CYBERSIKKERHED

Et scoping-review af humanistisk forskning i cybersikkerhed

Karina Dollerup

SHAPE
SHAPING
DIGITAL
CITIZENSHIP

Arbejdspapir| Februar 2025 | Karina Dollerup | Aarhus Universitet
www.shape.au.dk

Indholdsfortegnelse

Indledning

Cyberangreb udnytter ofte såkaldte *human factors* såsom menneskers tillid til falsk information, manglende uddannelse eller stort pres i beslutningssituationer. Således spiller adfærdsmæssige, organisatoriske og kulturelle udfordringer en væsentlig rolle for cybersikkerhed, hvilket medfører, at humanistiske forskningsperspektiver er nødvendige for forståelse og udvikling.

I det følgende fremlægges resultaterne af et scoping-review, som netop har undersøgt, hvordan humanistiske temaer er inddraget i forskning om cybersikkerhed. Reviewet viser, at følgende temaer står centralt i den undersøgte litteratur: *Human factors, organisatorisk sikkerhedskultur, uddannelse og træning, politik og samfund, etik samt design og maskinlæring*. I det følgende uddybes disse temaer, og der gives en række eksempler på, hvordan de indgår i forskningen.

Det skal bemærkes, at reviewet er eksplorativt og ikke udtømmende. I tråd med formålet for et scoping-review har formålet været at få et brugbart indblik i den eksisterende forskning og på den måde hente inspiration til en videreudvikling af humanistisk forskning i cybersikkerhed. Som det vil fremgå, er der således ikke bare plads til, men ligefrem brug for yderligere humanistisk forskning, hvis dette vigtige felt skal belyses og håndteres i praksis.

Metode

Et scoping-review muliggør kortlægning af væsentlige temaer og tendenser i et komplekst og dynamisk felt præget af interdisciplinære perspektiver (Arksey og O'Malleys 2005). Dette review tager udgangspunkt i spørgsmålet: *"Hvordan bidrager humaniora til forskning i cybersikkerhed?"* Fokus har især været lagt på et informationsvidenskabeligt perspektiv, hvor relationerne mellem det tekniske og det sociale står centralt. Reviewet blev udført i tre faser

- Fase 1: Valg af databaser og udvikling af søgestrategi
- Fase 2: Screening af artikler
- Fase 3: Kodning og kategorisering af udvalgte studier

Fase 1: Søgestrategi og valg af databaser

Litteratursøgningen blev udført i tre databaser: JSTOR, der dækker bredt inden for humanistiske områder, Science Direct, som er en tværfaglig database, og Sage Journals, da indledende søgninger viste, at der her fandtes relevante artikler. Den første søgning krævede, at termen

"cybersecurity" var indeholdt i titel, abstract, keywords eller brødtekst. Derudover skulle mindst ét af følgende søgeudtryk forekomme i keywords eller abstract: *Humanities, academic programs, ethics, Science Technology and Society Studies, STS eller critical theory*.

Den første søgning resulterede i 558 artikler. For at afgrænse resultaterne yderligere blev der stillet krav om, at artiklerne skulle være udgivet mellem 2020 og 2024 og være skrevet på engelsk, hvilket reducerede antallet til 392 artikler.

Fase 2: Screening

Herefter blev materialet manuelt screenet for at vurdere artiklernes relevans i forhold til undersøgelsesspørgsmålet. Hertil blev softwareprogrammet Covidence anvendt til at organisere og forenkle processen. 19 artikler blev automatisk identificeret som duplikater og fjernet. Dette medførte, at der var 373 artikler tilbage til den første screeningsrunde.

Første screeningsrunde

I den første screeningsrunde blev artikler, der inddrager både et cybersikkerhedsrelateret emne og et humanistisk perspektiv, identificeret. Udvælgelsen skete manuelt og blev baseret på, om "information security" eller "cybersecurity" blev nævnt i artiklernes titel, keywords eller abstract, samt om der var inkluderet humanistiske vinkler på cybersikkerhed. Som resultat af denne proces blev 288 artikler udelukket, og 85 artikler gik videre til den anden screeningsrunde.

Anden screeningsrunde

De resterende 85 artikler blev manuelt vurderet med henblik på at afgøre afgøre, hvilke der skulle fungere som primære kilder, og hvilke der kunne anvendes som støtteartikler:

- **Høj relevans:** Artikler, der har en stærk og direkte kobling mellem humaniora og cybersikkerhed, og som væsentligt bidrager til belysning af undersøgelsesspørgsmålet. Det inkluderer artikler, der introducerer nye perspektiver, metoder eller teorier.
- **Middel relevans:** Artikler, der refererer til både cybersikkerhed og humanistiske emner, men det sker sporadisk uden en uddybende forklaring på koblingen mellem de to områder. Artiklerne kan præsentere relevante temaer eller koncepter, men de bidrager ikke direkte til belysningen af undersøgelsesspørgsmålet.

