

DEN MÄNSKLIGA FAKTORN I

AI-DRIVEN CYBERSÄKERHET

Utmaningar med automatisering och
teknologiberoende

**THE HUMAN FACTOR IN AI-BASED
CYBERSECURITY**

Challenges with automation and
technological dependence

Examensarbete inom huvudområdet
Informationsteknologi
Grundnivå 30 Höskolepoäng
Vårtermin År 2025

Anton Carl Gustavsson

Handledare: Eva Söderström
Examinator: Hanife Rexhepi

Sammanfattning

Syftet med detta arbete är att kunna få en inblick i hur den mänskliga faktorn påverkas av automatisering och teknologiberoende med användning av AI-baserad cybersäkerhet. AI-baserade system och lösningar blir mer en central del av tekniska lösningar men det gör även att det blir ett ökat behov av att faktiskt förstå hur den mänskliga faktorn kan kopplas med denna teknologi. Detta arbete är baserat på en systematisk litteraturstudie med 25 inkluderande artiklar i sin analys som analyserats med hjälp av tematisk analys. Detta arbete har fått fram ett resultat kring att den mänskliga faktorn inte försvinner med användning av AI-baserade system inom cybersäkerheten utan att den istället förändras och kan skapa nya sårbarheter. Bristande förståelse och kunskap, teknologiberoende och för hög tillit, automatiseringens påverkan på mänsklig roll och etiska dilemman är de fyra identifierade teman som funnits i denna analys. Dessa fyra olika faktorer visar på en ökad risk för mänskliga misstag, passivitet och etisk osäkerhet trots den potential som AI-baserade system har för cybersäkerheten. Detta arbete visar att AI-baserad cybersäkerhet inte enbart är en teknisk fråga utan att det kommer behövas utbildning och etiska åtgärder för att säkerhetsställa en mer säker cybersäkerhet och att människan kommer fortsatt vara en central roll. Det mänskliga perspektivet är avgörande och kommer fortsatt vara avgörande för att AI ska kunna uppnå sin potential i framtidens digitala samhälle.

Nyckelord: Artificiell Intelligence, Cybersäkerhet, Mänskliga faktorn, AI-baserad cybersäkerhet.

INNEHÅLLSFÖRTECKNING

1 Inledning	1
2 Bakgrundskapitel	2
2.1 Vad är Cybersäkerhet	2
2.2 Vad är Artificiell intelligens	2
2.3 AI-baserad Cybersäkerhet	3
2.4 Automatiseringens påverkan på cybersäkerhet	4
2.5 Teknologiberoende och dess konsekvenser	5
2.6 Etiska och juridiska aspekter av AI i cybersäkerhet	5
2.7 Den mänskliga faktorn i Cybersäkerhet	6
3 Problemområde	8
3.1 Problem/fråga	9
3.2 Avgränsningar	9
3.3 Förväntat resultat	9
4 Metod	11
4.1 Systematisk litteraturstudie	11
4.1.1 Sökstrategier & urvalskriterier	11
4.1.2 Val av artiklar	13
4.1.3 Analys av artiklar	14
4.2 Forskningsetiska principer	15
5 Materialpresentation	17
5.1 Tematisk gruppering av artiklar	17
5.2 Översikt av inkluderande artiklar	17
5.2.1 Översikt av Grupp A	17
5.2.2 Översikt av Grupp B	19
5.2.3 Översikt av Grupp C	19
5.2.4 Översikt av Grupp D	20
5.2.5 Översikt av Grupp E	22
6 Analys	24
6.1 Bristande förståelse och kunskap	24
6.2 Teknologiberoende och för hög tillit till AI-baserade system	25
6.3 Automatiseringens påverkan på mänsklig roll	27
6.4 Etiska dilemman och otydlig ansvarsfördelning med användning av AI-baserade system	28
7 Resultat	30
7.1 Bristande förståelse och kunskap ökar fortsatt risken	30
7.2 Teknologiberoende för AI-baserade system ger nya sårbarheter	31
7.3 Automatisering leder till ett skiftat fokus mot övervakande och strategisk översikt men den mänskliga faktorn kvarstår	31
7.4 Bristande transparens skapar otydlig ansvarsfördelning och etiska dilemman	32
7.5 Sammanfattning av resultat	33
8 Diskussion	35
8.1 Metod	35

8.1.1 Vetenskaplig etik	36
8.2 Resultat	36
8.3 Samhälleliga aspekter	37
8.4 Etiska aspekter	37
8.5 Metodologiska begränsningar	38
8.6 Framtida arbeten	38
Referenser	39

1 Inledning

Den digitala utvecklingen sker i en väldigt hög hastighet och ännu mer nu när baserade system av artificiell intelligens (AI) blir en alltmer central roll i det digitaliserade samhället (Salem et al., 2024). Detta innefattar även AI-baserade systemimplementationer inom cybersäkerheten där dessa system förändrar möjligheterna men även riskerna inom området (Salem et al., 2024).

Ett AI-baserat system inom cybersäkerhet används för att kunna automatisera säkerhetsåtgärder i realtid, upptäcka hot och analysera stora mängder data (Salem et al., 2024). Enligt Salem et al. (2024) finns därför stor potential för AI-baserade system inom cybersäkerhet då dessa automatiserade system kan leda till en högre effektivitet. Samtidigt finns fortfarande den mänskliga faktorn i denna aspekt där människan fortfarande har en avgörande roll som både en sårbarhet men även som användbar instans för kontroll (Pawlicka et al., 2022).

Enligt Bouramdane (2023) är ett ökat teknologiberoende kring automatisering baserat på AI-baserade system som kan leda till nya utmaningar. Exempel kring nya utmaningar är en högre komplexitet och ett för högt förtroende för system som kan leda till brist på insyn kring beslutsfattande (Bouramdane, 2023).

Detta arbete kommer därför att undersöka hur den mänskliga faktorn påverkar AI-baserad cybersäkerhet till samt vilka potentiella risker som kan uppstå vid automatisering och teknologiberoende för att kunna få fram hur dessa faktorer ska hanteras och ha möjlighet att skapa en bättre och säker cybersäkerhet miljö.

2 Bakgrundskapitel

Detta kapitel kommer gå igenom den vetenskapliga bakgrund som finns kring arbetets ämne cybersäkerhet, artificiell intelligens, AI-baserad cybersäkerhet och mänskliga faktorn för att läsaren ska få en bättre förståelse.

2.1 Vad är Cybersäkerhet

Cybersäkerhet är idag en väldigt viktig faktor då samhället blir allt mer digitaliserat. Cybersäkerhet är att skydda digitala tillgångar såsom nätverk, datorer och data från obehörig åtkomst (Sarker et al., 2021). Cybersäkerhetens omfattning är ett stort spektrum med flera olika områden såsom, informationssäkerhet, applikationssäkerhet, driftssäkerhet, molnsäkerhet och nätverkssäkerhet där syftet med cybersäkerhet är att kunna nå konfidentialitet, integritet och tillgänglighet (Bouramdane, 2023; Mishra et al., 2022). Det innefattar att cybersäkerheten ska kunna skydda information från obehörig åtkomst, säkerställa att data är korrekt och att alla system och data ska finnas tillgänglig när den behövs (Sarker et al., 2021). Cybersäkerhet är att förstå och kunna förebygga olika typer av attacker och cyberhot, detta kan innefatta till exempel skadlig programvara, dataintrång, överbelastningsattacker, phishing men även hot från insidan (Sarker et al., 2021). Cybersäkerhet anses ha en hög prioritet i dagens samhällsnivå och den betraktas även idag som en integrerad del av samhällets övergripande säkerhet (Pawlicka et al., 2022). Det är därför samhällsviktigt att beakta i dagens samhälle cybersäkerhetens svagaste länkar för att kunna uppnå en säker cybersäkerhet. Enligt Mishra et al. (2022) är inte cybersäkerhet enbart om att skydda data utan även kring att skydda personer som använder tekniska tillgångar och befinner sig i en cybermiljö. Enligt Pawlicka et al. (2022) är den mänskliga faktorn och beteendet i cybersäkerhetsstrategier det som bör prioriteras då den mänskliga faktorn är just nu den svagaste länken. Bouramdane (2023) menar att det finns en stor betydelse av medvetenhet och utbildning inom cybersäkerhet för att kunna uppnå en säker IT-miljö för att kunna minimera risken för den mänskliga faktorn.

2.2 Vad är Artificiell intelligens

Artificiell intelligens (AI) är kortfattat ett brett område vars syfte är att skapa tekniska maskiner som ska kunna utföra uppgifter som normalt tidigare krävde mänsklig intelligens (Minh et al., 2022; Glikson & Woolley, 2020). AI består av en underkategori som är maskininlärning där maskininlärning använder data från matematiska modeller för att kunna förbättra maskinens intelligens (Minh et al., 2022; Glikson & Woolley, 2020). En maskininlärningsmodell tränas och konstrueras genom att använda sig av en specifik datauppsättning för att sedan på ett automatiskt sätt kunna få fram förutsägelser för att sedan kunna göra beslut för kommande ny data genom att maskinen har lärt sig mönster av beslut i den tidigare datauppsättningen (Minh et al., 2022; Du-Harpur et al., 2020). Maskininlärning har sedan även underkategori som är djupinlärning som just nu är en av det mest populära underkategorierna av maskininlärning då djupinlärning efterliknar mer hur den mänskliga hjärnan bearbetar

mönster och data för att kunna fatta olika beslut (Minh et al., 2022). Utvecklingen av AI har gjort med hjälp av maskininlärning, kunskapsbearbetning, och mönsterigenkänning där målet är att ge datorer en mer logisk resonansförmåga (Zhang & Lu, 2021). Enligt Glikson och Woolley (2020) är definieringen kring AI teknologier som har förmågan att kunna interagera med omgivningen genom att samla och tolka information för att generera och utvärdera resultat. Utvecklingen för AI-baserade system är snabb och potentialen ökar kring användningsområden med AI-baserade system. Enligt Zhang och Lu (2021) är det enbart en tidsfråga innan maskiners intelligens kan ha möjligheten att överträffa den mänskliga intelligensen. Minh et al. (2022) menar att det inte går att förneka den potential AI har som hjälpmedel men att det fortfarande finns en problematik kring beslutsfattande.

Minh et al. (2022) menar att AI är ett effektivt och snabbt system som kan skapa intelligens av stora mängder data och kan enkelt läsa av stora mängder data för att sedan kunna fatta beslut med nykommen data med hjälp av tidigare gjorda beslut som finns med i den matematiska modellen. Det finns däremot stora brister i transparensen i besluten som varje AI gör och det kan vara svårt att förklara hur dessa modeller kommer fram till sina beslut eftersom AI inte kan förklara hur ett specifikt beslut fattades (Minh et al., 2022). Enligt Minh et al. (2022) så har däremot AI sett en anmärkningsvärd utveckling på det senare åren och mycket är tack vare den exponentiella tillväxten i enorma mängder data och datorkraft där AI betraktas som den mest utbredda teknologin som skapats under de senaste decennierna. Det finns därför även chans att denna utveckling av AI kan i framtiden lösa den problematik som AI idag har med beslutsfattande och transparens och detta har lett till ett ökande behov av förklarbarhet (Minh et al., 2022).

2.3 AI-baserad Cybersäkerhet

AI-baserad cybersäkerhet kan användas i flera olika former enligt Salem et al. (2024). Den AI-baserade cybersäkerheten innefattas av Artificiell intelligens, maskininlärning och djupinlärning där syftet är att skapa ett bättre system för detektion och prevention av olika typer av cyberattacker (Salem et al., 2024). AI-baserad cybersäkerhet fungerar i grunden exakt som andra typer av AI system i andra områden menar Salem et al. (2024). Enligt Salem et al. (2024) menas det att AI-baserade system använder och simulerar kognitiva processer genom matematiska algoritmer och med hjälp av detta så kan systemet ha möjlighet att resonera och fatta beslut som är baserat på den data som systemet arbetar med. Enligt Salem et al. (2024) så är det AI-tekniker som används inom cybersäkerhet är Maskininlärning som används för nätverkstrafik där tekniken klassificeras och detekteras för att identifiera skadliga aktiviteter.

Djupinlärning som används för att kunna hitta icke-linjära och komplexa korrelationer inom data. Detta skapar möjligheten att snabbt identifiera nya tidigare okända hot och nya filtyper.

Enligt Sarker et al. (2021) så är syftet med AI-baserad cybersäkerhet att kunna automatisera, effektivisera och förbättra cybersäkerhetsprocessen jämfört med den Cybersäkerhetsprocess som används idag. AI-systemen kan även analysera stora mängder data på ett mycket mer effektivt sätt än vad det tidigare systemen kan göra och med en extrem noggrannhet menar Salem et al. (2024).

