta mer med cybersäkerhet (Hatcher, 2020).

För att kunna få en förståelse över hur kommunala verksamheter arbetar med cybersäkerhet är det relevant att diskutera förekomsten av arbetsmetoder som uppmuntras för att öka cybersäkerheten. Tidigare forskning kan vägleda vad som är relevanta arbetsmetoder för att skydda verksamheter mot cyberattacker.

2.4 Medvetenhet om cybersäkerhet

Förekomsten eller avsaknaden av medvetenhet kring cybersäkerhet kan i en offentlig verksamhet antingen underlätta eller agera hinder i arbetet med cybersäkerhet. Norris et al. (2021) menar att medvetenhet om cybersäkerhet är en viktig aspekt inom offentliga

verksamheter och kunde i en studie påvisa en brist där omkring 30% av de tillfrågade offentliga verksamheterna inte erbjuder anställda utbildning i medvetande kring cybersäkerhet, detta gällde både anställda som arbetade med cybersäkerhet och övriga anställda i verksamheten. Hatcher et al. (2020) påvisade i sin studie en högre procentandel, 41% av de tillfrågade erbjöd inte anställda utbildning om cybersäkerhet löpande. Anställda som inte informerats om säkerhetsåtgärder i arbetet kan utsätta verksamheten för risker genom ett naivt och oförsiktigt agerande som leder till att känslig information sprids (Khando et al., 2021). Chefer inom offentliga verksamheter behöver vara medvetna om att det finns ett behov av cybersäkerhet samt ge stöd för detta då detta motiverar verksamheten till att etablera cybersäkerhet i arbetet. (Norris et al., 2021).

Eftersom cybervärlden är i konstant förändring bör ledare och chefer inom offentlig förvaltning vara medvetna om aktuell information kring skyddsåtgärder mot cyberhot. Det har dock observerats att ledare och chefer inom offentlig förvaltning brister i medvetenhet kring cybersäkerhet, trots att offentliga verksamheter är vanliga måltavlor för cyberattacker (Wirtz & Weyerer, 2017).

Medvetenhet om cybersäkerhet är relevant att diskutera då det tidigare påvisats att chefer inom offentlig förvaltningen brister i medvetenhet (Wirtz & Weyerer, 2017). Graden av medvetenhet om cybersäkerhet skulle kunna påverka hur verksamheten arbetar med cybersäkerhet.

2.5 Förberedelse och kapacitet att bemöta en cyberattack

På grund av den accelererande digitaliseringen under de senaste årtiondena har offentliga verksamheter blivit mer mottagliga för cyberattacker vilket kan få stora konsekvenser om verksamheterna inte är förberedda med preventiva- och återhämtningsåtgärder. Finns det inte tillräcklig förberedelse kan offentliga verksamheter riskera att ha en stillastående verksamhet i dagar eller månader efter en cyberattack (Preis & Susskind, 2022).

Norris et al. (2019) rapporterar i sin studie att endast 48% av tillfrågade offentliga verksamheter bedömde sin förmåga att återhämta sig från en cyberattack som väldigt bra eller utmärkt, vilket tyder på bristande förberedelse hos en majoritet. Då hoten för cyberattacker konstant utvecklas

behöver offentliga verksamheter se utvecklingen och anpassa åtgärder efter förändringarna (Norris et al., 2019).

En metod som säkerställer förberedelse inför cyberattacker är ett evolutionärt förhållningssätt inom en organisation. Förhållningssättet innebär att organisationer ständigt är uppdaterade kring nya hot och därefter kontinuerligt anpassar nya säkerhetsåtgärder. Genom att arbeta med cybersäkerhet på detta sätt kan organisationer utveckla kunskaper i att förutse hot, förbereda hantering och återhämtning av attacker. Organisationer som kontinuerligt arbetar med cybersäkerhet med fokus på förberedelse har bättre förutsättningar att hantera cyberattacker innan, under och efter (Safitra et al., 2023). Dock brukar offentliga verksamheter ha ett större fokus på att vara reaktiva än proaktiva i implementering av policys för cybersäkerhet. Den bristande förberedelsen kan bero på finansiella aspekter då det kan vara utmanande att anställa personal och resurser i ett svårt ekonomiskt läge, en större utmaning om verksamheten tidigare inte blivit utsatta för en cyberattack. Det finns en bild bland offentligt anställda att ansvaret för cybersäkerhet endast ligger hos IT-tekniker inom verksamheten, vilket kan bidra till en bristande förberedelse då hela verksamheten bör tänka på cybersäkerhet. Vidare kan en avsaknad av samarbete mellan nivåer inom verksamheten bidra till en bristande förberedelse då samarbete och koordination är två viktiga aspekter för en lyckad cybersäkerhetspolicy (Caruson et al., 2012).

Hur förbered en kommun är och vilken kapacitet den har att hantera en cyberattack är relevant då detta kan ha en påverkan på hur väl en cyberattack hanteras och graden av konsekvenser (Preis och Susskind, 2022).

2.6 Sammanfattning av teoretisk referensram

Den teoretiska referensramens fem delar är enligt den tidigare forskningen inom fältet centrala och återkommande delar som anses vara viktiga för offentlig sektors hantering av cybersäkerhet. Den teoretiska referensramen bidrar med en förståelse för studiens frågeställningar och syfte genom att presentera vad tidigare forskning säger om existerade uppfattningar, strategier och hantering av cyberhot inom offentlig sektor.

3. Metod

I följande kapitel kommer studiens metod och urval att presenteras och motiveras. Vidare beskrivs studiens genomförande, forskningsetiska överväganden och studiens kvalitet.

3.1 Val av metod

För att kunna besvara studiens frågeställningar och uppfylla syftet valdes kvalitativ metod. Delar av samhällslivet går inte att se med kvantitativa metoder (Ahrne & Svensson, 2015) då den metod relaterar till frågor som svarar på till exempel hur många, hur ofta och hur vanligt något är (Trost och Hultåker, 2016). Kvantitativ metod är inte relevant att använda i vår studie då frågeställningarna syftar till att se uppfattningar och erfarenheter. Genom att använda den kvalitativa metoden intervjuer kan det inhämtas en bra bild av uppfattningar, föreställningar och erfarenheter (Carlsson & Carlsson, 2020). Ahrne och Svensson (2015) menar även att det går att fånga nyanser med kvalitativ metod på ett annat sätt än kvantitativa metoder.

3.1.1 Intervjuer

Carlsson och Carlsson (2020) menar att metodval bör göras med eftertanke, valen ska göras på ett sådant sätt att frågeställningar och syfte kan besvaras på bästa sätt. Den kvalitativa metoden semistrukturerade intervjuer valdes att användas i studien då vi ansåg att den skulle besvara frågeställningarna och uppfylla syftet på ett bättre sätt än andra metoder. Intervjuer är användbara vid insamling av uppfattningar, föreställningar och erfarenheter (Carlsson & Carlsson, 2020), då studiens frågeställningar relaterar till anställdas uppfattningar av cybersäkerhet samt erfarenheter av arbetsmetoder inom den kommunala verksamheten är intervjuer en passande metod.

Semistrukturerade intervjuer valdes framför strukturerade och ostrukturerade intervjuer eftersom en ostrukturerad intervju riskerar att missa viktiga frågor och en strukturerad intervju lämnar inte utrymme till spontana frågor som kan leda till mer utvecklade svar (Carlsson & Carlsson, 2020). Semistrukturerade intervjuer innebär en trygghet till oss intervjuare genom en intervjuguide samtidigt som det finns utrymme för spontana frågor.

Enskilda intervjuer genomfördes istället för gruppintervjuer då vi tror att intervjupersonerna är mer bekväma att besvara frågor enskilt i ett anonymt sammanhang, vi ville inte heller riskera att intervjupersonerna påverkas i sina svar av resterande grupps svar.

Kvalitativa enkäter valdes bort i metodvalet eftersom det inte finns utrymme för oss uppsatsskrivare att fråga efter förtydliganden och följdfrågor i en kvalitativ enkät (Karlsson, 2020), denna möjlighet finns i semistrukturerade intervjuer.

Observationer användes ej som metodval då det inte passar till att svara på våra frågeställningar eller uppfylla studiens syfte. Observationer används när en studie vill se till exempel beteenden, praxis eller rutiner (Svärd, 2020), vilket denna studie inte ska undersöka. Vi tror även att denna metod kräver mycket tid, då studien ska utföras inom en tidsram ansåg vi att det inte fanns utrymme att använda denna metod, samtidigt misstänkte vi att det förelåg sekretess inom vissa förvaltningar.

3.2 Urval

Det som studien avser att studera avgör val av intervjupersoner, valet i många fall kan påverkas av vilka personer som har möjlighet och intresse att ställa upp (Carlsson & Carlsson, 2020). Snöbollsmetoden kan användas för att välja ut intervjupersoner (Carlsson & Carlsson, 2020), vi ansåg dock att denna metod möjligtvis kan innebära en längre process i att färdigställa intervjuer, metoden valdes därmed bort på grund av tidsramen.

Till en början ville vi intervjua anställda inom en specifik förvaltning i en kommun i Sverige. Eftersom vi stötte på hinder planerade vi om vilket resulterade i att vi istället valde att intervjua olika chefer inom tre olika kommuner.

Valet baserades på idén att det vore intressant att se en varierad bild av anställdas uppfattningar och arbetsmetoder kopplat till cybersäkerhet. En variation i kommuner och typer av chefer kan bidra med en övergripande bild som kan belysa likheter och skillnader mellan kommuner och inom samma kommun.