- **Lav relevans:** Artikler, der omhandler enten humaniora eller cybersikkerhed uden at skabe en kobling mellem de to områder. Disse artikler bidrager ikke væsentligt til belysning af undersøgelsesspørgsmålet.

På baggrund af denne vurdering blev 44 artikler kategoriseret som lav, 24 som middel og 17 som høj relevans. Artiklerne med lav relevans blev sorteret fra, mens de øvrige indgår i reviewet. Det er dog de 17 artikler med høj relevans, der fungerer som de primære kilder.

Fase 3: Kodningsproces og kategorisering af artikler

De 17 højrelevante artikler blev systematisk kodet med i alt 361 koder, som blev organiseret i 24 kategorier. Disse kategorier blev derefter reduceret til seks, som repræsenterer de centrale temaer i artiklerne.

Temaer

Nedenfor præsenteres de seks centrale temaer identificeret i artiklerne:

- **Human factors:** Omhandler de menneskelige aspekter af cybersikkerhed, såsom adfærd, fejl, beslutningstagning og psykologiske faktorer, der påvirker sikkerhedspraksis
- **Organisatorisk sikkerhedskultur***:* Undersøger, hvordan organisationers sikkerhedskultur påvirker implementeringen af cybersikkerhedsforanstaltninger og risikohåndtering
- **Uddannelse og træning***:* Fremhæver betydningen af cybersikkerhedstræning og -uddannelse som redskaber til at forbedre sikkerheden på både individuelt og organisatorisk niveau
- **Samfund og politik:** Beskriver den politiske og samfundsmæssige kontekst for cybersikkerhed, herunder politisk indflydelse og informationskampagner på sociale medier
- **Etik:** Diskuterer etiske dilemmaer i cybersikkerhedsforskning og beslutningsprocesser inden for cybersikkerhed ud fra et menneskeligt perspektiv
- **Design og maskinlæring**: Undersøger, hvordan teknologier som fx *eye-tracking* kan bruges i undersøgelser af brugergrænseflader, og hvordan maskinlæring kan anvendes til at forbedre cybersikkerhed

Tema 1: Human factors

I artiklerne udtrykkes den humanistiske forskningsinteresse ofte gennem begrebet *human factors.* Begrebet beskriver, hvordan menneskers psykologiske og fysiske egenskaber påvirker deres interaktion med teknologiske systemer. I forskningen om cybersikkerhed bruges *human factor* således bredt om menneskelig adfærd (Mersinas et al., 2025; Das et al., 2020; Nobles & Robinson, 2024), hensynet til diversitet blandt brugere (Das et al., 2020), adfærdsændringer (Mersinas et al., 2025) og betydningen af *security hygiene,* som i nogle sammenhænge også betegnes som cyber-hygiejne (Edwards et al., 2023). I det følgende uddybes nogle af artiklernes centrale aspekter.

Nobles og Robinson (2024, p.1) fremhæver, at forståelsen af menneskelig adfærd, beslutningstagning, fejl og begrænsninger er afgørende for at kunne identificere og reducere sårbarheder. I tråd hermed refereres til Verizon's Data Breach Investigative Report (2023), som viser, at 74 % af sikkerhedsbrud skyldes menneskelige handlinger (Nobles & Robinson, 2024, p.1). Dette understreger, ifølge forfatterne, hvor vigtigt det er at integrere *Human Factors Engineering* (HFE) i cybersikkerhedsstrategier for at reducere organisatorisk risiko (Nobles & Robinson, 2024, p. 1) I forlængelse heraf beskrives HFE som en disciplin, der fokuserer på at anvende principper fra kognitiv psykologi og ergonomi til at designe systemer, der reducerer fejl og forbedrer menneskers interaktion med teknologi. HFE fremmer en tilgang til cybersikkerhed, hvor menneskers behov og begrænsninger bliver en central del af løsningen (Nobles & Robinson, 2024, p. 2).

Med den stigende brug af digitale teknologier bliver det stadig vigtigere at beskytte brugernes data mod digitale trusler. Et tema inden for *human factors*, som går igen i flere af artiklerne, er, at cybersikkerhedsforanstaltninger skal være anvendelige for alle brugere, uanset deres teknologiske kyndighed (Das et al., 2020, p. 361). Dette tema blev bl.a. diskuteret under en paneldebat, hvor forskere fra forskellige discipliner fremhævede behovet for at udvikle inkluderende designløsninger inden for cybersikkerhed (Das 2020).