Enligt Pawlicka et al. (2022) kan AI-baserad cybersäkerhet användas för att förebygga cyberbrott genom att identifiera och analysera sårbarheter och hot men även kunna förutsäga och mildra framtida attacker genom att kunna använda sin tidigare data. Salem et al. (2024) påpekar även att dessa AI-baserade system har möjlighet att kunna identifiera komplexa mönster och korrelationer i stora datamängder för att kunna upptäcka men även förebygga nya typer av attacker och tidigare okända hot.

2.4 Automatiseringens påverkan på cybersäkerhet

Automatiseringen har en stor inverkan på cybersäkerheten men där denna inverkan både har positiv och negativ påverkan. Enligt Timmers (2019) så måste det finnas ett mellanting i automatiseringen för att kunna uppnå en säkrare miljö. Timmers (2019) menar att automatisering kan förbättra cybersäkerheten genom en snabbare detektion och en minskad arbetsbelastning men där det är viktigt att vara medveten om riskerna som finns med AI-baserade automatiseringssystem och behålla en mänsklig kontroll för att kunna uppnå en säkrare miljö. Enligt Salem et al. (2024) så kan AI-baserade cybersäkerhet ge en positiv påverkan på flera olika faktorer. Det finns möjlighet att kunna få en snabbare detektion och respons då dessa system kan analysera stora mängder av data i realtid, Detta möjliggör att hot kan snabbare upptäckas och systemen kan göra automatiserade handlingar mot dessa hot.

Salem et al. (2024) menar även att det skapar möjligheten för effektivare sårbarhetshantering då AI-baserade system kan förutse potentiella sårbarheter innan dessa sårbarheter har utnyttjats som skapar möjligheten att ha ett bättre proaktivt säkerhetsarbete istället för ett reaktivt säkerhetsarbete. Automatisering kan även leda till att det blir en minskad arbetsbelastning då AI-baserade system kan ta över arbete från säkerhetsexperter, arbeten som skulle kunna vara repetitiva eller tidskrävande uppgifter som det tidigare har behövt utföra. Däremot så menar Guembe et al. (2022) att med möjligheten att kunna använda AI-baserade system så finns det även negativ påverkan för cybersäkerheten och ett exempel är AI-drivna attacker. Guembe et al. (2022) menar att cyberkriminella kommer också att börja använda AI-baserade system för att utföra sina attacker där det även finns risker att det kommer att utföras en ökad attackhastighet med högre komplexitet. Enligt Timmers (2019) kan det även vara en negativ påverkan kring etiska problem där det AI-baserade systemen som används för automatisering använder en typ av massövervakning där det blir en avvägning mellan informationssäkerhet och individuell integritet som kan skapa etiska dilemman.

2.5 Teknologiberoende och dess konsekvenser

Samhället blir allt mer digitaliserat och det leder till ett ökande beroende av IT, som medför flera konsekvenser. Samhällets informationsförsörjning har blivit beroende av IT och kommunikation över internet där samhällsfunktioner behöver använda sig av IT för att utbyta information (Oscarson, 2019). Oscarson (2019) menar att det finns en rad av konsekvenser som kan uppstå av teknologiberoende såsom sårbarhet för oavsiktliga hot som innebär att samhället och dess organisationer blir sårbara av störningar och haverier som kan vara orsakade av tekniska och mänskliga fel.

Risken för störningar i samhällsviktiga verksamheter, som pekar på att digitaliseringen även innefattar funktioner som är kritiska och som annars skulle kunna resultera i stora negativa konsekvenser. Energiförsörjning, hälso- och sjukvård och betalningssystem är idag exempel på teknologiberoende där digitaliseringen måste fungera (Oscarson, 2019). Salem et al. (2024) menar att samhället redan har haft ett stort teknologiberoende men att med AI-baserade system så ökar samhällets teknologiberoende ännu mer. Utvecklingen har gått till att AI-baserade system är ett verktyg för att kunna skapa en bättre cybersäkerhet, men även att utvecklingen för cyberattacker med AI-baserade system har blivit ett verktyg, så gör denna utveckling det svårt för organisationer att skydda sig utan AI-baserade system. Detta medför enligt Salem et al. (2024) att ett samhälle med denna utveckling, kommer att bli ännu mer teknologiberoende än vad vi tidigare har varit.

2.6 Etiska och juridiska aspekter av AI i cybersäkerhet

Det finns flera utmaningar både kring det etiska och det juridiska aspekterna av AI i cybersäkerhet där stora områden av cybersäkerheten har etiska utmaningar menar Timmers (2019). AI-baserade system i cybersäkerhet ger utmaningar gällande riskhanteringen, där dessa AI-baserade system används för övervakning och riskprevention som kan vara integritetskränkande och tvingande för alla individer (Timmers, 2019). Det finns även etiska dilemman som är kopplat till strategisk autonomi där det kan finnas svårigheter kring att avgöra vem som bär ansvaret när AI-baserade systemet gör felaktiga beslut (Timmers, 2019). Timmers (2019) menar även att det behövs göra en avvägning som ska vara mellan individuella och kollektiva intressen där det ska skapas en balans mellan att skydda individer eller samhället som helhet och att problematiken är att denna balans är svår att uppnå.

Det juridiska aspektet har stora utmaningar då ett av dessa exempel är ansvarsfördelning där det finns svårigheter genom att fastställa ansvar kring skador som är orsakade av det AI-baserade systemet (Bleher & Braun, 2022). Bleher och Braun (2022) Menar att utvecklingen av AI-baserade system har gått fort och att den juridiska aspekten inte hunnit med i samma takt och poängterar behovet av ett regelverk och organisatoriska strukturer för att kunna säkerställa ett skadeståndsanspråk och att detta ska kunna drivas rättsligt. Det finns även diskussioner som just nu är kring ansvarsfördelningen av AI-baserade system där diskussionen är kring ifall systemet ska

vara lagligt så måste det finnas kontrollmöjligheter i systemets design detta för att kunna möjliggöra tydliga ansvarsfördelningar (Bleher & Braun, 2022).

Det är därför svårt att diskutera de etiska och juridiska aspekterna fullt ut då denna faktor just nu är under beaktande men där det är tvunget att flera beslut måste tas på samhällsnivå kring det etiska och juridiska aspekterna kring användning av AI-baserade system (Bleher & Braun, 2022).

2.7 Den mänskliga faktorn i Cybersäkerhet

Den mänskliga faktorn inom cybersäkerhet är kring hur människors beteende, beslut och handlingar påverkar säkerheten i organisationer och informationssystem (Nobles, 2018). Många av de säkerhetsincidenter som har skett inom IT har orsakats av mänskliga misstag snarare än enbart olika typer av tekniska svagheter (Nobles, 2018). Enligt Nobles (2018) så har forskningen historiskt sett haft ett större fokus kring de tekniska aspekterna men att på senare tid har det blivit tydligt att förstå att företagskultur och arbetsmiljö påverkar den mänskliga faktorn och gör det säkerhetsmedvetna beteendet avgörande. Den mänskliga faktorn är så viktig för cybersäkerheten att ifall det skulle förbises så skulle det kunna leda till stora negativa konsekvenser för organisationer som till exempel rykte skador, ekonomiska förluster och även rättsliga påföljder (Nobles, 2018).

En del av forskningen som gjorts på den mänskliga faktorn är baserad på olika psykologiska ramverk som används för att analysera och förstå de olika mänskliga faktorer som kan påverka säkerhetsbeteendet (Pollini et al., 2022). Theory of planned behavior (TPB) är ett av dessa ramverk som fokuserar på hur människors intentioner och attityd kan påverka säkerhetsbeteendet. enligt Pollini et al. (2022) så är det flesta säkerhetsbristerna orsakade av den mänskliga faktorn är handlingar som inte haft direkt skadligt uppsåt eller oavsiktliga fel. Det finns däremot faktorer som ökar benägenheten att göra mänskliga fel som innefattar individens attityd till säkerhetspolicys, kunskapen om cybersäkerhetsrelaterade ämne och individens tro på konsekvenserna av dess handlingar (Pollini et al., 2022). En ytterligare modell inom det psykologiska ramverken är Knowledge-attitude-behavior (KAB) som är en modell som påpekar just att en ökad kunskap om olika typer av säkerhetspolicys leder till förbättrade attityder som leder individen till ett säkrare beteende (Pollini et al., 2022).

Enligt Oscarson (2019) är den mänskliga faktorn en av de största faktorerna som bidrar till informationssäkerhetsbrister. Oscarson (2019) menar att den mänskliga faktorn är svår att skydda sig från då en del i denna faktor är oavsiktliga hot som är handlingar utan uppsåt som kan vara okunskap, misstag eller slarv.

Den mänskliga faktorn kan även bero på avsiktliga hot som skadegörelse eller sabotage och det detta som Oscarson (2019) menar att den mänskliga faktorn är en svår aspekt då människan kan anses vara oberäknelig och irrationell som gör att det blir

svårkontrollerat och som skapar problematik att uppnå en bättre säkerhetsnivå enbart genom tekniska skyddsåtgärder.

Enligt Oscarson (2019) finns det risker som ökar genom att det satsas på utveckling av de tekniska delarna för cybersäkerhet, då dessa system kan bidra till falsk trygghet. Oscarson (2019) menar att människan kan få en för hög tillit till det tekniska skyddet och att detta kan bidra till att den mänskliga faktorn får mindre uppmärksamhet i säkerhetstänket.

Den mänskliga faktorn är väldigt väl studerad och har alltid varit en stor problematisk aspekt i cybersäkerheten. Enligt Pawlicka et al. (2022) Så är den mänskliga faktorn en central aspekt inom cybersäkerhet men menar även att särskilt nu när AI-baserad cybersäkerhet implementeras. Enligt Pawlicka et al. (2022) så påverkas cybersäkerheten mycket av hur människor har förståelse för den mjukvara och teknologi de använder, vilket i sin tur kan leda till användarens åsikter och beteenden.

Pawlicka et al. (2022) menar att det måste finnas en kunskap inom den teknologi som används för att kunna skapa en bättre miljö inom cybersäkerheten. Pawlicka et al. (2022) påpekar att en bristande förståelse kan innebära stora risker som kan vara både bristande tillit för AI-algoritmerna, kan vara för svåra att förstå, men även leda till en överdriven tillit och lita på AI-systemet utan att kritiskt granska dem.

Det är även viktigt att förstå att trots att AI har en större roll inom cybersäkerhet och många delar av cybersäkerhet kan automatiseras så kvarstår ändå den mänskliga faktorn som en viktig aspekt. Användare kommer fortfarande att integrera med system och kan vara potentiella måltavlor för IT-attacker (Pollini et al., 2022). Det finns även därför fortsatta risker för oavsiktliga hot när användare fortsatt integrerar med system där det är viktigt för organisationer att ha en bra säkerhetskultur för att kunna minska risken för oavsiktliga fel (Jeong et al., 2019).

Den mänskliga faktorn är därför en kritisk men även en komplex aspekt inom cybersäkerhet där det är viktigt för organisationer att förstå de faktorer som påverkar människans beteende för att möjliggöra strategier för att minska risken för säkerhetsincidenter (Nobles, 2018).

3 Problemområde

AI-baserade system är under utveckling för att i framtiden vara en integrerad del av cybersäkerheten. Cybersäkerhet innefattas av ett stort område där även dessa områden är väldigt breda och komplexiteten i många delar är hög (Bouramdane, 2023). Det gäller därför att inte enbart se från det perspektiv vilken potential AI baserad cybersäkerhet kan ha, utan även att försöka ta in i beräkningen det risker, utmaningar och hot som kan tillkomma av att implementera AI baserade system som framtida verktyg i cybersäkerheten (Bouramdane, 2023).

Ett av de problemområden som har varit och är en stor problematik inom informationssäkerhet och cybersäkerhet är den mänskliga faktorn. Den mänskliga faktorn är den faktor inom cybersäkerhet som anses vara den mest bristande faktorn (Pawlicka et al., 2022). Den mänskliga faktorn har därför under senare tid haft stort fokus inom cybersäkerhet och har varit en avgörande aspekt för att kunna förebygga och kunna uppnå en säker cybersäkerhet (Abbas et al., 2019).

Den mänskliga faktorns grund är att det teoretiskt sätt alltid kommer finnas en risk att det kan uppnå misslyckanden, oavsiktliga fel, avsiktliga fel och felaktig användning när det är kopplat till en människas handlingar då en mänsklig aspekt är att människan kan göra fel (Abbas et al., 2019).