Potentiella intervjupersoner och kontaktuppgifter hämtades på internet. Vi begränsade urvalet av potentiella intervjupersoner till olika varianter av chefer med motiveringen att vi trodde att dessa personer möjligtvis besitter kunskap kring hur den kommunala verksamheten hanterar

cybersäkerhet. En del av de potentiella intervjupersonerna var slumpmässiga chefer inom kommunal verksamhet, en del var chefer som besitter kunskap om digitalisering. Urvalet gjordes för att få en variation och eventuellt kunna se en skillnad i svar.

Avgränsningen till de tre utvalda kommunerna A, B och C baserades på möjligheten att få kontakt då vi med kommun C hade problem att få intervjutider, vi valde därmed att rikta oss mot mindre kommuner som vi trodde hade större möjlighet att få kontakt med. På grund av studiens tidsram var det viktigt att få tid för intervju snabbt, därför valde vi närliggande kommuner. Då studien inte syftar till att undersöka specifika kommuner i någon form av kategorisering, är urval av studerade kommuner ej väsentligt. Vi vill i studien se en generell bild av hur olika kommuner ställer sig till våra frågeställningar.

3.3 Genomförande

Vi mejlade både ett antal slumpmässiga chefer och ett antal som hade kunskap om digitalisering inom respektive kommun. I mejlet presenterade vi studien och frågade om det fanns intresse för medverkan. Vart och hur intervjuerna ska genomföras bör presenteras till intervjupersoner med flexibilitet för att öka möjligheten att få en intervju (Carlsson & Carlsson, 2020). I vår kontakt med intervjupersoner var vi tydliga med att tid och plats för intervjuerna kunde anpassas efter intervjupersonens schema, vårt önskemål var att intervjuerna skulle ske innan december och att vi föredrog att träffas på plats. Vi var dock flexibla gällande våra önskemål då majoriteten av intervjupersonerna föredrog att intervjun skulle ske digitalt via verktyget Teams, tre intervjuer genomfördes även i december.

Vi genomförde sju intervjuer där två genomfördes på intervjupersonernas arbetsplatser och fem genomfördes digitalt via Teams. Samtliga intervjuer spelades in med röstmemon och följde vår intervjuguide blandat med spontana frågor. Varje intervju inleddes med att informera intervjupersonerna att deras svar kommer att vara anonyma samt att transkribering och ljudinspelningar kommer att raderas efter bruk.

Carlsson och Carlsson (2020) anser att transkribering kan underlätta analysarbetet och menar att man bör transkribera i den utsträckning man har tid för då det är en process som kan ta lång tid, vi valde därmed att transkribera ljudinspelningarna med hjälp av AI-tjänsten Good Tape, då att ta hjälp av tjänsten sparade oss tid. Vi lyssnade igenom ljudinspelningarna och

korrigerade fel i transkriberingen för att säkerställa att AI-tjänsten gett rätt information. Vi färgmarkerade relevanta citat och viktiga svar för att underlätta resultat- och analysarbetet.

Del av titel	**I text nämnd som**	**Längd på intervju**
Sektorschef, Kommun A	Chef 1	35:20
Verksamhetschef, Kommun B	Chef 2	21:14
Verksamhetschef, Kommun B	Chef 3	22:08
Verksamhetschef, Kommun B	Chef 4	19:33
Digitaliseringschef, Kommun A	Chef 5	28:48
Verksamhetschef, Kommun A	Chef 6	42:23
IT-chef, Kommun C	Chef 7	15:19

Tabell 1: Respondenter och längd på intervju

3.3.1 Analys av data

Vid analys av datan från intervjuerna noterade vi viktiga svar från varje chef med färgmarkeringar. I analysen av datan hade vi vår teoretiska referensram i åtanke och valde därmed ut svar som hade kopplingar till den. Vi samarbetade i att välja ut den empiri från transkriberingen som var väsentlig för uppsatsens frågeställningar och syfte

När vi använde den teoretiska referensramen för att analysera empirin ansåg vi att den bästa metoden för att inte missa kopplingar var att skriva enskilda kortfattade analyser för att sedan väva ihop de två versionerna till en. Då vi är två uppsatsskribenter finns det en risk att vi gör olika kopplingar i analysen, för att skriva en sammanhängande analys var det viktigt att samarbeta.

Vi hade under arbetets gång i åtanke att ha en röd tråd i uppsatsen samt att skapa en tydlig struktur i arbetet. Vi undvek en missvisande redovisning genom att ange empirin korrekt i enlighet respondenternas svar (Theodorsson, 2020).

3.3.2 Sökprocess

I sökningen av artiklar till tidigare forskning och den teoretiska referensramen använde vi oss av Göteborgs Universitetsbiblioteks tjänst Supersök och Google Scholar. Sökord som användes var till exempel cybersecurity, artificial intelligence, public sector, public administration, cyberthreat, digitalization och internet of things.

3.4 Forskningsetiska överväganden

I processen att utföra studien har vi förhållit oss till Vetenskapsrådets forskningsetiska principer.

Informationskravet innebär att respondenter ska informeras om studiens syfte samt vilka som är ansvariga för studien och insitutionsanknytning (Vetenskapsrådet, 2002). Informationskravet har följts genom att ange den sortens information i mejl om förfrågan om deltagande.

Samtyckeskravet innebär att respondenterna behöver ge samtycke till deltagande i studien (Vetenskapsrådet, 2002), detta skedde både digitalt via mejl och muntligt.

Konfidentialitetskravet uppmanar till att uppgifter om respondenter ska till största grad hållas hemliga (Vetenskapsrådet, 2002). Kravet uppfylls då inga uppgifter om namn, exakt titel, kommunnamn eller annan information som kan röja respondenternas identitet presenteras i uppsatsen.

Nyttjandekravet innebär att insamlade uppgifter endast får användas i forskningsändamål (Vetenskapsrådet, 2002). Det har ej samlats in personuppgifter utöver namn på respondenter, namnen hålls hemliga och byts ut till andra benämningar i uppsatsen. Respondenternas svar används endast i uppsatsen.

3.5 Studiens kvalitet

Börjesson och Karlsson (2020) menar att trovärdighet är en viktig del av den etiska aspekten i uppsatsskrivande, läsaren ska uppleva att uppsatsen är trovärdig och det författarna skriver och rapporterar om stämmer. Transparens, triangulering och återkoppling till fältet är tre delar av trovärdighet i kvalitativ forskning (Svensson & Ahrne, 2015). Vi har i vår studie tydligt redogjort för tillvägagångssätt, genomförande och val av metod, det ger läsaren möjlighet att kritisera våra val vilket tyder på transparens (Svensson & Ahrne, 2015). Vi har inte använt oss

av triangulering på grund av den tidsram som studien ska utföras inom, vi anser att det vore svårt att hinna använda flera metodval även om vi hade kunnat kombinera intervjuer med kvalitativt sekundärmaterial i form av dokumentanalys (Solli, 2020). Vi har inte återkopplat till fältet då vi varit noggranna med att använda empirin korrekt.

Vidare har vi för att säkerställa trovärdighet i uppsatsen har vi noggrant valt ut pålitliga källor i form av peer-reviewed artiklar, rapporter från myndigheter och organisationer, avhandlingar, böcker och hemsidor som vi anser är trovärdiga.

En studies generaliserbarhet kan påverka dess trovärdighet då en trovärdig studies resultat kan appliceras på andra miljöer, områden och personer. En utmaning med kvalitativa studier är att generalisera resultatet, dock kan jämförelser göras med tidigare forskning (Svensson & Ahrne, 2015). Det är svårt att avgöra om det går att applicera resultatet på en annan miljö, område eller personer då det krävs en ny studie för att veta detta. Det kan vara möjligt att applicera studiens resultat på andra kommuner då urvalet av kommuner inte kategoriseras utan valdes utifrån tillgänglighet vilket kan tyda på ett generellt resultat. I slutsatsen presenteras delar av studiens resultat som återfinns i tidigare forskning, detta tyder på generaliserbarhet.

En svaghet i studien kan vara att spridningen bland respondenterna är ojämn då vi intervjuade en person i kommun C medan det var tre personer i respektive kommun A och B. Vi är medvetna om den ojämna fördelningen och det beror på att endast en person kunde delta i studien i kommun C. Studiens syfte är inte att se skillnader mellan olika kommuner och därmed anser vi att fördelningen fungerar. Spridningen mellan rollerna i de olika kommunerna är också en begränsning då vi inte fick kontakt med alla roller i de olika kommunerna.

4. Resultat

I följande kapitel kommer empirin som studien resulterat i utifrån sju stycken intervjuer att presenteras. Empirin är uppdelad i sex olika delar med rubriker som beskriver presenterad empiri.

4.1 Artificiell intelligens i offentlig verksamhet

Inledningsvis presenteras respondenternas attityd till användning av AI i offentlig sektor.

Samtliga respondenter ser användningen av AI inom offentlig sektor både som en möjlighet och risk. Det fanns en genomgripande positiv inställning till användningen och framfarten av AI bland respondenterna, samtidigt kunde samtliga se de risker som medkommer. Möjligheterna med AI var enligt respondenterna att det kan användas som hjälpmedel, effektivisera administration, utveckla verksamheten, försvara verksamheten mot cyberattacker, öka service och förbättra arbetet där det finns personalbrist. Risker kopplat till användning av AI inom offentlig sektor var enligt respondenterna viktigt att inte vara naiva, enligt chef 1 bör man inte lita blint på AI. Chef 7 lyfter säkerhetsaspekten kopplat till AI där det finns kapacitet att använda AI till rena angrepp, intrångsförsök samt skapande av information och desinformation. Majoriteten av respondenterna var medvetna om att cyberattacker kan utföras med artificiell intelligens. Chef 2 menar att det inte förekommit diskussioner om säkerhetsaspekten av AI.