Deltagerne understregede, at sikkerhedsproblemer hænger tæt sammen med menneskers behov, mål, overbevisninger og interaktioner med teknologi (Das et al., 2020, p. 361). Det blev ligeledes pointeret, at selv teknologikyndige personer kan have vanskeligheder med at skelne mellem grundlæggende sikkerhedsbegreber (Das et al., 2020, p. 362). I debatten blev det også påpeget, at eksisterende privatlivsmekanismer ofte er udviklet uden hensyntagen til diversiteten i brugerpopulationer, og det nævnes, at fx neurodivergente og ældre personer kan opleve særlige udfordringer (Das et al., 2020, p. 363).

Hvor ovenstående omhandler diversitet og tilgængelighed, har Mersinas, Bada og Furnell (2025) fokus på, hvordan adfærdsændringer og etiske principper kan integreres for at reducere menneskelige fejl og styrke sikkerheden. De peger på, at mange sikkerhedsbrud skyldes menneskelige fejl, ofte forårsaget af tidsmangel eller mangelfulde oplysninger. Derfor introducerer forskerne begrebet *Cybersecurity Behavior Change* (CBC), som dækker over ændringer i individers adfærd relateret til cybersikkerhed (Mersinas et al., 2025, p. 1).

Et centralt aspekt af CBC er *security hygiene* (cyberhygiejne), der defineres som: "a synonym for secure and/or preferable behaviors, on the criterion that they reduce the contextual attack surface" (Mersinas et al., 2025, p. 1). Dette inkluderer god praksis som håndtering af *phishing-mails*, brug af stærke adgangskoder og korrekt anvendelse af privatlivsindstillinger. God *security hygiene* kan fremmes gennem træning og uddannelse.

Undertema 1: Phishing

Såkaldte phishing-angreb fylder en del i artiklerne om *human factors*. Phishing består i, at angribere målrettet anvender manipulerende metoder til at skaffe følsomme oplysninger (Klimburg-Witjes & Wentland, 2021; Edwards et al., 2023). I den forbindelse nævnes også *social engineering* (Klimburg-Witjes & Wentland, 2021), *SMiShing* (Edwards et al., 2023), *spear-phishing* (Datta & Acton, 2023; Klimburg-Witjes & Wentland, 2021), og *disinformation attacks* (Datta & Acton, 2023).

Nina Klimburg-Witjes og Alexander Wentland (2021) undersøger, hvordan medarbejdere, der bliver udsat for *social engineering*-angreb, omtales (2021, p. 1319). Forskerne viser, at medarbejdere ofte beskrives som *the deficient users*, hvilket refererer til personer uden tilstrækkelig teknologisk viden og evner til at beskytte sig mod digitale trusler (Klimburg-Witjes & Wentland, 2021, p. 1319). Ifølge forskerne lægges ansvaret for cybersikkerhed dermed ofte over på den individuelle medarbejder fremfor organisationen: "The individual is simultaneously called upon as being responsible for processes of collective security as well as a potential liability and even a threat to it" (Klimburg-Witjes & Wentland, 2021, p. 1323).

Denne problematik forstærkes af, at cybersikkerhedsfagfolk ofte fremhæver teknisk viden som en nødvendighed for at håndtere sikkerhed og derfor ser medarbejdere med manglende kompetencer som den primære årsag til mange sikkerhedsproblemer i organisationer (Klimburg-Witjes & Wentland, 2021, p. 1326). Klimburg-Witjes & Wentland advarer om, at et sådant ensidigt fokus på menneskelige fejl risikerer at aflede opmærksomheden fra de organisatoriske og

strukturelle aspekter af cybersikkerhed. Som forskerne påpeger, bliver spørgsmål om, hvorfor nye sårbarheder opstår, og hvordan de kan løses kollektivt, ofte fortrængt i denne diskurs (Klimburg-Witjes & Wentland, 2021, p. 1332).

Forskerne opfordrer derfor til en kulturudvikling, hvor tilliden mellem ledelse, IT-afdelinger og medarbejdere styrkes, samtidig med at organisationerne anerkender de uundgåelige sårbarheder, der eksisterer i sociotekniske systemer. Deres forslag indebærer således, at diskursen om *social engineering* udvides til at inkludere både organisatoriske og samfundsmæssige aspekter frem for kun at fokusere på menneskelige fejl (Klimburg-Witjes & Wentland, 2021, p. 1317).