Det är däremot viktigt att veta att det går att förebygga den mänskliga faktorn och minimera riskerna som är kopplade till den mänskliga faktorn genom att öka medvetenheten och utbildning (Pawlicka et al., 2022). Men för att öka medvetenheten och utbildningen inom valt område som i denna rapport innefattar AI-baserad Cybersäkerhet så är det därför viktigt att klargöra vilka utmaningar kring den mänskliga faktorn som kan uppstå av automatisering med AI-baserad cybersäkerhet (Bouramdane, 2023). Det är även därför viktigt enligt Pawlicka et al. (2022) att undersöka ifall det finns en påverkan på den mänskliga faktorn när AI-baserade system för cybersäkerhet implementeras och ifall dessa implementationer kan ge ett ännu högre teknologiberoende.

En implementering av AI i cybersäkerhet skapar även utmaningar kring påverkan på automatisering och teknologiberoende (Bouramdane, 2023). Enligt Salem et al. (2024) är AI-baserade system en funktion i cybersäkerheten för att möjliggöra identifiering och hantera olika typer av cyberhot. Denna implementering påverkar även den mänskliga faktorn i detta säkerhetsarbete då medvetenhet och utbildning av dessa system ännu inte är allmänbildning då denna utveckling av AI-baserade system har gått väldigt snabbt (Pawlicka et al., 2022). Enligt Humphreys et al. (2024) är AI-baserade system just nu även trendigt där företag vill implementera AI-baserade system för att kunna visa att företaget utvecklas. En snabb utveckling och en snabb implementation av AI-baserade system skapar utmaningar med även frågetecken kring det etiska aspekterna av användning av AI-baserade cybersäkerhet men även problematik inom

juridiska lagar där ansvarsfördelning som exempel är en stora fråga just nu med AI-baserade system (Bleher & Braun, 2022).

3.1 Problem/fråga

Denna uppsats kommer att arbeta kring att öka kunskapen kring de utmaningar som uppstår med automatisering och teknologiberoende kring det arbete med AI-driven cybersäkerhet och hur dessa utmaningar påverkar den mänskliga faktorn.

Den frågeställningen som ska besvaras i denna uppsats är:

Hur påverkas den mänskliga faktorn av automatisering och teknologiberoende i AI-driven cybersäkerhet?

Syftet med denna uppsats är att öka kunskapen kring de utmaningar samt den påverkan som automatisering och ökat teknologiberoende medför för den mänskliga faktorn inom ramen. Syftet med arbetet är att kunna skapa ett förebyggande arbete för att sedan kunna minimera riskerna med den mänskliga faktorn i AI-baserad cybersäkerhet. För att lyckas minimera riskerna kring den mänskliga faktorn så behövs det insikter och konkreta anledningar till vad som är utmaningarna med automatisering och teknologiberoende i AI-driven cybersäkerhet och hur dessa utmaningar påverkar den mänskliga faktorn.

3.2 Avgränsningar

Avgränsningen i detta arbete kommer att ha fokus på AI:s roll inom cybersäkerhet och hur den mänskliga faktorn påverkas av dessa automatiserade system. Det kommer därför vara ett fokus kring hur den mänskliga faktorn påverkas av AI:s roll inom cybersäkerhet, Avgränsningen kommer även att vara den problematiska aspekten av AI-baserad cybersäkerhet där arbetet inte kommer att fördjupa sig i den potential AI-baserad cybersäkerhet har. Istället kommer arbetet avgränsa sig till de potentiella risker, utmaningar och påverkningar för den mänskliga faktorn som uppstår av automatisering och teknologiberoende när AI-baserad cybersäkerhet används som verktyg.

3.3 Förväntat resultat

Det förväntade resultatet i detta arbete kommer att vara att identifiera och kunna öka kunskapen kring de olika potentiella riskerna, utmaningarna och påverkningar för den mänskliga faktorn kring AI-baserad cybersäkerhet. Detta arbete förväntas även, med hjälp av denna insikt inom riskerna, utmaningarna och påverkningarna ge en grund till ökad medvetenhet. Detta för att kunna skapa ett förebyggande arbete för den mänskliga faktorns påverkan inom AI-baserad cybersäkerhet. Genom en ökad medvetenhet och utbildning kan riskerna minimeras kopplade till den mänskliga faktorns påverkan inom AI-baserad cybersäkerhet.

Detta arbete ska även förvänta resultat i en fördjupad förståelse kring hur organisationer kan hitta en balans mellan automation och mänsklig kontroll för att kunna skapa ett sådant bra och pålitligt cybersäkerhetsarbete.

4 Metod

Detta kapitel redogör och visar det fördelar med den valda forskningsmetoden som valts ut och använts för att skapa denna grund till detta arbete och besvara studiens frågeställning. Kapitlet redogör även datainsamlingsprocesser, analysmetod och forskningsetiska överväganden.

4.1 Systematisk litteraturstudie

Detta arbete har genomförts som en systematisk litteraturstudie. Det är en metod för att undersöka hur den mänskliga faktorn påverkas av automatisering och teknologiberoende i AI-baserad cybersäkerhet (Nightingale, 2009). En systematisk litteraturstudie är en metod som är strukturerad och som använts för att identifiera, analysera och granska redan befintlig forskning inom det specifika ämnet eller området (Nightingale, 2009). Detta arbetets syfte är att skapa en förståelse kring hur den mänskliga faktorn påverkas av automatisering och teknologiberoende i AI-baserad cybersäkerhet. En systematisk litteraturstudie syftar till att identifiera alla studier som berör en specifik fråga och metodiken har utvecklats för att minimera risken av att vara partisk (Nightingale, 2009). En systematisk litteraturstudie utgår från en specifik fråga men där metoden innebär flera steg för att minimera risken att vara partisk (Nightingale, 2009). De flera stegen i en systematisk litteraturstudie innefattas av utveckling av ett protokoll med inkludering och exkluderingskriterier, sökning av litteratur, urval av studier, kritisk granskning, och syntes av data (Nightingale, 2009). Dessa steg användes för att kunna ge en mer omfattande, balanserad och opartisk sammanfattning av all den tidiga forskningen (Nightingale, 2009). Det huvudsakliga syftet med en systematisk litteraturstudie är att få en litteraturöversikt över den befintliga forskningen för att kunna hitta användbar information, forskningsluckor och kunna informera framtida studier (Nightingale, 2009).

Eftersom syftet var att få en ökad förståelse och identifiera eventuella gap i forskningen kring ett komplext område gällande en specifik frågeställning har den systematiska litteraturstudien varit en passande metod för att samla in och analysera befintlig forskning. Metoden möjliggjorde ett transparent urval, en analys av befintlig forskning och en syntes av mönster som framträtt. Området har en snabb utveckling, detta gör att det är extra viktigt att analysera befintlig forskning för att identifiera kunskapsluckor och möjliga framtida studier. Genom att läsa den befintliga forskningen så möjliggjorde det att få en förståelse för det grundliga och återkommande problem, mönster och de möjligheter som är kopplat till studiens område (Nightingale, 2009).

4.1.1 Sökstrategier & urvalskriterier

Detta arbetets datainsamling har gjorts genom en systematisk sökning av de vetenskapliga artiklar enligt följande databaser: IEEE Xplore och Google Scholar.

Arbetet har gjorts med hjälp av olika typer av sökstrategier som genomförs med hjälp av specifika nyckelord för att få fram relevanta artiklar inom området. Några exempel av dessa sökningar är:

- “human factor” AND “AI-based cybersecurity”
- “Human factor” AND “AI”
- “Human factor” AND “Cybersecurity”
- “cybersecurity” AND “AI”

Det primära fokuset i detta arbete är den mänskliga faktorn och hur den påverkas av AI-baserad cybersäkerhet i form av automation och teknologiberoende. Det innebär att inom dessa sökstrategier finns det tre olika teman som är mänskliga faktorn, AI och cybersäkerhet. Eftersom att det finns ett begränsat antal vetenskapliga publikationer som behandlade alla tre teman så inkluderades även artiklar som enbart innefattar två av dessa tre teman (mänskliga faktorn, AI och cybersäkerhet) för att kunna möjliggöra en större bredare analys och diskussion.

Arbetet har gjorts genom olika kriterier i inkludering och exkluderingsprocessen som följts av prisma modellen där de vetenskapliga artiklarna filtrerats och det kriterierna är följande:

Det inkluderande kriterierna

- Vetenskapliga artiklar som har fokus inom området AI och cybersäkerhet (om den diskuterar implikation för mänsklig interaktion)
- Vetenskapliga artiklar som har fokus inom området Mänskliga faktorn och cybersäkerhet
- Vetenskapliga artiklar som har fokus inom Mänskliga faktorn och AI
- Med tanke på den snabba utvecklingen som sker inom AI så måste artiklarna vara publicerade senast 2018 för att säkerhetsställa artiklarna är aktuella.
- Det 30 första artiklarna per sökresultat som visas då sökningen i det olika databaserna går efter relevans

Det exkluderande kriterierna

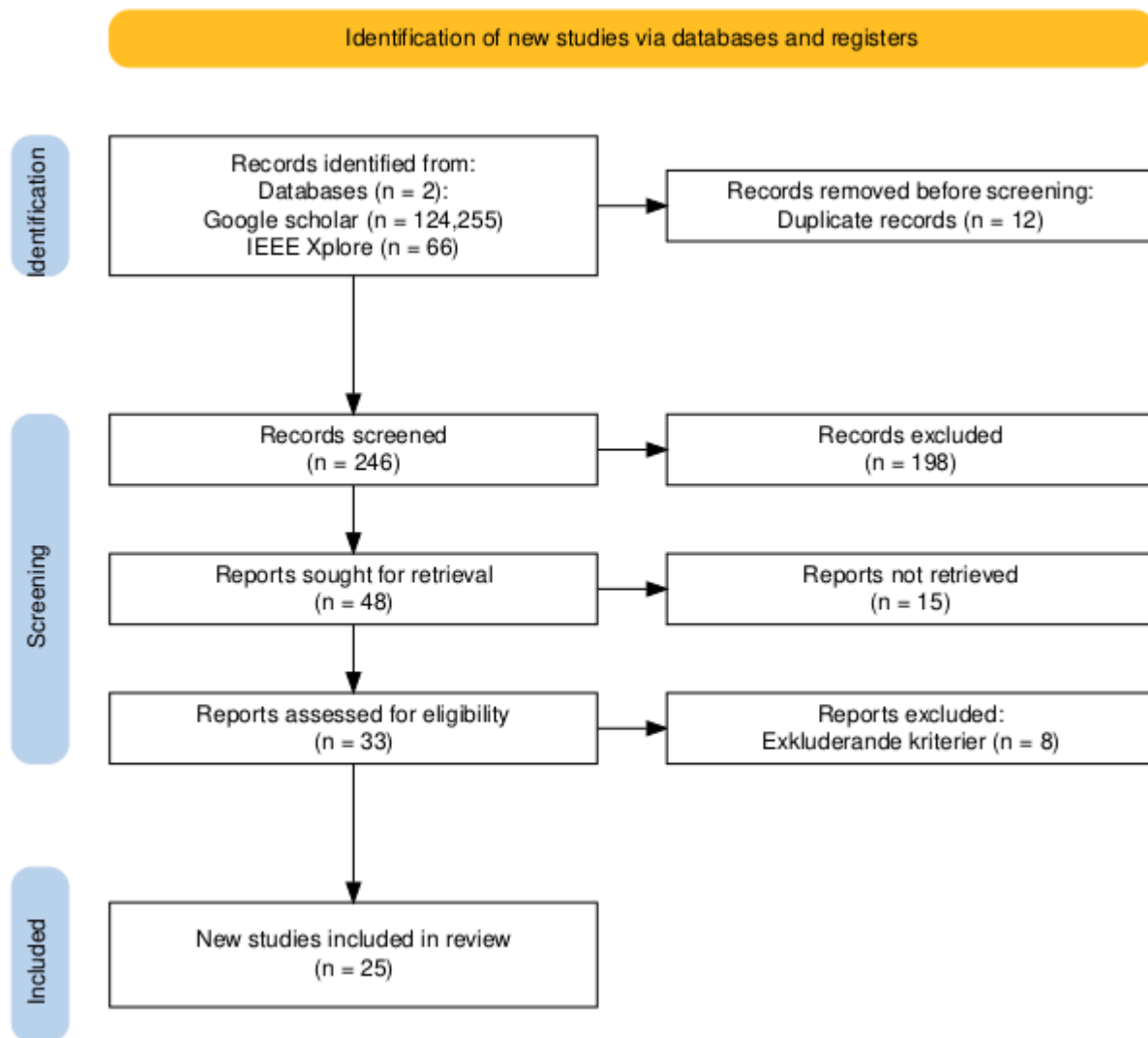
- Artiklar som enbart granskar de tekniska aspekterna av AI-baserad cybersäkerhet utan koppling till risker för den mänskliga faktorn.
- Artiklar som publicerades 2017 eller tidigare.
- Artiklar som saknar kontext av AI och Cybersäkerhet
- Artiklar som saknar implikation för mänsklig interaktion
- Artiklar som är dubletter från de inkluderande artiklarna.
- Artiklar som enbart innefattas av ett tema
- Artiklar som kommer efter det 30 första artiklar per sökresultat

Dessa kriterier och sökresultaten har sedan sammanställts och genomförts genom en manuell granskning av artiklarna för att säkerhetsställa relevansen.