Både chef 7 och chef 3 förtydligar att AI kan vara både en möjlighet och risk inom den kommunala verksamheten i kommande citat.

'' Så det blir väl liksom kampen från båda håll, så likväl som att det kan bygga bättre cybersäkerhet så kan det också öka attackerna cybersäkerhetsmässigt'' (Chef 7, kommun C).

''Den kan nog vara att den kan hjälpa oss ju mycket men den kan säkert skapa en hel del obehag för oss också'' (Chef 3, kommun B).

Chef 5 tar vid föregående två chefer och berättar gällande användning av AI i offentlig sektor att det bör finnas en proportionalitet mellan nytta och risk, hen menar att det digitala ofta får en orättvis behandling då det ofta förekommer krav att digitala plattformar och lösningar ska innebära noll risk, vilket icke digitala lösningar inte har som krav. Chef 5 menar att det krävs riskbedömningar av värdet av AI-lösningar samtidigt som man ser värdet i att förenkla, förbättra, öka service utifrån de välfärdsutmaningar som kommuner står inför.

''Vem är det som styr vad vi ska göra med AI? Ja, men om vi i offentlig sektor tar lid på vad vi vill ha det till, så är just sannolikheten större att man använder det till gott'' (Chef 5, kommun A)

Chef 2 menar att införande av AI-lösningar i hens förvaltning mer sannolikt kommer innebära en påverkan på professionerna än på cybersäkerheten. AI-lösningar kan enligt chef 2 innebära färre antal anställda i framtiden. Chef 6 har en önskan om att kommunen utifrån cybersäkerhetsperspektivet borde ta fram en AI-policy som bland annat förklarar vilka AI-verktyg som är säkra att använda av anställda, då hen misstänker anställda hade känt sig mer bekväma i att använda AI-tjänster om policys fanns. Chef 4 vill att användningen av AI ska vara reglerad och säker samt att EU bör tillhandahålla spelregler för att ytterligare reglera AI.

4.2 Den tröga förvaltningens påverkan på digitaliseringen inom kommunal verksamhet

Följande avsnitt tar upp den påstått tröga utvecklingen i offentlig sektor och hur detta tillsammans med digitaliseringens framfart kan påverka kommunernas cybersäkerhet.

Samtliga respondenter ansåg att bilden av den tröga förvaltningen stämmer, de menar att utvecklingen inom kommuner går långsammare än omvärlden, speciellt sett till digitaliseringens framfart. Chef 1 förklarar att det inom offentliga verksamheter kan finnas en osäkerhet inför förändringar, och att det snarare är osäkerheten som ligger grund till trögheten än ovilja. Vidare menar chef 1 att medborgarnas trygghet i att beslut tas i enlighet med lagar och legitimitet är en viktig del av offentliga sektorns arbete, vilket kan leda till att saker tar längre tid, och kommunens styrkor är viktigare än digitaliseringens framfart i sig.

"*En kommun ska vara bra på att vara kommun*" (Chef 1, kommun A).

Den långsamma förändringen inom förvaltningen kan enligt chef 2 förstås som en inbyggd säkerhetsåtgärd för anställda, trögheten fungerar som en trygghet och bromskloss som gör att förändringar inte går alltför snabbt fram.

Chef 5 förklarar att det finns en inbyggd tröghet i offentlig sektor eftersom sektorns uppgift är att förvalta det befintliga istället för att dra nytta av de möjligheter som finns. Hen har upplevt att det finns en vilja att ta hjälp av digitaliseringens möjligheter, men det finns en brist gällande kunskap, omställningsförmåga och resurser, vilket nästkommande citat förtydligar.

''Så som det egentligen ser ut är att vi är bäst i världen på att förstå digitaliseringens möjligheter. Det vill säga att vi skriver rapporter och förstudier, underlag och strategier och policys i all evighet för hur vi borde göra. Men sen när det kommer till görandet och vem ska bygga de här, alltifrån cybersäkerheten till AI-tjänsterna till de digitala omställningsmöjligheterna så har vi inte varken kunskapen eller förmågan eller resurserna att göra det.'' (Chef 5, kommun A).

Den tröga förvaltningens natur påverkar möjligheten för kommuner att följa med i digitaliseringens framfart.

''... kommunerna har ju liksom en digital skuld, alltså vi ligger så jädrans långt bakåt så att det kommer ju aldrig, vi kommer inte överleva, som organismer utifrån hur digitaliseringen rusar fram.'' (Chef 6, kommun A).

Chef 6 tror att kommuner på många sätt kan hantera digitaliseringens framfart, men samtidigt kan de på många sätt inte hantera det. Hen menar att kommunen inte använder sig av digitaliseringen fullt ut även om de hade kunnat. Chef 6 använder ett exempel där kommunen fortfarande använder blanketter och brev som transporteras mellan kollegor inom vissa delar av arbetet, trots att det skulle vara möjligt att utföra digitalt. Hen tror även att frågan om digitaliseringen inom den tröga förvaltningen är en generationsfråga, yngre har lättare att ställa om till förändringar.

Chef 7 förklarar i kommande citat att digitaliseringen innebär en ny värld och med detta tillkommer det risker.

''Här är det en helt ny värld så att det tillför ju en helt ny riskbild och framförallt också att vi kanske är lite omogna där och inte bara vi, utan de flesta är ju ganska omogna i det digitala'' (Chef 7, kommun C).

4.3 Rutiner för cybersäkerhet

Avsnittet presenterar rutiner och den organisering som finns inom de kommunala verksamheterna kring cybersäkerhet.

Flertalet respondenter berättade att användningen av mejl ingår i de arbetsrutiner som anställda uppmuntras vara vaksamma över på grund av säkerhetsrisken. Samtliga respondenter nämner att det inom respektive kommun finns brandväggar och liknande grundskydd, flertalet av respondenterna berättar att dessa skydd i ett tidigt skede sållar bort misstänksamma mejl. Chef 1 och chef 3 berättar att trots skydden nås anställda emellanåt av misstänksamma mejl, chef 2 har en motsatt upplevelse där anställda inte nås av detta. Chef 5 berättar att det finns inbyggda tekniska funktionaliteter i mejlen, till exempel notiser som uppmärksammar anställda om nya mejlkontakter. Majoriteten av respondenterna har en rutin att rapportera incidenter, avvikelser och misstänksamma mejl och telefonsamtal till säkerhetsavdelningen i respektive kommun. Chef 1 berättar även att IT-avdelningen i kommuner ibland skickar ut bluffmejl till anställda för att öka medvetenheten om cybersäkerhet, en form av påminnelse om att vara vaksam.

Det finns bland respondenterna en försiktighet i att inte kommunicera känsliga uppgifter via mejl, denna arbetsrutin syftar både till säkerhetsaspekter, sekretesslagstiftningen och offentlighetsprincipen då mejl kan begäras ut som allmän handling.

Utöver försiktigheten i hantering och kommunikation i mejl samt anmälningar till säkerhetsavdelningar menar chef 2 och chef 4 att det inte finns specifika arbetsrutiner kopplade till cybersäkerhet inom deras respektive förvaltning. Resterande respondenter berättar att arbetsrutiner kopplat till cybersäkerhet kan vara strategier, tvåfaktorsautentisering, anvisningar för användning av digitala verktyg och reserv- eller kontinuitetsplaner. Chef 4 uttrycker att hen

inte känner till att det inte förekommer specifika arbetsrutiner kopplat till cybersäkerhet inom hens förvaltning och uttrycker därmed i kommande citat att kommunen är underkänd i att upprätta arbetsrutiner kring cybersäkerhet.

''Så blir det ju ett underkännande där. Så att om inte jag vet det så vet ingen annan heller det'' (Chef 4, kommun B)

Chef 1 berättar att anställda inom kommunen meddelas om att regelbundet byta lösenord och använda tvåfaktorsautentisering. Chef 1 har upplevt en frustration hos anställda i de två arbetsrutinerna, dock finns det en dialog inom kommunen där anställda informeras varför det krävs lösenordsbyten regelbundet för att de anställda ska förstå att det är en viktig säkerhetsåtgärd.

Samtliga respondenter anger att det inom respektive kommun finns antingen någon form av IT-policy, IT-strategi, IT-avdelning, säkerhetsenhet eller digitaliseringsenhet. IT-policys inkluderar i vissa fall cybersäkerhet, det finns inga specifikt utformade policys för cybersäkerhet. IT-avdelningarna brukar enligt flertalet respondenter informera om cybersäkerhet.

4.4 Medvetenhet om cybersäkerhet bland anställda

I följande avsnitt presenterar respondenterna upplevd medvetenhet om cybersäkerhet i verksamheten.

Majoriteten av respondenterna uppgav att det finns en medvetenhet om cybersäkerhet inom kommunen de arbetar i. Graden av upplevd medvetenhet varierar mellan kommun A och B, samtliga respondenter i kommun A svarade att det finns en medvetenhet, medan respondenter inom kommun B beskriver medvetenheten antingen som generell, den finns till viss del eller att anställda är ganska medvetna. Chef 2 menar att det till viss del finns en medvetenhet, anställda känner en trygghet i att använda digitala verktyg men ämnet cybersäkerhet diskuteras inte i stor grad. Medvetenheten ansåg chef 2 var låg före covid-19 pandemin, en ökning skedde dock i takt med pandemin.

Medvetenheten visar sig på följande sätt i nästkommande två citat. Chef 3 syftar till att kommunen blivit utsatta för ett par cyberincidenter.