Klimburg-Witjes & Wentland (2021) mener ikke, at medarbejdere bør ses som passive modtagere af træning eller som *deficient users*, men snarere som mennesker, der kan styrkes og inddrages aktivt i udviklingen af en mere modstandsdygtig og inkluderende sikkerhedskultur. Dette er særligt vigtigt i forhold til at håndtere angrebsmetoder som *phishing* og *SMiShing,* der udnytter sårbarheder til at kompromittere organisationers sikkerhed. Hvor angriberen i *phishing* benytter falske e-mails, der udgiver sig for at være fra en legitim afsender, benytter *SMiShing*, SMS-beskeder til at nå modtagerne.

Edwards, Morris og kollegaer (2024) undersøger deltagernes bevidsthed om *SMiShing*-angreb, herunder de adfærdsmønstre og sårbarheder, der gør mennesker særligt udsatte for denne type cyberangreb (Edwards et al., 2024, p. 1911). Resultaterne peger på, at selvom mange er bevidste om farerne ved at åbne links fra ukendte afsendere, vælger de alligevel ofte at klikke på dem (Edwards et al., 2024, p. 1913).Forskerne konkluderer derfor, at *human factors* spiller en afgørende rolle i cybersikkerhed, særligt i relation til *SMiShing* (Edwards et al., 2024 p. 1915). De fremhæver i forlængelse heraf betydningen af at inddrage uddannelsesinstitutionerne i arbejdet med at identificere og belyse de sårbarheder, der gør mennesker modtagelige over for denne form for angreb. Samtidig understreger de behovet for at udvikle indsatser, der kan fremme adfærdsændringer og styrke menneskers modstandsdygtighed over for *SMiShing.*

Tema 2: Organisatorisk sikkerhedskultur

Organisatorisk sikkerhedskultur er et andet væsentligt tema i den gennemgåede litteratur. Hertil hører en interesse for medarbejdernes rolle og udviklingen af strategier, der kan styrke modstandsdygtighed gennem tværfagligt samarbejde og kulturelle tilpasninger (Trumbach et al., 2023; Fatima et al., 2024; Datta & Acton, 2023).

Et eksempel er Trumbach, Payne og Walsh (2023), der belyser cybersikkerhedens komplekse udfordringer i relation til organisationskultur. Forskerne argumenterer i den forbindelse for, at en interdisciplinær tilgang, der kombinerer flere fagområder og metoder, kan bidrage til at styrke både teknologiske løsninger og organisatoriske strategier (Trumbach et al., 2023, p. 38). Forskerne peger desuden på, at videregående uddannelsesinstitutioner bør uddanne studerende med dybdegående indsigt i kultur, strategi og ledelse, så cybersikkerhed kan integreres i bredere organisatoriske sammenhænge (Trumbach et al., 2023, p. 38).

Forskerne understreger, at både ledelse og medarbejdere skal have en grundlæggende forståelse for truslernes omfang og besidde de nødvendige værktøjer til effektivt at håndtere dem. Træning og kontinuerlig vidensdeling er nødvendig for at kunne identificere og reagere på potentielle trusler. En strategisk indsats, der integrerer cybersikkerhed i organisationens overordnede målsætninger, er afgørende for at opnå dette (Trumbach et al., 2023, p. 38).

Desuden kan HR-afdelinger spille en central rolle ved at sikre, at nye medarbejdere modtager nødvendig træning og dermed bidrager til at styrke organisationens modstandsdygtighed. Trumbach og kolleger peger også på behovet for risikovurderinger, beredskabsplaner og en samlet cybersikkerhedsstrategi for at minimere risici og håndtere trusler (Trumbach et al., 2023, p. 38). Dette kræver, at risikostyring bliver en del af organisationens strategiske planlægning og forretningskontinuitet, da cybersikkerhed ikke kun er et IT-anliggende, men en forretningsmæssig nødvendighed (Trumbach et al., 2023, p. 37).

Fatima, Hyatt, Rehman og kollegaer argumenterer for, at løbende forbedringer i procedurer, politikker og teknologiske løsninger er nødvendige for at fastholde offentlighedens tillid og styrke organisationers modstandskraft (Fatima et al., 2024, p. 248). De fremhæver, at det konstante trusselsmiljø ofte fører til stress og udbrændthed, hvilket øger risikoen for menneskelige fejl (Fatima et al., 2024, p. 248). I forlængelse heraf fremhæves ledelsen som en central faktor i skabelsen af et støttende arbejdsmiljø (Fatima et al., 2024, p. 253).