4.1.2 Val av artiklar

En prisma modell inkluderar ett flödesdiagram som visuellt sammanfattar de olika faser i den urvalsprocess som görs under inkludering och exkluderingsprocessen (Nightingale, 2009). Prisma modellen illustrerar det olika antalet artiklar som har hittats genom databassökning där dessa artiklar sedan antingen inkluderats eller exkluderats beroende av de olika kriterierna (Nightingale, 2009). För mer illustrerad information se figur 1.

För att identifiera de relevanta vetenskapliga artiklar genomfördes det systematiska sökningar i databaserna Google Scholar och IEEE Xplore och en urvalsprocess genomfördes där urvalsprocessen illustreras i figur 1 . Totalt resulterade dessa sökningar i 124300 ungefärliga träffar innan filtreringsprocessen startades. Många artiklar var inte relevanta eller låg utanför arbetets fokusområde. Det begränsade urvalet att enbart granska de 30 första artiklar från varje specifik sökning av använda nyckelord i Google Scholar och IEEE Xplore då dessa sökmotorer filtrerar efter relevans. Arbetet efter processen av titel och abstract återstod 246 artiklar där 48 av dessa verkade lovande och intressanta men där enbart 33 av dessa artiklar var möjliga att få tillgång till i fulltext. Den sista processen i screening är att läsa de 33 olika artiklarna där 8 av dessa inte uppfyllde de inkluderande kriterierna och resultatet efter PRISMA modellens riktlinjer är det 25 artiklar som inkluderandes i denna analys.



Figur 1 - Prisma modell: urvalsprocess

4.1.3 Analys av artiklar

Detta arbete har valt en tematisk analysmetod för att analysera litteraturen. Tematisk analysmetod är en metod som används för att utöka befintlig kunskap som fungerar tillsammans med en systematisk litteraturstudie (Xiao & Watson, 2019).

Arbetet har i analysprocessen extraherat teman från den inkluderande litteraturen där dessa teman sedan har blivit klustrad och syntetiserats till analytiska teman där grunden var att identifiera och kategorisera för att hitta mönster och samband (Xiao & Watson, 2019).

Den tematiska analysen består av följande steg:

1. **Kodning av material:** att analysera och identifiera återkommande teman och nyckelbegrepp(Xiao & Watson, 2019).
2. **Tematisering:** Gruppera information i ett större tema som till exempel mänskliga misstag, risker och säkerhetsstrategier(Xiao & Watson, 2019).
3. **Syntes och tolkning** - Analysera resultaten och identifiera forskningsluckor som kan finnas inom ämnet mänskliga faktorn och AI-baserad cybersäkerhet(Xiao & Watson, 2019).

Arbetet har kring kodning av material gjorts genom att läsa de 25 inkluderande artiklarna i sin helhet. Det som var relevant från artiklarnas innehåll markerades och antecknades manuellt. Det som var fokus kring kodningen var innehåll som var relaterat till områdets innehåll men även begrepp och återkommande uttryck.

Tematiseringen gjordes genom att sortera dessa koder och grupperade dessa i en översikt av teman. Arbetet gjordes sedan genom att jämföra kodernas kontext för att hitta olika mönster samt likheter kopplade till arbetets frågeställning. De huvudsakliga teman som identifierades var följande:

- Bristande förståelse och kunskap
- Teknologiberoende och för hög tillit till AI-baserade system
- Automatiseringens påverkan på mänsklig roll
- Etiska dilemman och otydlig ansvarsfördelning med användning av AI-baserade system

Dessa teman jämfördes sedan med den ursprungliga texten i artiklarna för att med säkerhet kunna se att det representerade innehållet på ett transparent sätt.

Syntes och tolkning har sedan gjorts i detta arbete genom att använda dessa teman för att svara på detta arbetets frågeställning där varje tema tolkades genom en koppling till den tidigare forskningen. Resultatet blev sedan en grund för de 4 huvudsakliga resultaten som syns i resultat kapitlet.

4.2 Forskningsetiska principer

Detta arbete är baserat på offentlig forskning och innehåller därför ingen känslig data men arbetet är baserat på de forskningsetiska aspekter som är enligt Vetenskapsrådets riktlinjer (2024).

Objektivitet: Arbetet har kritiskt granskat källorna för att säkerhetsställa att det är en rättvis och opartisk analys (Vetenskapsrådet, 2024).

Källhänvisning: De källor som använts har angetts på ett korrekt sätt enligt de akademiska riktlinjerna (Vetenskapsrådet, 2024).

Transparens: Arbetets analysmetoder och urval beskrivs tydligt för att kunna möjliggöra att arbetet kan replikeras (Vetenskapsrådet, 2024).

För att åstadkomma en objektivitet har arbetets urval av artiklar gjorts genom det fördefinierade inkludering och exkluderingskriterier och artiklar har inte tagits bort på grund av personliga åsikter. Källhänvisningen har följt APA där samtliga referenser som refereras i detta arbete kring påståenden, forskningsresultat och definitioner har hänvisats till texten för att visa resultat från tidigare forskares arbeten. Transparens har i detta arbete gjorts genom hela metoden från sökstrategi och urval till analys av artiklar för att kunna möjliggöra att arbetet går att reproducera. Prima modellen i figur 1 visar även hur detta arbete har gjorts för att uppnå sin analys av artiklar.

5 Materialpresentation

Detta kapitel kommer visa de olika tematiska grupperingarna av artiklar och hur många artiklar som är på respektive tematisk gruppering. Kapitlet inkluderar även en översikt av alla artiklar som är i respektive grupperad tabell och som valts till detta arbete efter inkludering och exkluderingsprocessen med titeln på artikeln, författaren och en kort sammanfattning av varje artikel.

5.1 Tematisk gruppering av artiklar

I tabell 1 presenteras de olika grupperna i en tematisk gruppering av artiklar med gruppnamn, fokusområde och hur många artiklar varje grupp innehas av. Grupperingen används för att strukturera materialet efter olika kombinationer av forskningsfokus.

Grupp	Fokus	Antal artiklar
A	Mänskliga faktorn + Cybersäkerhet	9
B	Mänskliga faktorn + AI/Automation	3
C	Mänskliga faktorn + Automation + Cybersäkerhet	4
D	AI + Cybersäkerhet	6
E	Mänskliga faktorn + AI + Cybersäkerhet	3

Tabell 1 - Tematisk gruppering av artiklar

5.2 Översikt av inkluderande artiklar

I detta avsnitt ges en översikt av alla inkluderande artiklar i respektive grupp med namn på artikeln, författaren och en kort sammanfattning om den inkluderande artikeln.

5.2.1 Översikt av Grupp A

De artiklar som identifieras i grupp A behandlar på olika sätt den mänskliga faktorn kopplat till cybersäkerhet. För mer information se tabell 2.

Artikel	Författare	Sammanfattning
Human factor, a critical weak point in the information security of an organization's Internet of things	Hughes-Lartey et al.(2021)	Undersöker den mänskliga faktorn som en kritisk svaghet inom cybersäkerhet där fokuseringen är i samband med Internet of Things (IoT).

The human factor: assessing individuals' perceptions related to cybersecurity	Ramlo och Nicholas (2021)	Det olika synsätt som finns på cybersäkerhet hos olika individer som är allt från experter inom området till individer med okunskap och vilka risker det finns med okunskap inom cybersäkerhet.
Human factor security: evaluating the cybersecurity capacity of the industrial workforce	Ani, He och Tiwari (2019)	Den mänskliga faktorns betydelse för en säkerhet inom industriella kontrollsistem. Argumenterande kring att cyberattacker vanligt utnyttjas av personalens brister i kunskap om cybersäkerhet.
A Review: Human Factor and Cybersecurity	Abzakh och Althunibat (2023)	belyser den mänskliga faktorn som den svagaste länken inom cybersäkerhet och betonar vikten av utbildning och medvetenhetshöjning för att uppfylla bättre säkerhetsstrategier.
Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution	Momoh, Adelaja och Ejiwumi (2023)	Utforskar om hur det mänskliga beteendet påverkar cybersäkerheten inom finanssektorn med ett särskilt fokus på Social engineering.
Addressing Human Factors in Cybersecurity Leadership	Triplett (2022)	Hur den mänskliga faktorn påverkar utmaningar inom cybersäkerhetens ledning på en arbetsplats och identifierar att oavsiktliga mänskliga handlingar är den svagaste länken för att skydda data.
Leveraging the Human Factors Discipline for Better Cybersecurity Outcomes: A Roundtable Discussion	Cunningham, Nobles, Robinson och Haney (2024)	Den mänskliga faktorn och hur den kan tillämpas inom cybersäkerhet. Vilka utmaningar organisationer kan stå inför och hur integrering av mänskliga faktorer kan leda till ett bättre resultat inom informationssäkerhet.
Leveraging human factors in cybersecurity: an integrated methodological	Pollini, Callari, Tedeschi, Ruscio, Save, Chiarugi och Guerri	Den mänskliga faktorns påverkan på cybersäkerheten inom hälsoorganisationer med

approach	(2022)	ett helhetssynsätt som integrerar tekniska, individuella och organisatoriska aspekter.
Understanding of Human Factors in Cybersecurity: A Systematic Literature Review	Rohan, Funilkul, Pal och Chutimaskul (2021)	Den mänskliga faktorns roll inom cybersäkerhet och en identifiering av valda metoder av tidigare forskning inom området och vilka brister den tidigare forskningen haft.

Tabell 2 - Grupp A artiklar

5.2.2 Översikt av Grupp B

De artiklar som identifieras i grupp B behandlar på olika sätt den mänskliga faktorn kopplat till AI och automation. För mer information se tabell 3.

Artikel	Författare	Sammanfattning
How to account artificial intelligence in human factor analysis of complex systems?	Zarei, Khan och Abbassi (2023)	Användning av AI och system baserade på suddig logik. Granskar hur det finns möjlighet att kunna förbättra förståelsen och hanteringen av mänskliga fel i industrier.
Addressing Behavioural Technologies Through the Human Factor: A Review	Irizar-Arrieta, Gómez-Carmona, Bilbao-Jayo, Casado-Mansilla, López-De-Ipiña och Almeida (2020)	Undersöker hur beteendeteknologier kan användas för att få en högre effektivitet genom att påverka det mänskliga beteendet.
Leading with AI in critical care nursing: challenges, opportunities, and the human factor	Hassan och El-Ashry (2024)	Hur sjuksköterskor inom intensivvård upplever en integration av AI med diskussion om utmaningar och möjligheter som finns inom vården med AI.

Tabell 3 - Grupp B artiklar

5.2.3 Översikt av Grupp C

De artiklar som identifieras i grupp C behandlar på olika sätt den mänskliga faktorn kopplat till cybersäkerhet och automation. För mer information se tabell 4.

Artikel	Författare	Sammanfattning
AI to Minimize Human Error in Cybersecurity: Enhancing Threat Detection and Incident Response Accuracy	James (2024)	Hur AI kan användas för att minska risken kring mänskliga fel men även hur automatisering och beslutssystem kan förbättra och effektivisera förmågan att upptäcka hot och hantera incidenter.
Botching Human Factors in Cybersecurity in Business Organizations	Nobles (2018)	Den mänskliga faktorns underskattning och den teknologiska determinism med kritik mot den utbredda tro att teknologi är lösningen på cybersäkerhetsproblem.
STRESS, BURNOUT, AND SECURITY FATIGUE IN CYBERSECURITY: A HUMAN FACTORS PROBLEM	Nobles (2022)	undersöker stress och utbrändhet som betydande faktorer för den mänskliga faktorn inom cybersäkerhet med kritik mot de tekniska lösningar som prioriteras och diskuterar kring mänskligt centrerade metoder inom cybersäkerhet.
Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity	Nobles (2019)	Hur mänskliga faktor program skulle vara effektivt för cybersäkerheten där artikeln använder paralleller från andra i områden som infört dessa program för att minska mänskliga fel.