"Ja, jag tycker det. Det har ju blivit mer och mer… nu när det är så instabilt läge, i världen med kriget i Ukraina, Ryssland, allt det här liksom, Kina. Så är det ännu mer. Det är väldigt mycket nu kring det" (Chef 1, Kommun A)

"Det tror jag nog att alla är ganska så medvetna om, har blivit under den senaste tiden för vi har ju varit utsatta för några stycken så att därför så vet man väl det". (Chef 3, Kommun B)

Citaten tydliggör att medvetenhet uppstår vid omvärldsbevakningen, samtidigt som en annan chef i nästa citat anger att det saknas kontinuerligt tänk kring potentiella risker i cybervärlden.

''...vi bara använder verktygen mer än att vi funderar över dem'' (Chef 2, kommun B)

Chef 4 anser att det finns en generell medvetenhet om cybersäkerhet inom kommunen, anställda har kunskap om säker kommunikation i mejl och hantering av känsliga uppgifter. Chef 4 känner inte till om kommunen bidrar med utbildningar kring cybersäkerhet till anställda, hen tror att de anställdas generella medvetenhet beror på ett omvärldsintresse och säkerhetsmedvetenhet, till skillnad från systematiskt lärande.

''Det finns nog ingen bra systematik eller metodik i hur vi säkrar oss mot cyberattacker'' (Chef 4, kommun B)

Chef 2 och 3 som arbetar inom samma kommun som chef 4 meddelar i enlighet med chef 4 att kommunen inte bidrar med utbildning kring cybersäkerhet till anställda.

Kommunen bidrar till medvetenheten genom kontinuitetsplaner, chefsutbildningar, information på intranät, workshops samt genom att uppmuntra chefer att tala om cybersäkerhet. Det finns en förhoppning om att den information som chefer får om cybersäkerhet ska färdas ner i organisationen ut till de anställda. Chef 1 tror inte att anställda inom kommunen vardagligen tänker specifikt på cybersäkerhet, men de påminns om säkerhetsaspekten kontinuerligt då det

regelbundet krävs lösenordsbyten. Chef 5 som arbetar i samma kommun som chef 1 berättar att kommunen tidigare bidragit med nanaoutbildningar kring cyber- och informationssäkerhet, dock är hen osäker på om det fortfarande genomförs och tror att det kontinuerliga stödet från kommunen har tappats. Chef 5 berättar att det inom kommunen finns tekniska funktionaliteter inbyggda i mejlsystem samt strategier för lagring av data och hur anställda ska tänka och logga in i de digitala systemen.

Chef 6 som arbetar i samma kommun som chef 1 och 5 berättar att hen inte fått någon utbildning kring cybersäkerhet, men hen har fått bra information om cybersäkerhet på andra sätt från kommunen. Hens uppfattning är att varje förvaltning ansvarar för arbetet med cybersäkerhet, det är ingen kommunal angelägenhet. Chef 6 ser brister i det förebyggande arbetet och anser att det borde pratas mer om cybersäkerhet, trots bristerna anser hen att det finns en medvetenhet om cybersäkerhet.

Kommunen chef 7 arbetar i bidrar till medvetenheten om cybersäkerhet genom introutbildningar, årliga utbildningar och information på intranätet.

Återkommande svar från respondenterna var att medvetenheten om cybersäkerhet har ökat under de senaste åren med anledning av Covid-19 pandemin, det instabila världsläget och uppmärksammade cyberattacker. Att det förekommer en högre medvetenhet och diskussion om cybersäkerhet på chefsnivå, säkerhetsenheter och IT-avdelningar är ett återkommande svar från respondenterna. Chef 7 berättar att det förekommer riktade interna utbildningar om cybersäkerhet, dock inte till hela verksamheten utan till riktade målgrupper, information till hela verksamheten ges digitalt.

4.5 Kommunernas förberedelse och kapacitet inför att hantera en cyberattack

I följande avsnitt presenterar respondenterna den förberedelse som finns inom verksamheterna och kapaciteten att hantera en eventuell cyberattack.

Majoriteten av respondenterna uttryckte en tro om att kommunen de arbetar i har god kapacitet att hantera en cyberattack, endast chef 4 i kommun B antog att kommunen hen arbetar i inte har en god kapacitet att hantera en cyberattack. Chef 4 och chef 2 inom samma kommun känner inte till att det finns kontinuitetsplaner eller policys inom kommunen för cyberattacker. Vidare förklarar chef 4 att kommunen har ett grundskydd mot cyberattacker, dock tror hen att om kommunen väl blir utsatt för en cyberattack kommer de vara oförberedda och att diskussionen om åtgärder kommer föras först efter attacken. Chef 3 och 4 som arbetar inom samma kommun tror båda två att de personer som utför cyberattacker alltid kommer att ligga steget före, vilket är en utmaning i arbetet att förbereda kommunen, vilket förtydligas i kommande citat.

''Man kan inte garantera sig mot allting'' (Chef 3, kommun B).

Chef 6 har inom hens förvaltning inga kontinuitetsplaner för arbetet efter en cyberattack, men uppger ändå en tro om att kommunen har en god kapacitet att hantera en cyberattack, dock poängterar hen att det är svårt att veta förrän det faktiskt skett en attack. I likhet med chef 3 tror hen att det är svårt att tänka på precis allt.

''Ungefär som att man kan liksom öva på brand, brandöva hela tiden, vi kan cyberattacköva. Men frågan är om vi kommer kunna täppa till allting som då blir ett faktum om det skulle ske'' (Chef 6, kommun A).

Chef 7 berättar att det inom kommunen finns policys som berör cybersäkerhet, hur verksamheten skyddar sig mot attacker vet bara de personer som ansvarar för det.

Resterande respondenter har kontinuitetsplaner eller policys som beskriver åtgärder som ska vidtas och hur arbetet ska ske vid en cyberattack inom verksamheten. De framgick att det skiljde sig mellan förvaltningar inom samma kommun huruvida det fanns kontinuitetsplaner eller policys. I kommun A angav två respondenter att det fanns antingen kontinuitetsplaner eller policys för cybersäkerhet inom deras förvaltning, medan en tredje respondent angav att det inom hens förvaltning inte fanns den typen av förberedelse, hen berättar dock att resten av kommunen arbetar mycket med åtgärder och kontinuitetsplaner kopplat till cybersäkerhet. Ett omvänt mönster återfinns i kommun B, två respondenter tillhörande olika förvaltningar menar

att det inte finns kontinuitetsplaner eller policys i deras förvaltning, medan en respondent berättar att det förekommer inom hens förvaltning.

De respondenter vars kommun som blivit utsatta för en cyberattack eller annan form av cyberintrång upplevde att kommunen hanterade händelsen bra, trots följder som påverkade verksamheten upplevde respondenterna att det hanterades väl. Chef 5 berättar att kommunen kan vara tekniskt sårbar till viss del vid en cyberattack, men olika policys stärker upp.

4.6 Potentiella förbättringar i arbetet med cybersäkerhet

Avsnittet presenterar de förbättringar och den utveckling som respondenterna menar borde ske i kommunens arbete med cybersäkerhet.

Gemensamt för majoriteten av respondenterna är att det finns utrymme för förbättring inom det kommunala arbetet med cybersäkerhet. Flertalet menar att kommunerna inte klarar av arbetet med cybersäkerhet på egen hand och att de behöver hjälp och stöd i takt med digitaliseringen. Chef 4 tror att Sveriges Kommuner och Regioner (SKR) i framtiden kommer behöva bistå hjälp då kommuner inte kan förstå området på egen hand. Chef 5 menar att det inte finns kapacitet att hantera cyberattacker i många av landets kommuner, både chef 5 och 7 menar att främst små kommuner har svårt att hantera en cyberattack medan större kommuner har kapacitet och fler resurser. Chef 5 tror att kommunernas kapacitet att hantera cyberattacker kan förbättras genom kommunsammanslagningar, nationella mål samt att överlåta IT-driften från kommunerna till andra aktörer. Chef 5 menar att 290 separata driftorganisationer ansvarar för IT i den egna kommunen inte är det bästa när det finns möjlighet att skala upp och ha nationella mål.

''De lägger alla sina resurser på att överhuvudtaget kunna leverera någon typ av digital infrastruktur och service till medarbetare och invånare. Det ligger liksom precis med näsan över vattnet och att även då lägga stort fokus på när det kommer attacker och motstånd till det, det är ju egentligen omöjligt.'' (Chef 5, kommun A).

Chef 5 menar att det är en utmaning för enskilda kommuner att lägga resurser på cybersäkerhet då resurserna knappt räcker till att leverera digital infrastruktur.

Chef 6 berättar att IT-avdelningen i kommunen har ett utbrett säkerhetstänk vid val av systemleverantörer, de vill säkerställa att systemet inte kommer från tredje part. Chef 6 tror att svaga och föråldrade system kan vara en svag punkt i kommuner då de är lätta att attackera, vilket blir en utmaning i cybersäkerhetsarbetet då avtal med systemleverantörer kan ha upphandlats för länge sen och vilket kan innebära att de inte hänger med i den digitala utvecklingen.

4.7 Hur uppfattar anställda inom kommunal verksamhet hotet om cyberattacker

Följande avsnitt presenterar hur anställda inom kommunal verksamhet upplever hotet om cyberattacker.

Det fanns en uppfattning om att hotet om cyberattacker mot den kommunala verksamheten har ökat i takt med den accelererande digitaliseringen. Chef 3 poängterar att ju mer digital en kommun blir desto större är risken att bli utsatt för en cyberattack. Enligt chef 7 har det skett en tydlig ökning av hotet om cyberattacker i takt med omvärlden.