Effektiv risikohåndtering fremhæves også som en vigtig del i cybersikkerhed, og forskerne påpeger, at løbende risikovurderinger og opdateringer af sikkerhedsprocedurer er nødvendige for at fastholde en robust cybersikkerhedsstrategi (Fatima et al, 2024, p. 253). Ved at arbejde proaktivt og etablere klare retningslinjer kan organisationer både reducere medarbejdernes stressniveau og forbedre deres reaktion på potentielle cyberangreb. Derudover påpeger forskerne, at god og tydelig kommunikation er af central betydning for cybersikkerhedsarbejdet, idet klare

kommunikationskanaler og -procedurer styrker samarbejde og effektivitet (Fatima et al., 2024, p. 253).

Boeken (2024) fremhæver det problematiske i, at organisationer for ensidigt fokuserer på overholdelse af standarder som NIST, NIS2 og GDPR og på tekniske risikovurderinger, mens det organisatoriske perspektiv på cybersikkerhed overses. Hun argumenterer for, at dette ensidige fokus kan skabe *blind spots* hos organisationer, da *compliance* med standarder ofte misforstås som lig med en stærk cybersikkerhedskultur (Boeken, 2024, p. 1).

Selvom *compliance* kan forbedre datasikkerheden i umodne organisationer, påpeger Boeken, at det samtidig kan forhindre dem i at opnå en mere helhedsorienteret beskyttelse (2024, p. 1). Mange standarder fokuserer på, at visse sikkerhedsprocesser er til stede, men tager ikke højde for deres kvalitet, hvilket kan medføre en falsk følelse af sikkerhed (Boeken, 2024, p. 1). Dette resulterer ofte i en *check-box* mentalitet, hvor organisationer blot afkrydser krav på en liste uden at vurdere de faktiske effekter af deres sikkerhedsforanstaltninger. Det, der derimod er behov for, er en bredere forståelse af organisationskultur, ledelse og medarbejderadfærd, som inddrager forskellige faglige perspektiver i udviklingen af mere robuste og tilpassede sikkerhedsløsninger i organisationer.

Tema 3: Uddannelse og træning

Flere artikler fremhæver uddannelse og træning som nødvendige elementer i styrket cybersikkerhed. Målet er ikke kun at styrke tekniske kompetencer, men også om at øge den generelle modstandsdygtighed over for cyberangreb gennem øget *cyber awareness* og god cyberhygiejne (Carreiro et al., 2024).

Carreiro, Silva og Antunes (2024) undersøger, om *gamification* kan anvendes til cybersikkerhedstræning i sundhedssektoren. Dette er et vigtigt område pga. de følsomme data og vitale medicinske enheder, som ved angreb kan bringe patienternes liv i fare (Carreiro et al., 2024, p. 526).

I det lys er det ifølge Carreiro og kollegaer en udfordring, at uddannelser inden for sundhed nedprioriterer digitale kompetencer og cybersikkerhed (Carreiro et al., 2024, p. 526). Derudover påpeger de, at traditionelle træningsmetoder ofte kritiseres for at være tidskrævende og ineffektive, især når det gælder fastholdelse af medarbejdernes motivation og engagement under træningsforløb (Carreiro et al., 2024, p. 529). Som et alternativ fremhæves *gamification* som en tilgang, der ikke blot gør læring mere engagerende, men også bedre kan tilpasses de

sundhedsfaglige medarbejderes specifikke behov og arbejdsmæssige baggrunde (Carreiro et al., 2024, p. 529).

Mens *gamification* fokuserer på engagement og læring gennem motiverende elementer, peger Maennel og kollegaer på *Concept of Cyber Defence Exercises* (CDX)som en mere praktisk metode til træning. Øvelserne baserer sig på realistiske scenarier, hvor deltagerne testes i områder som *defense, incident response*, kommunikation og samarbejde (Maennel et al., 2023, p. 1).

Forskerne kritiserer imidlertid mange af de nuværende *CDX*-øvelser for ikke at være baseret på viden om, hvordan mennesker lærer bedst. De påpeger, at et ensidigt fokus på praktiske og tekniske formål kan føre til manglende motivation, samarbejde og refleksion. For at imødekomme dette anbefaler de en tværfaglig tilgang, der balancerer de tekniske færdigheder med de sociale og emotionelle aspekter, idet de understreger, at cyberangreb ikke kun handler om teknisk indsigt, men også om kritisk tænkning og tværfagligt samarbejde (Maennel et al., 2023, p. 10).

Tema 4: Politik og samfund

Dette tema handler om, hvordan hybridkrig og indblanding fra fremmede stater gennem sociale medier kan føre til informationsmanipulation og misinformation, som påvirker menneskers demokratiske standpunkter eller ændrer retningen for politiske bevægelser (Whyte, 2022).