Tabell 4 - Grupp C artiklar

5.2.4 Översikt av Grupp D

De artiklar som identifieras i grupp D behandlar på olika sätt cybersäkerhet kopplat till AI. För mer information se tabell 5.

Artikel	Författare	Sammanfattning
----------------	-------------------	-----------------------

Artificial intelligence for cybersecurity: Literature review and future research directions	Kaur, Gabrijelčić och Klobučar (2023)	Användningen av AI och hur det skulle kunna stärka skyddet mot cyberattacker och automatisera uppgifter.
AI-Enhanced Cyber Security Proactive Threat Detection and Response Systems	Nallapareddy och Katta (2025)	AI kan användas för att förbättra cybersäkerheten och hur AI kan användas för att analysera stora mängder data för att kunna identifiera och reagera på cyberhot.
Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature	Wiafe, Koranteng, Obeng, Assyne, Wiafe och Gulliver (2020)	Hur AI har bidragit till förbättringar inom cybersäkerhet men att det även finns en applikationsområden där AI har presterat sämre och behovet av att fortsätta utforska nyare metoder och bredare tillämpningar för AI inom cybersäkerhet.
Artificial Intelligence in Cyber Security	Das och Sandhane (2021)	Hur AI kan förbättra olika skyddsmekanismer inom cybersäkerhet med en översikt om befintliga AI-lösningar men även diskutera kring det utmaningar som finns med att integrera AI inom området cybersäkerhet.
Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity	Zeadally, Adi, Baig och Khan (2020)	undersöker hur AI kan förbättra cyber säkerhetslösningar men även belyser utmaningar och den pågående situation mellan försvar, anfall och mänsklighet av användning för AI inom cybersäkerhet.
Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity	Kuzlu, Fair och Guler (2021)	Vilka risker det finns som är specifika mot Internet of Things-enheter och hur AI kan användas både för att skydda dessa system men även att genomföra

		attacker. Diskuterar även det risker som finns att AI kan missbrukas av angripare och manipulera olika typer av AI-system.
--	--	--

Tabell 5 - Grupp D Artiklar

5.2.5 Översikt av Grupp E

De artiklar som identifieras i grupp E behandlar på olika sätt den mänskliga faktorn kopplat till cybersäkerhet och AI. För mer information se tabell 6.

Artikel	Författare	Sammanfattning
AI Efficiency in Cybersecurity: Estimating Token Consumption for Optimal Operations	Romanous och Ginger (2024)	Undersöker hur effektiv AI inom cybersäkerhet är med ett särskilt fokus på kostnadsoptimering. Genom användning av tre olika modeller enbart mänskligt, AI och en hybrid mellan de två kunna hitta den bästa säkerhetsstrategin av användning med AI.
Cybersecurity Automation with AI: Reducing Human Error and Improving Incident Response	Anayat (2024)	Utforskar hur AI och maskininlärning kan tillämpas på flera olika tekniska domäner för att kunna förbättra cybersäkerheten och minska den mänskliga faktorn.
Serious Games for Cybersecurity: How to Improve Perception and Human Factors	Santa Barletta, Calvano, Caruso, Curci och Piccinno (2023)	Hur utbildning inom cybersäkerhet kan förbättras för att minimera den mänskliga faktorn men även kring att utveckla mer omfattande metoder som integrerar förståelsen av mänsklig perception där AI kan användas som ett verktyg.

Tabell 6 - Grupp E artiklar

6 Analys

Detta kapitel baseras på analysen av hur den mänskliga faktorn påverkas av automatisering och teknologiberoende inom AI-baserad cybersäkerhet. Analysen är baserad på 25 vetenskapliga artiklar som tagits fram genom en systematisk litteraturstudie.

Det har identifierats 4 huvudsakliga teman i denna analys som är kopplad till arbetets frågeställning. De 25 vetenskapliga artiklarna har tillsammans ett brett fokusområde men det var ett måste att skala ner det analyserade teman för att kunna uppnå ett svar för syftet med detta arbete. De 4 huvudsakliga teman som har analyserats kom fram genom den tematiska analysen av artiklarnas innehåll och byggdes på återkommande mönster. Artiklar från de olika grupperna kan bidra till samma tema då ett tema kan kopplas till flera olika forskningsfokus. De 4 huvudsakliga teman som analyserat kring detta arbete är följande: (1) bristande förståelse och kunskap, (2) teknologiberoende och för hög tillit till AI-baserade system, (3) automatiseringens påverkan på mänsklig roll och (4) Etiska dilemman och otydlig ansvarsfördelning med användning av AI-baserade system. Det finns en stor forskningslucka inom just hur den mänskliga faktorn påverkas av en AI-baserad cybersäkerhetsmiljö där forskning relaterat till AI till största del handlar om dess potential. Det är därför viktigt att även kunna se vilka risker och hur den mänskliga faktorn påverkas av AI inom cybersäkerhet där dessa fyra teman kan visualisera hur den mänskliga faktorn påverkas av automatisering och teknologiberoende inom AI-baserad cybersäkerhet.

6.1 Bristande förståelse och kunskap

En stor del av de inkluderande artiklarna i denna analys har visat på att det finns en begränsad kunskap inom cybersäkerhet och AI-system för användare. Detta var ett återkommande tema i de inkluderande artiklarna från flera av de olika grupperna men där detta framstod tydligt i särskilt grupp A (se Tabell 2) och grupp B (se Tabell 3). Den bristande förståelsen och kunskapen inom cybersäkerhet är en referering till den mänskliga faktorn är hur avsaknaden av viktig information och insikt som individer behöver för att kunna ha möjligheten att agera säkert i en digital miljö (Ramlo & Nicholas, 2021; Ani et al., 2019). Hughes-Lartey et al. (2021) och Anayat (2024) menar att detta kan leda till antingen medvetna beslut eller oavsiktliga handlingar som ökar risken för dataintrång och säkerhetsincidenter. Pollini et al. (2022) gjorde en studie för att se skillnaden på beteenden, attityder och kunskap mellan IT-personal och icke IT-personal inom området cybersäkerhet. Studien visade att IT-personal som hade kunskap rent generellt självklart presterade bättre men det visade även att trots kunskapen som IT-personalen borde ha som en grund så i vissa aspekter presterade den icke IT-personalen bättre kring sociala nätverk och incidentrapportering. Pollini et al. (2022) menar att detta kan vara en indikation på att det fortfarande kan finnas luckor i förståelsen även hos IT-specialister kring vissa specifika aspekter av säkerhet.

Det kan därför även visa hur viktigt det är att bilda kunskap och förståelse kring alla olika aspekter inom cybersäkerhet. Det kan därför finnas en risk att utbilda personal i vissa aspekter av cybersäkerhet då detta kan göra att det byggs ett självförtroende hos individen som gör att individen tror att det har bättre koll än vad den har och det kan i sin tur leda till oavsiktliga fel och handlingar. Flera av de olika artiklarna från specifikt grupp A betonar vikten av utbildningsprogram inom cybersäkerhet för att kunna öka medvetenheten och förbättra kunskapen. Momoh et al. (2023) menar dessa utbildningsprogram kan hjälpa individer att identifiera och avvisa social ingenjörskonst, bedöma den tillförlitlighet som kan uppkomma och hur individen ska agera i olika situationer. Det finns även risker kring utbildningar beroende på individens synsätt och beteende för utbildningen och det rekommenderas att utbildningar ska ske regelbundet och att det ska finnas en förstärkt utbildning för att kunna motverka att kunskapen hos individen avtar med tid men även för att kunna visa vikten av utbildningen (Cunningham et al., 2024).

För trots att AI-baserade system göra stora framsteg i utveckling för cybersäkerhet så ändrar inte det kring hur viktigt kunskapen och förståelsen för AI-baserade system är inte enbart en teknisk fråga då mänskliga fel fortfarande utgör betydande sårbarheter (James, 2024). Enligt Wiafe et al. (2020) och Irizar et al. (2020) är det därför viktigt att trots automatisering av AI-baserade system så är det viktigt att hitta en balans mellan teknik, människor och policyhantering. Specifikt grupp A och grupp B visar artiklarna att en bristande förståelse och kunskap om cybersäkerhet är och kommer vara en fortsatt kritisk mänsklig faktor som bidrar till olika typer av säkerhetsrisker. Det kan analyseras att bristande förståelse och kunskap leder till brist på medvetenhet, kunskapsluckor och felaktiga uppfattningar, det framgår därför att utbildningar och medvetenhetshöjande insatser är viktiga åtgärder för att kunna motverka dessa brister och kunna ha möjlighet att förbättra den övergripande cybersäkerheten (Ramlo & Nicholas, 2021; Abzakh et al., 2023).

Sammanfattningsvis i denna analys är det flera indikationer på att bristande förståelse och kunskap är centrala för cybersäkerheten, AI-baserade system ger en stor potential för att förbättra cybersäkerheten men den mänskliga faktorn försvinner inte. Kunskap och förståelse är någonting som denna analys tyder på kommer att behövas för att kunna uppnå en säker cybersäkerhet men även kunna ge AI-baserade lösningar den fulla potentialen.

6.2 Teknologiberoende och för hög tillit till AI-baserade system

Det finns inom denna analys ett tema kring hur organisationer men även på samhällsnivå har kontinuerligt haft en ökad beroendeställning till teknik och det kommer fortsätta vara en ökad riktning med särskilt AI-baserade system. Det finns mycket av det inkluderande artiklarna som påpekar den potential som AI-baserade system har för cybersäkerheten men en stor del av artiklarna påpekar även att det finns påverkningar på den mänskliga faktorn att använda sig av AI-baserade system och vilka risker det finns med teknologiberoende och att för hög tillit rent generellt är en

riskfaktor. Romanous och Ginger (2024) och Nobles (2018) menar att i dagsläget så är det svårt, kostsamt och riskfyllt att göra en fullständig övergång till AI-baserade system utan mänsklig inblandning, där ett ensidigt fokus på implementering av AI-baserade system som enbart är från teknisk synpunkt är skadligt utan att beakta de mänskliga faktorerna.

En övertro på AI-baserade system kan leda till risker med att den mänskliga vaksamheten minskar men även till fler felbedömningar om AI-systemen gör misstag och det uppkommer nya hot som systemet inte är tränat för (Romanous & Ginger, 2024). Flera av de olika källorna betonar att det är viktigt att hitta en balans i dagsläget mellan AI och mänsklig interaktion. Romanous och Ginger (2024) menar att det behöver finnas en hybridmodell där användning av mänsklig expertis kan använda AI-teknik som ett verktyg för att kunna dra nytta av styrkorna från båda håll men där automatisering med AI inom alla områden inom cybersäkerhet inte är rätt väg. Automatisering med AI-baserade system är att automatisera rutinmässiga uppgifter och analysera stora datamängder men att det ska fortfarande finnas en mänsklig interaktion med kritiska beslut, hantering av undantag och ett fokus på strategisk ledning (Nallapareddy & Katta, 2025; Triplett, 2022). Hassan och El-Ashry (2024) menar att det finns en oro med implementering av AI-baserade system som ska automatisera att det uppstår en "deskilling" som betyder att mänsklig expertis kan minska om individer förlitar sig för mycket på AI-system och inte underhåller sin egna expertis inom området. Det finns därför en betoning på hur viktigt det är att mänskliga experter behöver planering och utbildning för att ha förståelse och kunna använda AI-system på ett effektivt sätt (Das & Sandhane, 2021).

Flera artiklar betonar oron av användning av Automatiserade AI-system och risken för en för hög tillit till AI-system då AI-system kan även vara sårbara för nya attacker som systemet inte har tränats på tidigare (Romanous & Ginger, 2024). Das och Sandhane (2021) menar att cyberkriminella använder också sig utav AI och detta kan leda till mer utvecklade attacker och att därför kan ett överdrivet teknologiberoende av det nya AI-baserade lösningarna skapa nya risker som tidigare inte varit känt.

Flertalet artiklar i denna analys förespråkar därför vikten återigen av en balans mellan människa och AI och att enbart använda AI-system som ett extra verktyg för att kunna effektivisera en verksamhet men att det inte ska finnas ett beroende att använda sig av systemet. Romanous och Ginger (2024) menar att det finns risker med att ha en för hög tillit till systemet men där Hassan och El-Ashry (2024) även menar att det finns risker med att ha för låg tillit till systemet och att det måste finnas en tydlig balans mellan att vara ett effektivt system men ha möjlighet att kunna visa transparens. Hassan och El-Ashry (2024) beskriver i sin artikel att det kan finnas risker för en "black box"-problematik där användarna av systemet inte förstår hur det AI-baserade systemet har kommit fram till sina slutsatser och att det kan leda till en misstro mot systemet ifall det finns en avsaknad av transparens. Detta kan i sin tur leda till en misstro på systemet och det används på ett felaktigt sätt och att för att ett AI-system ska kunna integreras på

ett effektivt sätt i praktiken så behöver det finnas tolkningsbara och tydliga förklaringar till hur resultatet har kommit fram (Hassan & El-Ashry, 2024).