''...med omvärldsläget i sig men också den till exempel den organiserade brottsligheten och tredje land. Vi har ju miljontals egentligen attacker varje dag som stoppas av brandväggar och andra skydd. Så vi vet ju att vi är utsatta dagligen för extremt många attacker helt enkelt och en offentlig sektor är väl alltid också ett utsatt mål ur vissa perspektiv'' (Chef 7, kommun C)

Det fanns två respondenter som nedtonade hotet. Chef 5 menar att kommunen hen arbetar i inte har något större hot mot sig än andra offentliga verksamheter medan chef 2 upplever att det finns ett generellt hot som varit oförändrat de senaste åren.

Chef 4 tror att det inom hens kommun i framtiden kommer att etableras en bra cybersäkerhet då det finns ett intresse för det, samtidigt poängterar hen att intresset för cybersäkerhet ska konkurrera med alla andra intressen som finns inom en kommun.

5. Analys/Diskussion

I kommande kapitel kommer empirin analyseras tillsammans med den teoretiska referensramen. Kapitlet är strukturerat utefter den teoretiska referensramens fem aspekter som återkommer inom fältet i tidigare forskning.

5.1 AI som aspekt - möjlighet eller hot

Följande del relaterar till frågeställningen:

- *Hur uppfattas hotet mot cybersäkerheten i accelerationen av digitaliseringen/AI?*

Utifrån empirin kan det konstateras att samtliga respondenter ser AI både som en möjlighet och ett hot inom den kommunala verksamheten. Respondenterna anser att AI är en möjlighet då det kan användas som verktyg att komplettera och effektivisera administration, utveckla verksamheten, ett hjälpmedel, öka service samt bidra till arbetet där det förekommer personalbrist. Automatiserat beslutsfattande kan även bidra till ett effektivare arbete inom verksamheten (Henman, 2020; Wirtz et al., 2019; Mergel et al., 2023). Enligt en respondent bör det finnas en proportionalitet mellan nytta och risk, kommuner bör nyttja effektiviseringen som AI-teknik innebär samtidigt som de vakar över riskerna. Det finns bland respondenterna en önskan om att AI ska kontrolleras då det är en omogen företeelse, en alltför snabb utveckling kan leda till att offentliga verksamheter inte kan utföra adekvat styrning (Writz et al., 2020). Det fanns bland respondenterna en idé om att EU bör tillhandahålla spelregler för användningen av AI.

Cyberkriminella kan utnyttja AI-teknik för att begå brott och cyberattacker mot offentliga verksamheter, genom den accelererande utvecklingen av AI-teknik kommer cyberattacker kunna utföras självständigt utan mänsklig hjälp (Khisamova et al., 2019). I likhet med Henman (2020) och Guembe et al. (2022) menar ett antal respondenter att AI kan användas som försvar mot cyberattacker inom den kommunala verksamheten, AI ska bekämpa AI. Bland respondenterna fanns det en upplevd bristande diskussion om säkerhetsarbetet kring AI, det förekom sällan AI-policys och utbildningar om AI. En respondent menar att om kommunen bidrog med utbildning kring AI hade anställda känt sig tryggare i att använda AI tjänster.

Norris et al. (2021) menar att det fanns en okunskap i offentliga verksamheter kring förekomsten av cyberhot, samma okunskap återfanns inte bland respondenterna då majoriteten var medvetna om eller hade hört att AI kan användas i cyberattacker, det fanns även en kunskap om att offentliga verksamheter är utsatta för cyberattacker. Om respondenterna är medvetna hur ofta cyberattacker sker mot kommuner framgick ej förutom hos en respondent.

En respondent påpekade i likhet med Susskind och Susskind (2017) att professionerna inom kommunen i framtiden kommer påverkas eller försvinna i samband med framfarten av AI. Respondenten berättar att det inom den kommun hen arbetar i finns planer att implementera AI-teknik vilket med stor sannolikhet kommer innebära att arbetstillfällen försvinner.

Sammantaget menade respondenterna att användandet av AI borde utvecklas inom offentlig sektor med tanke på de möjligheter som finns och hur det kan hjälpa den kommunala verksamheten med cybersäkerhet. Kontroll måste dock finnas och en medvetenhet om risker och olämpliga användningsområden.

5.2 En trög förvaltning i accelererande omvärld

Följande del relaterar till frågeställningen:

- *Hur uppfattas hotet mot cybersäkerheten i accelerationen av digitaliseringen/AI?*
- *Vilka arbetsmetoder använder kommunen för att säkerställa cybersäkerheten för verksamheten?*

Samtliga respondenter menade i enlighet med Melin (2018) att utvecklingen inom den kommunala verksamheten kan ses som trög, speciellt sett till digitaliseringens framfart. Majoriteten menade att det låg i förvaltningens natur att utveckling ska ske långsamt, vilket är en utmaning då digitaliseringen i omvärlden sker snabbt. Resurs- och kunskapsbrist, osäkerhet inför förändringar och medborgares trygghet är enligt respondenterna tänkbara orsaker till att digitaliseringen inom den kommunala verksamheten inte är utbredd. Lagar, legitimitet och strävan att göra rätt är enligt en respondent en grund för att digitaliseringen går långsamt i likhet med Andréasson (2015). Kombinationen av en accelererande digitaliserad omvärld och en trög förvaltning kan innebära att kommuner inte kan hantera de nya varianterna av cyberattacker

som dyker upp i takt med teknikens utveckling, till exempel AI styrda cyberattacker (Guembe et al., 2022). En respondent förtydligar att kommuner på grund av sin tröga natur har en digital skuld som är svår att ta igen.

Trots att utvecklingen sker långsamt inom offentlig sektor finns det enligt respondenterna en vilja att ta hjälp av digitala verktyg och AI både i det kommunala arbetet och som skydd mot cyberattacker, men det saknas kunskap, kompetens och resurser. Respondenternas svar överensstämmer med Campion et al. (2020) att offentlig sektor är i ett tidigt utvecklingsstadie gällande implementering av AI-teknik trots ett intresse och vilja använda digitaliseringens möjligheter till den kommunala verksamhetens fördel.

5.3 Arbetsmetoder och organisering kopplat till cybersäkerhet

Följande del relaterar till frågeställningen:

- *Vilka arbetsmetoder använder kommunen för att säkerställa cybersäkerheten för verksamheten?*

Utifrån empirin syntes olika arbetsmetoder bland de olika kommunernas förvaltningar, det fanns en variation bland respondenterna i antal förekommande rutiner med syfte att skydda verksamheten mot cyberattacker. Grundläggande skydd mot cyberattacker fanns i form av brandväggar hos samtliga kommuner med syfte att skydda mot cyberintrång och misstänksamma mejl. Wirtz och Weyerer (2017) betonar att offentliga verksamheter måste vidta skyddsåtgärder i form av brandväggar, utbildningar för anställda, antivirusprogram och kryptering. Respondenterna rapporterade endast om brandväggar och utbildningar för anställda. Skyddsåtgärderna resulterar i att anställda inte nås av suspekt material och cyberattacker motas bort. Utifrån empirin kan det konstateras att samtliga kommuner har identifierat mejl som en digital svaghet då samtliga respondenter rapporterar att det sker en varsam hantering och kommunikation i mejl. Arbetsmetoden går i linje med Wrtiz och Weyerer (2017) varning om den potentiella cybersäkerhetsrisken kopplat till mejl samt deras poängtering att offentliga verksamheter kan stärka sitt skydd mot cyberhot genom att identifiera svagheter, Demertzi et al. (2023) betonar även tyngden i att identifiera svagheter. Det förekommer i en kommun att IT-avdelningen sänder ut bluffmejl för att testa de anställdas medvetenhet om suspekta mejl. I

samtliga kommuner finns en rutin om att rapportera misstänksamma incidenter till motsvarande säkerhetsenhet inom respektive kommun.

En respondent rapporterade att det förekommer tvåfaktorsautentisering och regelbundna lösenordsbyten inom kommunen. Samtliga respondenter har någon form av IT-policy som adresserar cybersäkerhet, däremot förekommer det inga specifikt utformade policys för cybersäkerhet som Hatcher et al. (2020) menar är viktigt. Ett antal respondenter menar att det förekommer fler metoder och rutiner kopplat till cybersäkerhet hos IT-avdelningen och säkerhetsenheten i respektive kommun.

De rekommendationer som Norris et al. (2019) presenterar återfanns ej i stor utsträckning i empirin. Samtliga respondenter rapporterar att det finns medvetenhet kring cybersäkerhet genom hela verksamheten, dock finns det respondenter som rapporterar om en högre medvetandegrad och andra som rapporterar om en lägre medvetandegrad. Utifrån den bild respondenterna ger kan det tolkas som att det mer eller mindre finns en kultur för cybersäkerhet genom hela verksamheterna. Utifrån empirin syns inget som tyder på att verksamheterna adresserar det som sätter stopp för utvecklingen av cybersäkerhet, istället syns en bild av den tröga förvaltningen där digital utveckling sker långsamt. Det framgår ej genom empirin om kommunerna följer bästa praxis för cybersäkerhet.

Ramverket som presenteras av Safitra et al. (2023) återfinns i empirin då en respondent berättar om hur chefer uppmuntras till att informera anställda om cybersäkerhet samt att samtliga respondenter rapporterar till säkerhetsenheter när de möter misstänksamma mejl och incidenter.

En respondent tar upp problematiken kring föråldrade och svaga digitala system bland kommuner som är lätta att attackera. Hen berättar att digitala system upphandlas för att användas under långa perioder men tekniken som upphandlats hänger inte med i digitaliseringen. Wu et al. (2018) berättar om samma problematik då det krävs utveckling av gamla system gällande åtkomstkontroll, kryptering och tekniker för att upptäcka intrång.