Whyte analyserer, hvordan cybersikkerhedsdiskurser i stigende grad omfatter sociale og politiske dimensioner, særligt i forbindelse med udenlandske aktørers forsøg på at påvirke demokratiske processer. Gennem et casestudie af *Black Lives Matter* (BLM) undersøger han, hvordan bevægelsen er blevet fremstillet som en potentiel sikkerhedsrisiko (Whyte, 2022, p. 342). Han fremhæver desuden, at russiske *troll*-kampagner angiveligt har anvendt sociale medier til at skabe racemæssige spændinger. Disse kampagner har haft til formål at forstærke eksisterende samfundsmæssige skel og gøre konflikter mere synlige. Dette skete bl.a. gennem falske opslag, der både støttede og kritiserede BLM samt ved brug af målrettede hashtags som #TakeTheKnee og annoncer rettet mod geografiske områder, der tidligere har været centrum for store BLM-protester (Whyte, 2022, p. 344). En sådan framing bidrager til at fremstille BLM som en trussel mod den nationale orden snarere end som en legitim social bevægelse. .

Også enkeltpersoner på sociale medier kan blive mål for informationsmanipulation. Vićić og Gartzke understreger, at cybersikkerhed også omfatter, hvordan man håndterer manipulation af menneskers tanker, politiske holdninger og handlinger. De introducerer *Cyber Enabled Influence*

Operations (CEIO) som en ny form for cyberkonflikt, der fokuserer på at manipulere mennesker i stedet for teknologiske systemer, og beskriver dette som *hacking human minds* (Vićić & Gartzke, 2024, p. 11).

Denne form for manipulation adskiller sig fra traditionelle cyberangreb ved at udnytte sociale medier som platforme, hvor algoritmer gør det muligt at målrette budskaber præcist til specifikke mennesker (Vićić & Gartzke, 2024, p. 11). Dette skaber en unik mulighed for at forstærke eksisterende spændinger og udnytte sociale kløfter, hvilket kan påvirke samfundets sammenhængskraft og demokratiske processer.

For at undersøge fænomenet har forskerne anvendt *semantisk netværksanalyse* (SNA) på data fra Facebook-annoncer under det amerikanske præsidentvalg i 2016. Denne metode muliggør kortlægning af relationer mellem ord og temaer, hvilket bidrog til at afsløre, hvordan annoncerne var målrettet afroamerikanere og forstærkede eksisterende sociale spændinger, især i relation til emner som politivold og raceforhold, og at de var designet til at skabe splittelse blandt forskellige grupper i det amerikanske samfund (Vićić & Gartzke, 2024, p. 22).

Tema 5: Etik

Flere artikler behandler både direkte og indirekte de etiske dilemmaer, der opstår i forskning i og forebyggelse af cybersikkerhed.

Macnish og van der Ham (2020) påpeger, at både akademiske forskere og cybersikkerhedsfagfolk kan påvirkes af manglende etisk styring, og at uvidende forskningsdeltagere risikerer at blive udsat for alvorlige konsekvenser, især i autoritære regimer (Macnish & van der Ham, 2020, p. 2).

Forskerne fremhæver også en systemisk mangel på etikuddannelse inden for datalogi, hvilket betyder, at mange forskningsetiske komitéer mangler kompetencer til at vurdere cybersikkerhedsforskning fyldestgørende. Forskerne opfordrer desuden til klare og håndhævelige kodekser, der kan fremme konsistens og ansvarlighed i cybersikkerhedsforskning. De understreger også behovet for en aktiv diskussion om etiske spørgsmål, der kan støtte både udvikling og praksis inden for området (Macnish & van der Ham, 2020, p. 7).

Fenech, Richards og Formosa undersøger, hvordan utrænede mennesker håndterer dilemmaer, der opstår i *ransomware*-angreb, som stiller mennesker over for svære valg, hvor

beslutningen om at betale løsesummen eller risikere at miste data ikke kun er et teknisk spørgsmål, men også et komplekst etisk dilemma (Fenech et al., 2024, p. 1).

Forskerne fremhæver, at mennesker ofte betragtes som *the weakest link* i cybersikkerhedssystemer, fordi angreb udnytter manglende træning i cybersikkerhed og fraværet af klare retningslinjer (Fenech et al., 2024, p. 1). Ifølge forskerne står ofre for cyberangreb ofte alene med etiske valg, der kan have alvorlige konsekvenser (Fenech et al., 2024, p. 1).