Sammanfattningsvis visar analysen därför att en för hög tillit och ett teknologiberoende till AI-baserade system är riskabelt och att det istället förespråkas om en integrerad och balanserad väg där människan och AI-system används som verktyg. För att kunna motarbeta en för hög tillit och negativa risker och konsekvenser så behövs det förklaringar till resultat, transparens och ett fokus på den mänskliga faktorn när designen för systemet utvecklas men även utbildningar för de användare som kommer att arbeta med det AI-baserade systemet (Kaur, Gabrijelčić och Klobučar, 2023).

6.3 Automatiseringens påverkan på mänsklig roll

Flertalet artiklar i denna analys påpekar automatisering i både positiva och negativa ansatser. Det finns ett tydligt tema kring effektiviseringen med automatisering men det kan även tydligt analyseras att det finns en påverkan på mänsklig roll. Det finns en väldigt delad uppfattning av hur automatiseringen påverkar den mänskliga rollen där artiklar från specifikt grupp D (se Tabell 5) har en väldigt positiv syn på den potential AI-baserade system har för cybersäkerhet medan artiklar från Grupp B har en mer negativ syn till hur automatisering inom cybersäkerhet ska gå till. Automatisering i form av särskilt AI-baserade system har en inverkan på den mänskliga rollen inom cybersäkerhet och komplexa system (Zarei et al., 2023). Det finns ett flertal möjligheter med den potential som AI-baserade system har att kunna förbättra incidenthantering och även kunna minska mänskliga fel och det finns många delar av cybersäkerheten som idag kan automatiseras (James, 2024). Kaur et al. (2023) menar att policyhantering i nätverk där AI-baserade system kan automatisera med hjälp av centraliserade kontroller, åtkomstkontroller, riskanalys och konsekvensbedömningar är specifika delar som AI-baserade system idag skulle kunna automatiseras med hjälp av den potential AI-system har.

Övergången från mänskligt drivna uppgifter måste ske gradvis och att det behöver en mänsklig interaktion för att kunna installera systemen, träna och ha en tillsyn för att möjliggöra att AI-systemet utvecklas (Romanous & Ginger, 2024). Romanous och Ginger (2024) menar att när AI-systemen har utvecklats tillräckligt så finns det en stor möjlighet att AI-baserade system kan ta över det vanliga rutinmässiga uppgifter. Romanous och Ginger (2024) menar att det kan minska den mänskliga interaktionen och menar att det finns en uppskattning att den mänskliga interaktionen kan minska till under 10% för de flesta uppgifter inom 5 år.

James (2024) menar att denna ökade automatisering och den potential AI så är syftet att kunna påskynda svarstider, förbättra detektions noggrannhet och även kunna minska antalet positiva resultat som är falska. AI kan analysera stora mängder data som till exempel säkerhetsloggar för att kunna upptäcka säkerhetsrisker där det kan finnas utmaningar för mänskliga analytiker att upptäcka riskerna manuellt (James, 2024).

Men trots den potential AI-baserade system har för automatiseringen så finns det fortfarande stora risker med att automatisera system, det kommer vara fortsatt viktigt att ha ett högt fokus på den mänskliga faktorn då den mänskliga faktorn fortfarande är en betydande faktor för cyberhot och tekniska lösningar är inte alltid tillräckligt (Momoh et al., 2023). Nobles (2018) menar att organisationer har en tendens att lägga ett för stort fokus och investeringar på de tekniska delarna istället för att förstå mänskliga beteenden inom cybersäkerhet. Nobles (2018) menar även att automatisering kan även leda till en lägre tillit och en misstro hos individer och det kan bli en rekyleffekt ifall användarna känner sig fränkopplade. Det är därför viktigt att kunna se vilka uppgifter och funktioner som kan optimeras tillräckligt för automatisering för att förhindra att automatiseringen inte missbrukas och det går att fastställa alla de kognitiva krav som varje funktion och uppgift har (Nobles, 2019).

Det är därför viktigt att veta att införande av AI-baserade system inom cybersäkerhet leder till förändrade roller och ansvarsområden för människan och att automatisering har en påverkan på den mänskliga rollen (Hassan & El-Ashry, 2024). Ett införande av AI-baserade system kan därför leda till att det blir mer övervakande roller för människan att hantera AI-systemets utdata och kan fastställa att systemet fungerar korrekt (Hassan & El-Ashry, 2024). Das och Sandhane (2021) och Nobles (2022) menar att det är viktigt att investera i den mänskliga aspekten när implementering av AI-system görs där detta är inklusive utbildning och planering för att personalen sedan ska kunna effektivt kunna jobba med deras nya system.

Sammanfattningsvis så har automatisering en stor påverkan på den mänskliga rollen inom cybersäkerhet och där det är viktigt att redan i utvecklingsfasen av systemet att få in de mänskliga aspekterna (Santa Barletta et al., 2023). En automatisering inom cybersäkerhet leder till att det skiftar ett fokus från manuella rutinuppgifter till att det blir en mer övervakande och strategiskt översikt. En mer komplex problemlösning med samarbete med AI-baserade system och mänsklig interaktion men trots det framsteg som kan göras med automatisering så förblir hanteringen av den mänskliga faktorn och dess förståelse en fortsatt faktor för att säkerhetsställa effektiva och säkra system (Ani et al., 2019).

6.4 Etiska dilemman och otydlig ansvarsfördelning med användning av AI-baserade system

Det sista huvudsakliga tema som denna analys kan hitta som är kring arbetets frågeställning är att det finns viss problematik kring etiska dilemman och otydliga ansvarsfördelningar med användning av AI-baserade system. Kaur et al. (2023) menar att bristen på transparens inom AI-baserade system gör att inom cybersäkerhet så blir det svårt för en människa att tolka varför systemet identifierar något som ett hot eller varför systemet gör en åtgärd. Kaur et al. (2023) och Hassan och El-Ashry (2024) menar även att bristen på transparens gör det även svårare för att kunna fastställa ansvar ifall systemet skulle göra misstag eller misslyckas och att transparensen är nödvändig för

cybersäkerhetens förtroende och ansvarsskyldighet. Hassan och El-Ashry (2024) och James (2024) menar även att det finns även risker för att ett AI-system skulle kunna vara partiskt och att detta är en etisk oro och ifall systemets träningsdata skulle vara ofullständig eller fel så finns det risker att det AI-baserade systemet kommer ge ofullständiga och fel resultat.

Zarei et al. (2023) menar därför att det finns en stor osäkerhet med användning av AI-baserade system då risken för opålitliga resultat från AI-system kan leda till felaktiga bedömningar som skapar etiska problem som till exempel att systemet blockerar en legitim trafik.

Ansvarsfördelningen med användning av AI-baserade system är svårt att fastställa en ansvarig och det krävs ramverk och tydliga riktlinjer för att kunna besluta ansvaret när AI-system tar beslut (Hassan & El-Ashry, 2024). Utan ett ordentligt ramverk så är risken stor att ansvaret blir otydligt, speciellt när det gäller system inom cybersäkerhet och där risker kring felaktiga beslut kan få enorma konsekvenser (Ani et al., 2019). Zeadally et al. (2020) menar att det finns stor potential för AI men även stora potentiella risker, AI-baserade system har möjligheten att göra cybersäkerheten säkrare men det finns även potentiella risker att Cyberhot kan vara AI-baserade system som kan manipulera AI-algoritmen. Det finns även risker kring Input attacker menar Kuzlu et al. (2021) där AI-baserade system manipuleras och ger fel resultat och detta kan vara i form av både fysiskt och digitalt. Dessa risker kring manipulering av AI-systemen gör det svårt kring ansvarsfrågan när ett system gör fel (Kuzlu et al., 2021).

Sammanfattningsvis av denna analys så är det otydligt kring ansvarsfördelningen och det etiska dilemman när användning av AI-baserad cybersäkerhet då det finns brister kring transparens och de potentiella riskerna med partisk data och manipulering. Den utmaning som finns beskrivs kunna lösas genom att använda sig av både tekniska lösningar men med mänskliga faktoranalyser, tydliga ansvars ramverk och etiska riktlinjer.

7 Resultat

Detta kapitel baseras på det resultat som denna tematiska analys har tagit fram kring arbetets frågeställning hur den mänskliga faktorn påverkas av automatisering och teknologiberoende i AI-driven cybersäkerhet. Den tematiska analysen indikerar att den mänskliga faktorn påverkas av automatisering och teknologiberoende inom AI-baserad cybersäkerhet. Den mänskliga faktorn försvinner inte av automation i form av AI-baserade system och kommer fortsätta vara en central roll och risk för cybersäkerheten. Det har identifierats ett huvudresultat för varje huvudsakligt tema från analysen där presenteras det resulterande från varje huvudsakligt tema. Det presenteras även en sammanfattning av resultatet för att knyta ihop resultatet kring arbetets frågeställning *Hur den mänskliga faktorn påverkas av automatisering och teknologiberoende i AI-baserad cybersäkerhet*.

7.1 Bristande förståelse och kunskap ökar fortsatt risken

Det första resultatet bygger på analysens första huvudsakliga tema kring *bristande förståelse och kunskap*. Den tematiska analysens resultat visar att den mänskliga faktorn fortsatt är en central roll inom cybersäkerheten trots automatisering med AI-baserad cybersäkerhet. Den automatisering som är i dagens cybersäkerhet finns det fortfarande en mänsklig interaktion med systemen och där denna analys visar att förståelse och kunskap är den mest effektiva lösningen för att uppfylla en säker cybersäkerhet (Ramlo & Nicholas, 2021; Ani et al., 2019). Analysen visar att det finns mycket potential för användning av AI-baserade system inom cybersäkerheten men för att uppfylla den fulla potentialen så behövs det individer som har kunskap om systemen för att det ska fungera (James, 2024). Det finns flera indikationer på att AI-baserade lösningar inte enbart är tekniska lösningar och att det är viktigt att kunna hitta en balans mellan mänsklig interaktion och de tekniska lösningar som görs för att det ska fungera optimalt och att det ska finnas möjlighet att förlita sig på systemen (Momoh et al., 2023). Men analysen visar även ett resultat att just denna mänskliga interaktion som behövs utgör även att en bristande förståelse och kunskap skulle fortsatt öka risken för mänskliga misstag inom cybersäkerheten. Utbildning kring systemen och cybersäkerhet kommer fortsatt vara en central roll för att kunna uppfylla en säker cybersäkerhetsmiljö. Att använda sig av AI-baserade system inom cybersäkerheten tar inte bort människor från sina arbetsuppgifter utan istället ändrar arbetsuppgifterna (Hassan & El-Ashry, 2024). Det är därför viktigt att det finns en tillräcklig förståelse för hur dessa AI-system fungerar och det är både tekniskt och operationellt. En bristande förståelse och kunskap påverkar den mänskliga interaktionen negativt med systemet och det finns fler risker och sårbarheter som skulle kunna leda till säkerhetsincidenter som är kopplade till den mänskliga faktorn (James, 2024). Resultatet visar att ifall utbildning inte prioriteras hos individerna som arbetar med systemet så finns det risker att cybersäkerheten försvagas på grund av mänsklig osäkerhet och förvirring.

7.2 Teknologiberoende för AI-baserade system ger nya sårbarheter

Detta resultat bygger på analysens andra huvudsakliga tema kring *teknologiberoende och för hög tillit till AI-baserade system*. Det som analysen resulterar i visar kring hur den mänskliga faktorn påverkas negativt av teknologiberoende inom AI-baserad cybersäkerhet och att den mänskliga faktorn påverkas enormt av AI-baserad cybersäkerhet. Det finns flera delar som beskriver kring den potential AI-baserade system har för cybersäkerheten men även vilka stora risker och nya sårbarheter som skapas när individer och organisationer förlitar sig på systemen (Das & Sandhane, 2021). Analysen visar att det har alltid funnits en oro kring en ökad beroendeställning till teknik på samhällsnivå och speciellt nu med AI-baserade verktyg. Romanous och Ginger (2024) och Nobles (2018) beskriver även att det i dagsläget är svårt och kostsamt att göra en fullständig övergång till AI-baserade system utan mänsklig inblandning. När mänsklig inblandning är med finns det alltid risker kring den mänskliga faktorn och hur den påverkas av nya verktyg. Ett av de risker som analysen tar upp kring är att användning av AI-baserade system kan leda till en övertro av systemet trots att systemet inte är optimerat att arbeta själv (Romanous & Ginger, 2024). Analysen visar att en ökad användning av AI-system skapar ett teknologiberoende och där risken finns att människor får en övertro till systemet och litar blint på vad systemet gör och slutar ifrågasätta systemets beslut. Det finns därför risken att det kritiska tänkandet för individer kan minska och detta kan skapa en falsk trygghet och att det leder till att hot inte längre hanteras på rätt sätt ifall det finns luckor i AI-systemets träningsdata och att systemet gör fel beslut.