5.4 Medvetenhet om cybersäkerhet

Följande del relaterar till frågeställningarna:

- *Hur uppfattas hotet mot cybersäkerheten i accelerationen av digitaliseringen/AI?*
- *Vilka arbetsmetoder använder kommunen för att säkerställa cybersäkerheten för verksamheten?*

Majoriteten av respondenterna upplevde en medvetenhet om cybersäkerhet, ett antal respondenter upplevde dock en lägre grad medvetenhet, Norris et al. (2019) är av uppfattningen att det är viktigt att det finns en medvetenhet om cybersäkerhet inom offentliga verksamheter, vilket respondenterna rapporterar att det finns. Flertalet respondenter från samtliga kommuner menar att medvetenheten om cybersäkerhet och cyberattacker inom kommuner kommer från omvärldsbevakning då anställda tar lärdom från uppmärksammade cyberattacker, det instabila världsläget och Covid-19 pandemin. En respondent är av tron att den medvetenhet som existerar om cybersäkerhet i kommun B beror på omvärldsbevakning då kommunen ej bidrar med information eller utbildning kring cybersäkerhet till de anställda, resterande respondenter inom samma kommun rapporterade att de inte går utbildningar om cybersäkerhet. Writz & Weyerer (2017) poängterar att en viktig del av cybersäkerhet är att anställda inom en verksamhet får utbildning om ämnet. Däremot bidrar kommun A och C med olika varianter av utbildningar och information som berör cybersäkerhet.

I likhet med Hatcher et al. (2020) var det omkring 40% av respondenterna som ej fick utbildning om cybersäkerhet av kommunen. Trots att respondenterna i kommun B har en medvetenhet om cybersäkerhet utifrån omvärldsbevakning är det inte säkert att den informationen är tillräcklig, Khando et al. (2021) menar att anställda som inte besitter information om säkerhetsåtgärder kan utgöra en risk för verksamheten där känslig information kan spridas på grund av naivt och oaktsamt agerande. Utifrån empirin går det inte att avgöra om respondenterna i kommun A och C besitter information om säkerhetsåtgärder som hindrar naivt eller oaktsamt agerande trots utbildning och information från kommunerna, till exempel berättar en respondent om en tro att det krävs mer diskussion om cybersäkerhet inom kommunen.

Ett antal respondenter menar att det på chefsnivå, säkerhetsenheter och IT-avdelningar finns en större medvetenhet om cybersäkerhet, vilket inte överensstämmer med Writz och Weyerer

(2017) som menar att medvetenheten om cybersäkerhet i många fall brister på chefsnivå. Samtidigt vittnar andra respondenter som alla är chefer, om att det finns en medvetenhet som beskrivs som generell, finns till viss del eller att anställda är ganska medvetna, vilket kan tyda på en bristande medvetenhet.

5.5 Förberedelse och kapacitet att bemöta en cyberattack

Följande del relaterar till frågeställningen:

- *Vilka arbetsmetoder använder kommunen för att säkerställa cybersäkerheten för verksamheten?*

Enligt respondenterna finns det en övergripande tro att respektive kommun kan hantera en cyberattack, en respondent menar dock att kommunen är oförberedd på att hantera en cyberattack. Respondenten tror att diskussionen om åtgärder kommer dyka upp inom kommunen först efter att en cyberattack skett, samma respondent samt en till inom samma kommun vittnar båda om att de inte känner till att det existerar kontinuitetsplaner kopplat till cybersäkerhet inom kommunen. Antagandet går i linje med Caruson et al. (2012) som menar att offentliga verksamheter ofta är mer reaktiva än proaktiva i implementeringen av cybersäkerhetspolicys, dock rapporterar flertalet respondenter att det förekommer kontinuitetsplaner och IT-policys vilket går emot Caruson et al. (2012) påstående. En respondent som anser att kommunen har en god kapacitet att hantera en cyberattack poängterade dock att det är svårt att avgöra innan det faktiskt skett en cyberattack. Det kan anses oroväckande att det förekommer respondenter som är av tron att kommunen inte är väl förberedda på att hantera en cyberattack då kommuner i takt med den accelererande digitaliseringen blivit mer mottagliga för cyberattacker. Förekommer det inga åtgärder för återhämtning eller prevention kan kommunen efter en cyberattack ha en stillastående verksamhet i dagar eller månader efter en attack (Preis & Susskind, 2022).

Flertalet respondenter rapporterade att det finns tydliga kontinuitetsplaner och åtgärder för hur anställda ska kunna fortsätta arbeta efter en cyberattack, detta tyder på ett kontinuerligt och förberedande arbete med cybersäkerhet vilket kan underlätta hanteringen innan, under och efter en cyberattack (Safitra et al., 2023).

I empirin kan ett varierande resultat ses gällande förekomsten av kontinuitetsplaner där förekomsten skiljer sig åt mellan olika förvaltningar inom samma kommun, detta är tecken på bristande koordination och samarbete genom verksamheten som Caruson et al. (2012) menar är viktigt för en lyckad cybersäkerhetspolicy.

Norris et al. (2019) och Safitra et al. (2023) menar att offentliga verksamheter bör vara uppmärksamma för den konstanta utvecklingen av cyberattacker och utefter det anpassa åtgärder, flertalet respondenter menar att det finns en medvetenhet om uppmärksammade cyberattacker i omvärlden, det framgår dock ej om åtgärder anpassas till detta.

Majoriteten av respondenterna uttrycker att det bör ske förbättringar i arbetet med cybersäkerhet inom kommunerna. Det är enligt respondenterna en utmaning för kommunerna att i takt med den accelererande digitaliseringen hantera cybersäkerheten på egen hand. Bland respondenterna ges förslag till att förbättra kapaciteten i form av stöd från SKR, kommunsammanslagningar, nationella mål, IT-drift bör skötas av andra aktörer samt stöd från säkerhetsavdelningar. Förslagen går i linje med Hatcher et al. (2020) som menar att kommuner bör ta hjälp av utomstående aktörer och staten i arbetet med cybersäkerhet.

En respondent menar att den bristande kapaciteten att hantera cyberattacker inom kommunen beror på bristande resurser, vilket går i linje med Caruson et al. (2012) och Hatcher et al. (2020) som menar att bristande finansiella resurser hindrar arbetet med cybersäkerhet.

6. Slutsats

I det avslutande kapitlet presenteras till en början svar på studiens frågeställningar, därefter behandlas syfte, studiens bidrag och avslutningsvis förslag till vidare forskning.

6.1 Första frågeställningen

- *Hur uppfattas hotet mot cybersäkerheten i accelerationen av digitaliseringen/AI?*

Vår studie visar att anställda inom den kommunala verksamheten har en medvetenhet om cybersäkerhet i sitt arbete, graden av upplevd medvetenhet kan variera, detta är ett motsatt resultat till vad Wirtz & Weyerer (2017) påvisade i sin studie då dem menade att chefer och ledare inom den offentliga förvaltningen brister i medvetenhet om cybersäkerhet.

En del av medvetenheten om hotet mot cybersäkerheten i den kommunala verksamheten har under de senaste åren ökat på grund av omvärldsbevakning där anställda fått till sig information genom uppmärksammade cyberattacker, covid-19 pandemin och det instabila läget i världen. Det finns en uppfattning om att hotet mot cybersäkerheten i den kommunala verksamheten har ökat i takt med digitaliseringen och att allt fler anställda är uppmärksamma för hot om cyberattacker. Det finns en önskan och ett behov av stöd och hjälp av andra aktörer i arbetet att säkra kommunen mot cyberattacker då det är en stor utmaning för kommuner att hantera detta på egen hand i den accelererande digitaliseringen, vilket även Hatcher et al. (2020) menar att de finns ett behov av.

Studien visar att det finns en önskan om att använda digitala verktyg inom den kommunala verksamheten, bland annat AI-teknik. Det finns en tydlig positiv inställning till möjligheterna som AI-teknik kan innebära inom den offentliga sektorn, möjligheterna innefattar att effektivisera, öka service, agera hjälpmedel och försvara verksamheten mot cyberattacker. Samtidigt är anställda inom den kommunala verksamheten medvetna om de säkerhetsrisker som AI kan innebära och anser att det bör finnas en proportionalitet mellan nytta och risk.

Enligt studien är den tröga förvaltningens natur en anledning till att digitaliseringen inom den kommunala verksamheten går långsamt. På grund av den tröga naturen kan det vara svårt för kommuner att hantera nya varianter av cyberhot som dyker upp i takt med den digitaliserade omvärlden.

6.2 Andra frågeställningen

- *Vilka arbetsmetoder använder kommunen för att säkerställa cybersäkerheten för verksamheten?*

Studien påvisar att det förekommer förutbestämda arbetsrutiner kopplat till cybersäkerhet inom den kommunala verksamheten i form av försiktighet i hantering av mejl, kontinuitetsplaner, brandväggar, rapportering av suspekta incidenter, tvåfaktorsautentisering och IT-policys. Studien visar samtidigt att det i vissa fall inte finns specifika arbetsrutiner som anställda uppmuntras att följa som syftar till att säkerställa cybersäkerheten. Studien påvisar i likhet med Hatcher et al. (2020) studie att det förekommer policys som adresserar cybersäkerhet, men inte specifikt utformade cybersäkerhetspolicys.

Förekomsten att cybersäkerhetsutbildningar varierar och chefer samt IT-personal genomgår utbildning i högre utsträckning än anställda i verksamheten. I likhet med Hatcher et al. (2020) påvisade studien att omkring 40% av respondenterna inte genomgick utbildning om cybersäkerhet.

Det förekommer att kommuner har utformade kontinuitetsplaner som ska användas vid en cyberattack, studien visar dock att förekomsten varierar mellan förvaltningar inom samma kommun. Trots att det finns en önskan och ett behov av stöd och hjälp i arbetet med cybersäkerhet finns det en övergripande uppfattning om att kommunerna har en god kapacitet att hantera en eventuell cyberattack.