Mersinas, Bada og Furnell (2025 p. 1) påpeger, at etiske aspekter ofte overses i arbejdet med adfærdsændringer i relation til cybersikkerhed. Derudover advarer de mod at anvende metoder, der kan skade medarbejdere, herunder brug af manipulerende teknikker eller *blame and shame*-kulturer, som kan skabe stress og modstand (Mersinas et al., 2025, p. 4). For at imødekomme dette foreslår de et etisk framework, der består af følgende seks principper:

- *Autonomy:* Respekt for individers ret til at træffe egne beslutninger
- *Beneficience:* Fremme det gode og maksimere positive resultater
- *Nonmaleficene*: Undgå at forårsage skade eller negative konsekvenser for individer
- *Justice:* Sikre fair og lige behandling af alle individer i forbindelse med interventioner
- *Transperency:* Være åben og tydelig omkring formål, metoder og forventede resultater af interventioner
- *Privacy:* Beskytte individers personlige oplysninger og sikre fortrolighed i interventionsprocessen

Ved at anvende dette framework kan organisationer udvikle interventioner, der både mindsker sikkerhedsrisici og understøtter en organisationskultur præget af tillid og læring. Når medarbejdere oplever et miljø, hvor fejl kan erkendes uden frygt for straf, og hvor individuelle fejl omdannes til læringsmuligheder for alle, kan det bidrage til en mere åben og tillidsfuld arbejdskultur (Mersinas et al., 2025, p. 4).

Tema 6: Design og maskinlæring

Nogle artikler undersøger, hvordan design af digitale løsninger kan styrke sikkerheden. Fx nævnes, at interfaceforbedringer og nudging-elementer kan øge brugernes opmærksomhed og påvirke adfærd (Katsarakes et al., 2024). Samtidig argumenterer nogle forskere for, at *machine learning* kan anvendes til at identificere angrebsmønstre og understøtte sikkerhedsbeslutninger (Chignell

et al., 2021). Følgende artikler dykker ned i, hvordan teknologiske og designorienterede løsninger kan forbedre cybersikkerheden.

Katsarakes, Edwards og Still undersøger ved hjælp af *eye-tracking*-teknologi, hvordan mennesker vurderer ægtheden af SMS-beskeder, og hvor de retter deres opmærksomhed hen. I studiet analyseres både hvilke elementer som afsenderoplysninger, links og stavefejl, der tiltrækker deltagernes opmærksomhed, og hvordan disse vægtes i vurderingen af beskedernes ægthed (Katsarakes et al., 2024, p. 1).

På trods af den stigende udbredelse af *SMiShing*-angreb vurderer forskerne, at området stadig er underbelyst (Katsarakes et al., 2024, p. 1). Forskerne påpeger, at *SMiShing*-angreb udnytter, at mange mennesker dagligt modtager et stort antal SMS-beskeder. Dette kan reducere opmærksomheden på beskedernes indhold og legitimitet (Katsarakes et al., 2024, p. 2). De understreger også, at mobiltelefonernes begrænsede skærmstørrelse yderligere vanskeliggør vurderingen, da det bliver sværere at opdage og evaluere afgørende indikatorer for ægthed. Fraværet af visuelle signaler, som f.eks. logoer, bidrager yderligere til at øge menneskers sårbarhed og har ført til betydelige økonomiske tab relateret til *SMiShing* (Katsarakes et al., 2024, p. 2).

Forskerne foreslår, at fremtidige initiativer bør fokusere på både at styrke brugertræning og forbedre designet af mobilinterfaces, så brugerne lettere kan identificere *phishing*-indikatorer (Katsarakes et al., 2024, p. 5). Udviklingen af uddannelsesprogrammer fremhæves også som en vigtig indsats. Derudover foreslås brugen af visuelle *nudging*-elementer, såsom advarsler placeret tæt på mistænkelige links, som en mulig måde at øge brugernes opmærksomhed på mulige trusler (Katsarakes et al., 2024, p. 5).

Et andet tema inden for udviklingen af softwareløsninger er, hvordan organisationer kan anvende *machine learning* for bedre at identificere og håndtere disse angreb. Denne problematik undersøges af Chignell og kollegaer, som ser på, hvordan interaktiv maskinlæring (iML) kan anvendes til at forbedre cybersikkerhed (Chignell et al. 2021, p. 1495). En del af tilgangen involverer en kombination af menneskelig ekspertise og maskinlæring for at reducere antallet af falske alarmer og understøtte beslutningsprocesserne i organisationerne.