Resultatet visar även att det finns en oro kring att bli beroende av AI-baserade system kan leda till att den mänskliga expertisen inom området kan minska ifall individer förlitar sig för mycket på AI-system och att det leder till att mänskliga expertisen inte underhåller sin expertis inom området. Det som analysen visar är att den största risken för den mänskliga faktorn påverkan på teknologiberoende av AI-baserade system är att det skapar en övertro till systemen. Artiklarna betonar oron för en övertillit till dessa system då dessa system skapar även nya sårbarheter. Sårbarheter kring nya attacker som systemet inte är tränats för och att AI-baserade lösningar kan skapa nya risker som tidigare inte har varit känt (Romanous & Ginger, 2024). Det finns därför ett tydligt resultat att AI-baserade lösningar har en stor potential men att systemet ska enbart användas som ett verktyg för att kunna effektivisera en verksamhet men att individer ska aldrig vara beroende av att använda sig av systemet.

7.3 Automatisering leder till ett skiftat fokus mot övervakande och strategisk översikt men den mänskliga faktorn kvarstår

Detta resultat är byggt kring analysens tredje huvudsakliga tema *automatiseringens påverkan på mänsklig roll*. Ett tydligt resultat som syns i denna analys är att automatisering i form av AI-baserade verktyg inte tar bort den mänskliga faktorn utan att det snarare istället förskjuts. Automatiseringen med AI-baserade system är gjord för att kunna ta över repetitiva uppgifter inom cybersäkerheten men där det fortfarande i

dagsläget behövs en mänsklig interaktion i form av övervakning av systemet och se ifall besluten och handlingarna som systemet gör är korrekta. I dagsläget påverkas därför den mänskliga faktorn genom AI-baserad automation inom cybersäkerhet då systemen inte kan klara sig själva än och att det istället förändrar arbetsuppgifter för individer till ett mer övervakande arbete på själva systemet (Hassan & El-Ashry, 2024).

Det finns ett tydligt resultat från denna analys att utbildning kommer fortsatt vara en fortsatt central roll för att motverka risker och incidenter då den mänskliga interaktionen kommer fortsatt vara avgörande för att systemet ska fungera så optimalt som möjligt (Ani et al., 2019). Automatisering med AI-baserade system har en enorm potential för att kunna skapa en säkrare cybersäkerhet men för att uppfylla denna potential behövs den mänskliga interaktionen och den mänskliga faktorn kommer därför att kvarstå. Resultatet visar att automatiseringen kan hjälpa cybersäkerheten enormt men att det även kommer leda till ett skiftat fokus mot strategiska översikter och övervakande uppgifter för individer (Hassan & El-Ashry, 2024). Det är därför viktigt för att möjliggöra att AI-baserad automation i cybersäkerhet uppfyller sin potential genom att utbilda kring dessa förändrade arbetsuppgifter och skapa en förståelse för systemen. Den mänskliga faktorn kommer trots automatisering av AI-baserade system att vara en fortsatt faktor för att säkerhetsställa effektiva och säkra system.

7.4 Bristande transparens skapar otydlig ansvarsfördelning och etiska dilemman

Detta resultat bygger på analysens fjärde huvudsakliga tema *etiska dilemman och otydlig ansvarsfördelning med användning av AI-baserade system*. Det sista resultatet är att det finns en negativ påverkan på den mänskliga faktorn genom AI-baserade system då det finns en avsaknad av transparens och tydliga ansvarsfördelningar. Det finns flera AI-baserade system inom cybersäkerheten som fungerar som en "black box" där användaren inte får någon information kring hur beslut och handlingar har fattats, detta kan vara till exempel varför viss trafik kan anses som ett hot och viss trafik ej (Hassan & El-Ashry, 2024). Resultatet visar att detta kan leda till att människor känner en osäkerhet med användning av AI-baserade system då dom för det första blir osäkra på när det ska ingripa eller ej men även att systemet kan göra felbedömningar som leder till etiska problem ifall systemet blockerar trafik som är legitim (Zarei et al., 2023).

Det finns en tydlig problematik med ansvarsfördelningen med AI-baserade system och det är svårt att fastställa en ansvarig och det krävs tydliga riktlinjer och ramverk för att kunna besluta dessa ansvar när AI-systemen tar beslut (Hassan & El-Ashry, 2024). Det framgår även att det finns risker att dessa AI-baserade system kan vara potentiella risker genom att systemet kan manipuleras och det gör ännu svårare att kunna fastställa ansvarsfördelningen ifall systemen har blivit manipulerade till att göra fel beslut (Ani et al., 2019). Resultatet visar att det är en stor utmaning just nu att skapa en lösning med denna problematik och att det kommer behövas tekniska lösningar men med mänskliga faktoranalyser, tydliga ansvars ramverk och etiska riktlinjer för att kunna uppnå en

framtida lösning. Resultatet visar därför att det finns potential för användning av AI-baserade system inom cybersäkerheten men att i dagsläget så finns det flera negativa påverkningar på den mänskliga faktorn men implementering av dessa system som skapar otydliga ansvarsfördelningar, etiska dilemman och bristande transparens.

7.5 Sammanfattning av resultat

Resultatet visar att den mänskliga faktorn påverkas på flera olika sätt av både automatisering och teknologiberoende inom AI-baserad cybersäkerhet. Arbetet har fått resultat av fyra effekter som tillsammans besvarar arbetets frågeställning där resultatet med hjälp av en tematisk analys av 25 olika vetenskapliga artiklar. Den första effekt som arbetet resulterar i är att bristande förståelse och kunskap om AI-system och cybersäkerhet kommer fortsatt vara en central roll som skapar osäkerheter och risker för mänskliga misstag.

Den mänskliga faktorn påverkas fortfarande negativt om användaren inte förstår hur systemet fungerar och risken finns att användaren använder systemet antingen på fel sätt eller agerar passivt. Den andra effekten så visar det ett resultat kring hur teknologiberoende och för hög tillit till AI-baserade system påverkar den mänskliga faktorn. Resultatet visar att en för hög tillit till AI-system kan minska det kritiska tänkandet för användaren och att användaren slutar ifrågasätta systemets beslut som skapar ett teknologiberoende men ökar risken ifall beslutet systemet gör är bristfälligt eller felaktigt. Den tredje effekten visar ett resultat kring hur automatisering leder till ett skiftat fokus mot övervakande och strategisk översikt men den mänskliga faktorn kvarstår.

Resultatet visar att den mänskliga faktorn inte försvinner med hjälp av AI-baserad automatisering utan att den istället förskjuts till nya arbetsuppgifter för användaren. Den mänskliga inblandningen minskar men försvinner inte helt och risker för mänskliga misstag kan istället för användaren hamna på att missa ifall AI-baserade systemen gör misstag eller felaktiga beslut i övervaknings processen. Den fjärde effekten visar ett resultat kring den bristande transparens, otydliga ansvarsfördelningar och etiska dilemman som är kortfattat sagt en svår fråga att få ett konkret resultat från. Det som däremot syns tydligt av detta resultat är att AI-baserade system har en negativ påverkan på den mänskliga faktorn då det finns en avsaknad av transparens i systemet och tydliga ansvarsfördelningar. Den bristande transparensen i sig leder till etiska dilemman där användarna inte vet vem som bär ansvaret när fel inträffar som leder till att användaren blir passiv och inte agerar när deras ingripande skulle kunna vara avgörande.

Det sammanfattande resultatet visar att den mänskliga faktorn inte försvinner av AI-baserad cybersäkerhet i när AI-baserade system leder till automatisering och ett högre teknologiberoende den mänskliga faktorn istället förändras. AI-baserad cybersäkerhet har potentialen att kunna förstärka säkerheten men enbart ifall människan har en förståelse, möjlighet att agera och ett ansvar. Detta arbete har visat ett resultat på att den mänskliga faktorn kan påverkas genom minskad kunskap, en övertillit

till teknik och ett högre teknologiberoende, etisk osäkerhet och ett förskjutet ansvar som tillsammans kan riskera att skapa nya sårbarheter inom cybersäkerheten.

8 Diskussion

Detta kapitel kommer gå igenom och diskutera det olika fynd som detta arbete har gjort men även diskutera kring de olika aspekterna och eventuella framtida arbeten inom området.

8.1 Metod

Detta arbete har varit baserat på en systematisk litteraturstudie med tematisk analys. Den valda metoden har lämpat sig väl för att kunna identifiera olika mönster hur den mänskliga faktorn påverkas av automatisering och teknologiberoende i AI-baserad cybersäkerhet. Att använda sig av och följa Prisma-modellen med olika valda sökord kunde med en inkludering och exkluderingsprocess hitta 25 vetenskapliga artiklar som detta arbetets analys inkluderat. En fördel med att använda den valda metoden var att kunna få fram en bred översikt av dagslägets aktuella kunskapsläge. Det finns däremot vissa begränsningar då arbetet inte har varit baserat på någon primärdata som har samlats in utan enbart ett resultat från tolkning av tidigare forskning. Ytterligare en svaghet i detta arbete är att arbetet är gjort av en person som kan tack vare den mänskliga faktorn påverka tolkningen av materialet trots att arbetet har försökt vara transparent.

En fördel med den valda metoden är att med det olika valda sökorden kunde även en forskningslucka identifieras kring just arbetets frågeställning. Det kunde identifieras att mycket av den tidigare forskningen inte inkluderade de tre olika teman kring mänskliga faktorn, AI och cybersäkerhet utan att majoriteten inkluderade två av tre teman. Det var anledningen till varför den tematiska grupperingen gjordes för att kunna särskilja de olika artiklarna. Det gjorde även analysen svår då mycket av de artiklar som enbart handlade om Mänskliga faktorn och AI hade en mer lutad negativ inställning till AI medan artiklar som enbart var AI och cybersäkerhet hade en väldigt positiv inställning till AI. Det gjorde dock arbetet med denna metod mer intressant då det skapade möjligheten att kunna läsa från två olika perspektiv för att kunna hitta och analysera huvudsakliga teman som berör arbetets frågeställning.

Arbetet var först planerat att använda sig av semistrukturerade intervjuer men där det blev ändring då inga av de kontaktade företagen ville diskutera potentiella sårbarheter och nackdelar med AI-baserade system inom cybersäkerhet trots anonymitet. Det finns därför potentiellt en forskningslucka eller forskning om AI-baserad cybersäkerhet som inte säger hela sanningen med tanke på att företag ännu inte vill diskutera detta område.

Det finns såklart fördelar och nackdelar med alla typer av metoder men att trots detta har metoden systematisk litteraturstudie givit ett trovärdigt resultat då flera av detta arbetets tema återkom i studier som var oberoende från olika typer av forskningsfält.

8.1.1 Vetenskaplig etik

Detta arbete har kring den vetenskapliga etiken försäkrats genom att följa de principer som är etablerade för en systematisk litteraturstudie. Urvalet av artiklar har gjorts genom att följa Prisma modellens riktlinjer som innebär att urval, identifiering, inkludering och granskning av artiklar är dokumenterade och har redovisats transparent. Arbetet har även använt förbestämd inkludering och exkluderingskriterier som funnits i förväg och har implementerats metodiskt under arbetets urvalsprocess. Exempel på dessa inkluderingskriterier är att artiklarna måste vara från senast 2018 för att säkerställa att artikeln är aktuell och att artikeln har ett fokusområde på minst två av de tre teman: mänskliga faktorn, AI och cybersäkerhet. Exempel kring exkluderingskriterier är att artikeln enbart granskar de tekniska aspekterna av AI-baserad cybersäkerhet utan koppling till risker för den mänskliga faktorn. Dessa kriterier minskar därför risken att urvalet av artiklar skulle sakna trovärdighet och partiska bedömningar.