Att kommuner ligger efter i digitaliseringen jämfört med omvärlden menar anställda inom kommunal verksamhet kan bero på den tröga förvaltningens natur, resursbrist och en osäkerhet inför det okända. Samtidigt fungerar den tröga förvaltningens natur som en säkerhetsåtgärd som säkerställer medborgarnas trygghet framför digitalisering.

6.3 Sammanfattning

Sammanfattningsvis kan vi baserat på studiens resultat säga att anställda inom den kommunala verksamheten är medvetna och uppmärksamma för det cyberhot som finns mot kommuner och att hotet har ökat i takt med den accelererande digitaliseringen. Vidare kan det konstateras att det finns både möjligheter och risker med digitala verktyg då de både kan försvara

verksamheten i form av AI-teknik men även göra verksamheten mer utsatta för cyberattacker. Slutligen påvisar studien att det förekommer arbetsmetoder kopplat till cybersäkerhet med en viss variation mellan förvaltningar, det finns utrymme för förbättring och en önskan om hjälp och stöd.

6.4 Syfte

Studiens syfte är uppfyllt då studien har resulterat i en förståelse för existerande uppfattningar, strategier och hantering av cyberhot som den kommunala förvaltningen utsätts för i samband med den accelererande digitaliseringen och utvecklingen av artificiell intelligens.

6.5 Studiens bidrag

Vår studie bidrar till forskningsfältet inom cybersäkerhet på kommunal nivå som flertalet forskare rapporterat kräver mer forskning (Writz & Weyerer, 2017; Norris et al., 2021; Preis & Susskind, 2022; Choodakowska et al., 2022; Hatcher et al., 2020; Caruson et al., 2012). Studien bidrar med resultat som visar hur de konstanta hotet mot cybersäkerheten mot kommuner uppfattas av dess anställda samt vilka arbetsmetoder som förekommer i arbetet att säkerställa cybersäkerhet inom den kommunala verksamheten. Studiens resultat kan användas i utvecklingen av arbetet med cybersäkerhet inom den kommunala verksamheten då resultaten belyser utvecklingsområden, existerande metoder, attityder till digitala verktyg och anställdas uppfattningar om cybersäkerhet.

Studien studerade kommuner i en svensk kontext vilket tidigare forskning inte gjort i stor utsträckning, länder som tidigare studerats har bland annat varit USA och Tyskland (Norris et al., 2019; Wirtz & Weyerer, 2017). En kommande svensk studie ska studera cybersäkerhet i svenska kommuner och den ansvarige forskaren menar att kunskaper om hur cybersäkerhet uppfattas och hanteras av kommuner är värdefullt då det inte finns utbredd forskning inom området (Högskolan Väst, 2022). Vår studie har visat hur hotet mot cybersäkerheten uppfattas och hanteras av verksamhets-, enhets- och digitaliseringschefer inom kommunal verksamhet.

6.6 Vidare forskning

Utifrån vår studie och presenterad tidigare forskning upplever vi att det finns ett behov att fortsätta studera området cybersäkerhet på kommunal nivå. Kommande studier bör fortsätta

utforska hur kommuner arbetar med cybersäkerhet och specifika rutiner, förslagsvis kan det studeras hur anställda på golvet arbetar med cybersäkerhet i det dagliga arbetet eller hur anställda inom IT övergripande arbetar med cybersäkerhet. Att studera olika kategoriseringar av kommuner och se hur arbetet med cybersäkerhet kan skilja sig mellan kommuner är också ett förslag på vidare forskning.

Ytterligare förslag på vidare forskning är att undersöka möjligheten att implementera nationella mål och lösningar för AI och cybersäkerhet för Sveriges 290 kommuner, vår studie påvisade en önskan om detta, därmed är detta intressant för framtida studier. Intressant vore även att se specifikt hur AI kan stärka cybersäkerheten och motverka cyberattacker inom kommuner.

7. Referenslista

Advencia. (2023). *Kommunerna är inte förberedda på cyberattacker*. https://advenica.com/sv/blog/2023-04-05/kommunerna-ar-inte-forberedda-pa-cyberattacker. Publicerad 2023-04-05. Hämtad 2023-11-07.

Ahrne, G., & Svensson, P. (2015). Kvalitativa metoder i samhällsvetenskapen. I G. Ahrne & P. Svensson (Red.), *Handbok i kvalitativa metode*r (s. 8-16). Stockholm : Liber

Andréasson, E. (2015). *Digitalisering i den offentliga förvaltningen. IT, värden och legitimitet.* Linköping : Linköpings universitet.

Barcik, P., Coufalikova, A., Frantis, P., & Vavra J. (2023). The Future Possibilities and Security Challenges of City Digitalization. *Smart Cities*, 6(1):137-155. https://doi.org/10.3390/smartcities6010008.

Butun, I., Österberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys and Tutorials,* 22(1), 616-644. https://doi-org.ezproxy.ub.gu.se/10.1109/COMST.2019.2953364

Börjesson, A., & Karlsson, L. (2020). Etik. I C. Abrahamsson Löfström och B. Rombach (Red.), *Andra hjälpen: allt du behöver veta för att skriva en uppsats* (S. 55-66). Lund : Studentlitteratur.

Cadeo. (u.å). *Vad betyder digitalisering?* https://www.cedeo.se/kunskapsbanken/digitalisering/vad-betyder-digitalisering Hämtad: 2023-12-21

Campion, A., Hernandez, M., Mikhaylov Jankin, S., & Esteve, M. (2020). Managing Artificial Intelligence Deployment in the Public Sector. *Computer (Long Beach, Calif.), 53*(10), 28-37. https://ieeexplore-ieee-org.ezproxy.ub.gu.se/document/9206418

Carlsson, J., & Carlsson, V. (2020). Intervjuer. I C. Abrahamsson Löfström och B. Rombach (Red.), *Andra hjälpen: allt du behöver veta för att skriva en uppsats* (S. 93-106). Lund : Studentlitteratur.

Caruson, K., MacManus, S., & McPhee, B. (2012). Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to success. *Journal of Homeland Security and Emergency Management, 9*(2), 1-22. https://www-degruyter-com.ezproxy.ub.gu.se/document/doi/10.1515/jhsem-2012-0003/html

Choodakowska, A., Kandula, S., & Przybylska, J. (2022). Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. *Lex Localis-journal of Local Self-government,20*(1), 161-192. https://www.proquest.com/docview/2624993471?parentSessionId=FL5tvD6YqW0nqXJgmY%2BjbY%2BrV12%2BQ3DSH%2FWZp2JGzQk%3D&pq-origsite=primo&accountid=11162

Demertzi, V., Demertzis, S., & Demertzis K. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. *Applied Sciences,* 13(2):790. https://doi.org/10.3390/app13020790.

Dir. 2012:61. *Digitaliseringskommissionen – en kommission för den digitala agendan.* https://www.regeringen.se/contentassets/538820854ece4bf2842e139f84b4b723/digitaliseringskommissionen---en-kommission-for-den-digitala-agendan-dir.-201261

Ford, N. (2023). List of data breaches and cyber attacks in 2023. ITgovernance UK. https://www-itgovernance-co-uk.translate.goog/blog/list-of-data-breaches-and-cyber-attacks-in-2023?_x_tr_sl=en&_x_tr_tl=sv&_x_tr_hl=sv&_x_tr_pto=rq. Hämtad 2023-11-07. Senast uppdaterad 2023-11-03.

Frandell, A., & Feeney, M. (2022). Cybersecurity Threats in Local Government: A Sociotechnical Perspective. *American Review of Public Administration, 52*(8), 558-572. https://journals-sagepub-com.ezproxy.ub.gu.se/doi/full/10.1177/02750740221125432

Guembe, B., Azeta, A., Misra, S., Osamor, V., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence,*

36(1), Applied artificial intelligence, 2022, Vol.36 (1), Article 2037254. https://www.tandfonline.com/doi/full/10.1080/08839514.2022.2037254

Hatcher, W., Meares, W., & Heslen, J. (2020). The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. *Journal of Cyber Policy, 5(2).* Article 1792956. https://www.tandfonline.com/doi/abs/10.1080/23738871.2020.1792956.

Högskolan Väst. (2022). *Forskare ska studera cybersäkerheten i kommuner.* https://www.mynewsdesk.com/se/hogskolanvast/news/forskare-ska-studera-cybersaekerheten-i-kommuner-440300. Publicerad 2022-01-04. Hämtad: 2023-12-20.

Henman, P. (2020). Improving public services using artificial intelligence: Possibilities, pitfalls, governance. *Asia Pacific Journal of Public Administration = Ya Tai Gong Gong Xing Zheng Xue, 42*(4), 209-221. https://www-tandfonline-com.ezproxy.ub.gu.se/doi/full/10.1080/23276665.2020.1816188

IoT Sverige. (u.å.). IoT - så funkar det. *Internet of Things Sverige.* https://iotsverige.se/om-oss/iot-sa-funkar-det. Hämtad 2023-11-20.

Karlsson, D. (2020). Enkäter. I C. Abrahamsson Löfström och B. Rombach (Red.), *Andra hjälpen: allt du behöver veta för att skriva en uppsats* (195-211). Lund : Studentlitteratur.

Khando, K., Gao, S., Islam, S., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, 102267 https://www.sciencedirect.com/science/article/pii/S0167404821000912

Khisamova, Z. I., Begishev, I. R., & Sidorenko, E. L. (2019). Artificial intelligence and problems of ensuring cyber security. *International Journal of Cyber Criminology*, 13(2), 564-577. doi:https://doi.org/10.5281/zenodo.3709267

Larsson, P. J. (2023). *Så ska AI förändra bankbranschen - trots riskerna:"Kan orsaka finanskris".* Aftonbladet Plus. https://www.aftonbladet.se/minekonomi/a/q1lwnm/sa-paverkar-ai-bankerna-kan-orsaka-finanskris. Publicerad 2023-11-13. Hämtad 2023-11-13.