Konklusion

Dette review har beskrevet, hvordan humanistiske perspektiver inddrages i forskning i cybersikkerhed. Gennemgangen viser, at temaer som human factor, organisatorisk sikkerhedskultur, uddannelse og træning, politik og samfund, etik samt design og maskinlæring spiller en vigtig rolle, når det kommer til cybersikkerhed. Selvom reviewet ikke hævder at være dækkende, viser det dog, at humanistiske perspektiver allerede spiller en rolle inden for forskningen, men også, at humaniora med fordel kan indtage en langt stærkere position inden for dette område. Cybersikkerhed er således ikke kun et spørgsmål om tekniske løsninger, men også om menneskelige erfaringer og adfærd, organisatoriske forhold samt kulturelle ændringer. At bidrage med viden om disse emner i tværfaglige forsknings- og udviklingsopgave fremstår således som en vigtig udviklingsretning for humanistiske forskere.

Litteraturliste

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19–32. https://doi.org/10.1080/1364557032000119616

Boeken, J. (2024). From compliance to security, responsibility beyond law. *Computer Law & Security Review*, *52*, 105926. https://doi.org/10.1016/j.clsr.2023.105926

Carreiro, A., Silva, C., & Antunes, M. (2024). The use of gamification on cybersecurity awareness of healthcare professionals. *Procedia Computer Science*, *239*, 526–533. https://doi.org/10.1016/j.procs.2024.06.202

Chignell, M. H., Chung, M.-H., Yang, Y., Cento, G., & Raman, A. (2021). Human Factors in Interactive Machine Learning: A Cybersecurity Case Study. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *65*(1), 1495–1499. https://doi.org/10.1177/1071181321651206

Das, S., Gutzwiller, R. S., Roscoe, R. D., Rajivan, P., Wang, Y., Jean Camp, L., & Hoyle, R. (2020). Humans and Technology for Inclusive Privacy and Security. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *64*(1), 461–464. https://doi.org/10.1177/1071181320641104

Datta, P. M., & Acton, T. (2023). From disruption to ransomware: Lessons From hackers. *Journal of Information Technology Teaching Cases*, *13*(2), 182–192. https://doi.org/10.1177/20438869221110246

Edwards, M., Morris, T., Chen, J., & Still, J. (2023). SMiShing Attack Vector: Surveying End-User Behavior, Experience, and Knowledge. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *67*(1), 1911–1915. https://doi.org/10.1177/21695067231192193

Fatima, F., Hyatt, J. C., Rehman, S. U., De La Cruz, E., Nadella, G. S., & Meduri, K. (2024). Resilience and risk management in cybersecurity: A grounded theory study of emotional, psychological, and organizational dynamics. *Journal of Economy and Technology*, *2*, 247–257. https://doi.org/10.1016/j.ject.2024.08.004

Fenech, J., Richards, D., & Formosa, P. (2024). Ethical principles shaping values-based cybersecurity decision-making. *Computers & Security*, *140*, 103795. https://doi.org/10.1016/j.cose.2024.103795

Katsarakes, E. A., Edwards, M., & Still, J. D. (2024). Where Do Users Look When Deciding If a Text Message is Safe or Malicious? *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 10711813241264204. https://doi.org/10.1177/10711813241264204

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses. *Science, Technology, & Human Values*, *46*(6), 1316–1339. https://doi.org/10.1177/0162243921992844

Macnish, K., & Van Der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society*, *63*, 101382. https://doi.org/10.1016/j.techsoc.2020.101382

Maennel, K., Brilingaitė, A., Bukauskas, L., Juozapavičius, A., Knox, B. J., Lugo, R. G., Maennel, O., Majore, G., & Sütterlin, S. (2023). A Multidimensional Cyber Defense Exercise: Emphasis on Emotional, Social, and Cognitive Aspects. *Sage Open*, *13*(1), 21582440231156367. https://doi.org/10.1177/21582440231156367

Mersinas, K., Bada, M., & Furnell, S. (2025). Cybersecurity behavior change: A conceptualization of ethical principles for behavioral interventions. *Computers & Security*, *148*, 104025. https://doi.org/10.1016/j.cose.2024.104025

Nobles, C., & Robinson, N. (2024). The Missing Engineering Discipline in Cybersecurity: Human Factors Engineering. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 10711813241275926. https://doi.org/10.1177/10711813241275926

Trumbach, C. C., Payne, D. M., & Walsh, K. (2023). Cybersecurity in business education: The 'how to' in incorporating education into practice. *Industry and Higher Education*, *37*(1), 35–45. https://doi.org/10.1177/09504222221099389

Vićić, J., & Gartzke, E. (2024). Cyber-enabled influence operations as a 'center of gravity' in cyberconflict: The example of Russian foreign interference in the 2016 US federal election. *Journal of Peace Research*, *61*(1), 10–27. https://doi.org/10.1177/00223433231225814

Whyte, J. (2022). Cybersecurity, race, and the politics of truth. *Security Dialogue*, *53*(4), 342–362. https://doi.org/10.1177/09670106221101725