Arbetets analys har även gjorts genom en tematisk analys som är en systematisk och erkänd metod för att analysera vetenskapliga artiklar. Kodningen, tematiseringen och syntes är dokumenterad i arbetet för transparensen och möjlighet för replikerbarhet. Arbetet har även följt APA som källhänvisning där samtliga referenser som refereras i detta arbete kring påståenden, forskningsresultaten och definitioner har hänvisat till texten för att visa resultat från de tidigare forskares arbeten. Arbetet har därför på detta sätt uppnått de krav på vetenskapliga etiken kring transparens, objektivitet och källhänvisning.

8.2 Resultat

Att det skulle finnas någon påverkan på den mänskliga faktorn inom cybersäkerhet med användning av AI-baserad cybersäkerhet var ingenting som egentligen förvånade. Det däremot som förvånade var kring hur lite forskning det faktiskt fanns i dagsläget som inriktar sig just på frågan med den mänskliga faktorn och användning av AI med tanke på hur snabbt utveckling sker inom användning av AI. Resultatet visade att den mänskliga faktorn inte försvinner med ökad automatisering och teknologiberoende med användning av AI-baserade system utan att den istället förändras och blir en mer komplex fråga (Ani et al., 2019). Resultatet indikerar även på att AI-system har en stor potential för framtida cybersäkerhet men samtidigt även kring hur det kommer att finnas höga krav på den mänskliga förståelsen för systemet (Ramlo & Nicholas, 2021). Det som visades speciellt var att en övertillit till teknik och bristande förståelse skapar sårbarheter i cybersäkerheten (Ramlo & Nicholas, 2021). Det kan därför dras slutsatser om att resultatet visar att företag och organisationer inte kan skapa ett för stort beroende och förlita sig på tekniska lösningar för mycket även när det gäller AI-system (Das & Sandhane, 2021). Det kommer fortfarande finnas ett stort behov av att utbilda personal och öka personalens medvetenhet samtidigt som det kommer behövas en tydlig ansvarsfördelning. Det som resultaten har visat kan egentligen ses som ett mönster från tidigare utveckling inom IT, utvecklingen går snabbt och företag vill vara

med i utvecklingen trots att sårbarheter, lagar och regler inte hunnit med i denna takt som i sig kan också skapa sårbarheter. Arbetet har resulterat i att det finns många luckor inom ämnet som behöver fyllas ut innan en full potential av AI kan användas inom cybersäkerhet och att företag och organisationer kan få utmaningar med implementering och användning av AI-baserade system.

8.3 Samhälleliga aspekter

Med tanke på hur digitaliseringen utvecklas i samhället och teknologiberoende ökar så är inte längre cybersäkerhet enbart en fråga för människor med expertis och cybersäkerheten har blivit mer av en samhällsfråga. Resultatet har indikerat på att det påverkar människor i alla olika roller från beslutsfattare, vårdpersonal men även vanliga privatpersoner om hur användning av AI-baserade system kommer att användas och utvecklas. Ifall AI-baserade system rent generellt skulle fortsätta att utvecklas utan att det finns mänskligt ansvar och att förståelsen för system inte hänger med riskerar det att leda till att ingen känner sig kapabel till att ingripa vid tekniska fel som absolut skulle påverka på en samhällsnivå. Arbetet indikerar därför vikten av att AI-baserade system behöver utvecklas med den mänskliga förståelsen och kunskapen i åtanke och detta är både kring design, regler och utbildningar. För att AI-baserade system ska fungera på en samhällsnivå så kommer det att behövas en transparens, tydliga ramverk och en tillgång till en relevant kompetens för att kunna bibehålla den tillit som finns på samhällsnivå inom digitala miljöer. Användning av denna forskning skulle kunna användas för att öppna upp frågan kring riskerna, sårbarheterna och de otydligheter som just nu finns inom ämnet AI-baserad cybersäkerhet, särskilt inom mer samhällsbärande funktioner som till exempel sjukvården.

8.4 Etiska aspekter

Det är en väldigt komplex och svår fråga kring etiken inom AI-baserade system i cybersäkerheten, dels på grund av den bristande transparens men även att det leder till ökad autonomi. En bristande transparens och ökad autonomi ger väldigt otydliga ansvarsförhållande som även påverkar användaren kring att vilja agera i kritiska incidenter. Ett AI-baserat system är extremt effektivt och snabbt och kan därför uppfattas som att det är ofelbart och bara ger ett korrekt beslut eller svar. Det som detta arbete har fått genom sin analys är att de inkluderande vetenskapliga artiklarna även nämner AI som en "black box" för sin bristande transparens. Ett effektivt system fast med en bristande transparens visar det inkluderande artiklarna att det kan leda till svårare att få informerade beslut men även att användare inte tar ansvar i ren osäkerhet. Denna problematik kan därför leda till att det blir en etisk gråzon där ingen riktigt vet om användaren ska agera eller ej. Det behövs därför en högre förståelse kring systemet men även vilka konsekvenser systemet kan leda till ifall det blir fel. Den etiska delen behöver därför lösas och inte bara för att systemet ska fungera rent tekniskt men även för att användarna ska kunna förstå och kunna ifrågasätta systemet.

8.5 Metodologiska begränsningar

Det finns flera metodologiska begränsningar att ha i åtanke när arbetets metod är en systematisk litteraturstudie. En av dessa begränsningar är risken för partiskhet, trots att en systematisk litteraturstudie är utformad för att minimera risken för partiskhet så finns det fortfarande risker för olika typer av partiskhet som selektions partiskhet och dataextraktion partiskhet (Nightingale, 2009).

En systematisk litteraturstudie så finns det heller ingen enighet hur på bästa sätt kvalitetsbedömningen ska utföras där det menas att studierna måste nå en viss metodologisk kvalitet, men där det även finns en vinkel om risk att exkludera för många studier som kan leda till en selektion partiskhet(Nightingale, 2009).

8.6 Framtida arbeten

Framtida arbeten behöver fokusera mer på den mänskliga faktorn när det gäller AI-baserad cybersäkerhet. Det borde komplettera arbetet med intervjuer och observationer för att kunna få en bättre förståelse kring den problematik som faktiskt finns och vilka risker och sårbarheter den kan leda till. Det är viktigt att kunna få en bättre syn på denna problematik rent praktiskt men även kunna få en inblick i hur användarna uppfattar dessa AI-baserade lösningar inom cybersäkerheten. Det kommer även att behövas få fram ett resultat kring vilka utbildningsformer som är mest effektiva för att användare ska öka sin förståelse och kunskap inom området och hur AI kan utvecklas för att kunna lösa problematiken med den bristande transparens och de etiska ansvarerna. Det behövs även en utveckling kring tydliga ramverk när det gäller användning av AI-baserade system för att kunna fastställa en tydligare ansvarsfördelning.

Referenser

- Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, 121, 1189-1211.
- Abzakh, A., & Althunibat, A. (2023, August). A Review: Human Factor and Cybersecurity. In *2023 International Conference on Information Technology (ICIT)* (pp. 589-592). IEEE.
- Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, 21(1), 2-35.
- Anayat, R. (2024). Cybersecurity Automation with AI: Reducing Human Error and Improving Incident Response.
- Bleher, H., & Braun, M. (2022). Diffused responsibility: attributions of responsibility in the use of AI-driven clinical decision support systems. *AI and Ethics*, 2(4), 747-761.
- Bouramdane, A.-A. (2023). Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*, 3(4), 662-705. <https://doi-org.libraryproxy.his.se/10.3390/jcp3040031>
- Cunningham, M., Nobles, C., Robinson, N., & Haney, J. (2024). Leveraging the Human Factors Discipline for Better Cybersecurity Outcomes: A Roundtable Discussion. *IEEE Security & Privacy*, 22(6), 99-104
- Das, R., & Sandhane, R. (2021, July). Artificial intelligence in cyber security. In *Journal of Physics: Conference Series* (Vol. 1964, No. 4, p. 042072). IOP Publishing.
- Du-Harpur, X., Watt, F. M., Luscombe, N. M., & Lynch, M. D. (2020). What is AI? Applications of artificial intelligence to dermatology. *British Journal of Dermatology*, 183(3), 423-430.
- Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of management annals*, 14(2), 627-660.
- Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: A review. *Applied Artificial Intelligence*, 36(1), 2037254.
- Hassan, E. A., & El-Ashry, A. M. (2024). Leading with AI in critical care nursing: challenges, opportunities, and the human factor. *BMC nursing*, 23(1), 752.

- Humphreys, D., Koay, A., Desmond, D., & Mealy, E. (2024). AI hype as a cyber security risk: The moral responsibility of implementing generative AI in business. *AI and Ethics*, 4(3), 791-804.
- Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7(3).
- Irizar-Arrieta, A., Gómez-Carmona, O., Bilbao-Jayo, A., Casado-Mansilla, D., López-De-Ipiña, D., & Almeida, A. (2020). Addressing behavioural technologies through the human factor: A review. *IEEE Access*, 8, 52306-52322.
- James, C. (2024, June). AI to minimize human error in cybersecurity: Enhancing threat detection and incident response accuracy [Manuskript]. ResearchGate.
https://www.researchgate.net/publication/385747239_AI_to_Minimize_Human_Error_in_Cybersecurity_Enhancing_Threat_Detection_and_Incident_Response_Accuracy
[hämtad 04 april 2025]
- Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019, December). Towards an improved understanding of human factors in cybersecurity. In 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC) (pp. 338-345). IEEE.
- Kaur, R., Gabrijelčić, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804
- Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things*, 1(1), 7.
- Minh, D., Wang, H. X., Li, Y. F., & Nguyen, T. N. (2022). Explainable artificial intelligence: a comprehensive review. *Artificial Intelligence Review*, 1-66.
- Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors*, 22(2), 538.
- Momoh, I., Adelaja, G., & Ejiwumi, G. (2023). Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution. IEEE: Piscataway, NJ, USA.
- Nallapareddy, V. S. S. R., & Katta, S. K. R. (2025, February). AI-Enhanced Cyber Security Proactive Threat Detection and Response Systems. In 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL) (pp. 1510-1514). IEEE..
- Nightingale, A. (2009). A guide to systematic literature reviews. *Surgery (Oxford)*, 27(9), 381-384.
- Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, 9 (3), 71–88.

- Nobles, C. (2019). Establishing human factors programs to mitigate blind spots in cybersecurity. *MWAIS 2019 Proceedings*, 22, 12.
- Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *Holistica Journal of Business and Public Administration*, 13(1), 49-72.
- Oscarson, P. (2019). *Informationssäkerhet*. Lund: Studentlitteratur.
- Pawlicka, A., Pawlicki, M., Kozik, R., & Choraś, M. (2022). Human-driven and human-centred cybersecurity: policy-making implications. *Transforming Government: People, Process and Policy*, 16(4), 478-487.
- Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, 24(2), 371-390.
- Ramlo, S., & Nicholas, J. B. (2021). The human factor: Assessing individuals' perceptions related to cybersecurity. *Information & Computer Security*, 29(2), 350-364.
- Rohan, R., Funilkul, S., Pal, D., & Chutimaskul, W. (2021, December). Understanding of human factors in cybersecurity: A systematic literature review. In *2021 International Conference on Computational Performance Evaluation (ComPE)* (pp. 133-140). IEEE.
- Romanous, E., & Ginger, J. (2024, August). AI Efficiency in Cybersecurity: Estimating Token Consumption for Optimal Operations. In *2024 21st Annual International Conference on Privacy, Security and Trust (PST)* (pp. 1-5). IEEE.
- Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data*, 11(1). <https://doi-org.libraryproxy.his.se/10.1186/s40537-024-00957-y>
- Santa Barletta, V., Calvano, M., Caruso, F., Curci, A., & Piccinno, A. (2023, October). Serious games for cybersecurity: how to improve perception and human factors. In *2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRINE)* (pp. 1110-1115). IEEE.
- Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, 2(3). <https://doi-org.libraryproxy.his.se/10.1007/s42979-021-00557-0>
- Timmers, P. (2019). Ethics of AI and cybersecurity when sovereignty is at stake. *Minds and Machines: Journal for Artificial Intelligence, Philosophy and Cognitive Science*, 29(4), 635-645. <https://doi-org.libraryproxy.his.se/10.1007/s11023-019-09508-4>
- Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, 2(3), 573-586.

Vetenskapsrådet (2024). God forskningssed Tillgänglig:
<https://www.vr.se/analys/rapporter/vara-rapporter/2024-10-02-god-forskningssed-2024.html> [Hämtad 03 mars 2025]

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: a systematic mapping of literature. *Ieee Access*, 8, 146598-146612.

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of planning education and research*, 39(1), 93-112.

Zarei, E., Khan, F., & Abbassi, R. (2023). How to account artificial intelligence in human factor analysis of complex systems?. *Process safety and environmental protection*, 171, 736-750.

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access*, 8, 23817-23837.

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. *Journal of Industrial Information Integration*, 23, 100224.