Melin, U. (2018). *Vetenskaplig kunskap och bildning för samhällets framtida digitalisering – ett nationellt centrum*. Utredningsrapport 2018-11-05. Linköping : Linköpings universitet.

Mergel, I., Dickinson, H., Stenvall, J., & Gasco, M. (2023). Implementing AI in the public sector. *Public Management Review, Ahead-of-print*(Ahead-of-print), 1-13 https://www-tandfonline-com.ezproxy.ub.gu.se/doi/full/10.1080/14719037.2023.2231950

Microsoft. (u.å). *Vad är cybersäkerhet?*. https://support.microsoft.com/sv-se/topic/vad-%C3%A4r-cybers%C3%A4kerhet-8b6efd59-41ff-4743-87c8-0850a352a390 Hämtad 2023-12-05.

Myndigheten för digital förvaltning, Arbetsförmedlingen, Bolagsverket & Skatteverket. (2023). *Uppdrag att främja offentlig förvaltnings förmåga att använda artificiell intelligens*. https://www.digg.se/download/18.5b30ce7218475cd9ed39384/1674479294670/Slutrapport%20Uppdrag%20att%20fr%C3%A4mja%20offentlig%20f%C3%B6rvaltnings%20f%C3%B6rm%C3%A5ga%20att%20anv%C3%A4nda%20AI%20I2021-01825.pdf.

Myndigheten för digital förvaltning. (2023). *Digitala Sverige 2022*. https://www.digg.se/download/18.1e68c05518649f2b2eb6a8e/1677659508496/Digitala%20Sverige%202022.pdf

Myndigheten för digital förvaltning. (u.å). *Vårt uppdrag*. https://www.digg.se/om-oss/vart-uppdrag. Senast uppdaterad 2023-08-14. Hämtad 2023-11-11.

Myndigheten för samhällsskydd och beredskap. (u.å). *Cyberhot*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/. Hämtad 2023-11-13.

Norris, D.F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. *Public Administration Review, 79*(6), 895-904. https://onlinelibrary-wiley-com.ezproxy.ub.gu.se/doi/10.1111/puar.13028

Norris, D.F., Mateczun, L., Joshi, A., & Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity.

Journal of Urban Affairs, 43(8), 1173-1195. https://doi-org.ezproxy.ub.gu.se/10.1080/07352166.2020.1727295.

Preis, B., & Susskind, L. (2022). Municipal Cybersecurity: More Work Needs to be Done. *Urban Affairs Review (Thousand Oaks, Calif.),58*(2), 614-629. https://journals-sagepub-com.ezproxy.ub.gu.se/doi/full/10.1177/1078087420973760

Regeringskansliet. (2017). *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi.* https://www.regeringen.se/contentassets/c9bc0cd3a4374f9388e714ae7fb1ec1d/for-ett-hallbart-digitaliserat-sverige-en-digitaliseringsstrategi.pdf

Riksrevisionen. (2023). *Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet,* Skr 2023/24:26. Regeringskansliet. https://regeringen.se/rattsliga-dokument/skrivelse/2023/10/skr.-20232426. Publicerad 2023-10-12. Hämtad 2023-11-13.

Safitra, M.F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, 15(18):13369. https://doi.org/10.3390/su151813369.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law, 12*(2), 53-74. https://www.proquest.com/scholarly-journals/towards-more-representative-definition-cyber/docview/2035634435/se-2.

Solli, R. (2020). Kvalitativa sekundärmaterial. I C. Abrahamsson Löfström och B. Rombach (Red.), *Andra hjälpen: allt du behöver veta för att skriva en uppsats* (s. 123-134). Lund : Studentlitteratur.

SOU 2016:89. *För digitalisering i tiden: slutbetänkande.* https://www.regeringen.se/contentassets/f7d07b214e2c459eb5757cea206e6701/sou-2016_89_webb.pdf

Stahle, N. (2022, 25 januari). *It-attacken mot Kalix kommun - detta har hänt. SVT nyheter.* https://www.svt.se/nyheter/lokalt/norrbotten/it-attacken-mot-kalix-kommun-detta-har-hant

Susskind, R., & Susskind, D. (2017). *Professionernas framtid: hur teknologin kommer att förändra experters arbete*. Göteborg : Daidalos.

Svensson, P., & Ahrne, G. (2015). Att designa ett kvalitativt forskningsprojekt. I G. Ahrne & P. Svensson (Red.), *Handbok i kvalitativa metode*r (s. 17-31). Stockholm : Liber

Svärd, O. (2020). Observationer. I C. Abrahamsson Löfström och B. Rombach (Red.), *Andra hjälpen: allt du behöver veta för att skriva en uppsats* (s. 107-121). Lund : Studentlitteratur.

Tegmark, M. (2023). Pause Giant AI Experiments: An Open Letter. *Future of life institute*. https://futureoflife.org/open-letter/pause-giant-ai-experiments/?fbclid=IwAR2Wx2S8IYpiOMk0BB09pbGuOULIKJxMUiidM7jskdxux02nzuy9aqhx_1k. Publicerad 2023-03-22. Hämtad 2023-11-16.

Theodorsson, A. (2020). Presentera kvalitativa studier. I C. Abrahamsson Löfström och B. Rombach (Red.), *Andra hjälpen: allt du behöver veta för att skriva en uppsats* (s. 149-162). Lund : Studentlitteratur.

Transportstyrelsen. (u.å.). Nollvisionen. *Transportstyrelsen.se.* https://www.transportstyrelsen.se/sv/vagtrafik/statistik/olycksstatistik/statistik-over-vagtrafikolyckor/nollvisionen. Senast uppdaterad 2022-12-23. Hämtad 2023-11-20.

Trost, J., & Hultåker, O. (2016). *Enkätboken*. Lund : Studentlitteratur.
Vetenskapsrådet. (2002). *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning.* https://www.vr.se/download/18.68c009f71769c7698a41df/1610103120390/Forskningsetiska_principer_VR_2002.pdf.

Wirtz, B.W., & Weyerer, J.C. (2017). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. *International Journal of Public Administration, 40*(13), 1085-1100. https://www-tandfonline-com.ezproxy.ub.gu.se/doi/full/10.1080/01900692.2016.1242614

Wirtz, B.W., Weyerer, J.C., & Geyer, C. (2019). Artificial Intelligence and the Public Sector—Applications and Challenges. *International Journal of Public Administration*, 42(7), 596-615. https://doi.org/10.1080/01900692.2018.1498103.

Wirtz, B.W., Weyerer, J.C., & Sturm, B.J. (2020). The Dark Sides of Artificial Intelligence: An Integrated AI Governance Framework for Public Administration. *International Journal of Public Administration*, 43(9), 818-829. https://doi-org.ezproxy.ub.gu.se/10.1080/01900692.2020.1749851.

Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for digital manufacturing. *Journal of Manufacturing Systems,* 48(C), 3-12. https://doi-org.ezproxy.ub.gu.se/10.1016/j.jmsy.2018.03.006.

8. Bilaga 1 - Intervjuguide

Inledande frågor

- Hur länge har du arbetat på kommun X?
- Vad är din titel?
- Vad ingår i ditt arbete?
- Hur ser en vanlig arbetsdag ut för dig?

Medvetenhet

- Hur får du som anställd information om cybersäkerhet?
- Får du som anställd information om cybersäkerhet i era digitala forum från kommunen?
- Finns det en medvetenhet för cyberattacker inom kommunen? (Får förklara vad vi menar med medvetenhet)
- Skulle du säga att det finns en hög, medel eller låg nivå av medvetenhet för cyberattacker inom förvaltningen?
- Bidrar kommunen med kurser eller andra former av utbildning kring cybersäkerhet i arbetet?
- Du som chef/ansvarig, informerar du din personal om cybersäkerhet?
- Hur ser diskussionen kring cybersäkerhet ut i kommunen?
- Hur upplever du risken för cyberhot mot kommunen?

Arbetsmetoder

- Finns det några övergripande strategier eller policys för cybersäkerhet?
- Finns det några arbetsrutiner anställda uppmuntras följa kopplat till cybersäkerhet?
- Vet du hur dessa arbetsrutiner följs upp?

Artificiell intelligens

- Har du hört talas om att cyberattacker numera kan utföras av artificiell intelligens?

Om JA = I vilket forum (arbetsplats, internet m.m) blev du informerad om detta?

Om NEJ = Vad är din spontana tanke kring detta? Tycker du att kommunen borde ha informerat sina anställda om detta?

- Hur ser du på AI sett till cybersäkerhet? Risk eller möjlighet? (Hot eller ett sätt att skydda eller utveckla verksamheten)
- Vad tycker du om att det dyker upp AI tjänster och arbetsmetoder inom den offentliga sektorn?

Digitalisering

- Hur ser du på förvaltningen och den accelererande digitaliseringen? Finns det kompetens till att hantera denna snabba utveckling?
- Har ni sett en ökad hotbild mot cybersäkerheten i takt med digitaliseringen?

Kapacitet

- Tror du att kommunen har en god kapacitet att hantera en cyberattack?
- Tror du att de flesta offentliga verksamheter har en god kapacitet att hantera en cyberattack?
- Har ni någon ansvarig för data som samlas in i kommunen?

Avslutande frågor

- Hur ser du på framtiden och cybersäkerheten inom förvaltningen?
- Har du något du vill tillägga?
- Har du eventuellt någon intressant person vi kan gå vidare med?