Hvem er cybereksperten? Ekspertise og professioner i cybersikkerhedsfeltet

Temanummer: Cybersikkerhed

Cybersikkerhedseksperter spiller en vigtig rolle i at identificere digitale risici og at definere hensigtsmæssige løsninger. Denne artikel gør brug af professions- og ekspertsociologien til at belyse konkurrerende epistemiske rationaliteter i konstruktionen af digitale risici. På baggrund af et nyt datasæt omhandlende ekspertprofiler i offentlige og private cybersikkerhedsråd og -udvalg, argumenteres der for, at profilen af cybersikkerhedseksperter har bevæget sig væk fra et rent teknisk fokus og hen imod en procesorientering, som både er bredere i fokus og placeret tættere på beslutningstagere. Den nye ekspertprofil er positioneret i et spændingsfelt imellem tekniske, organisatoriske og økonomiske rationaliteter. I fraværet af en bred politisk debat kan denne udvikling styrke ekspertmagten, som nu er begrænset til få hybride aktører, som formår at bygge bro imellem de forskellige rationaliteter. En sådan udvikling vil være skadelig for demokratiet, men udviklingen imod en procesorienteret forståelse af cybersikkerhed åber samtidlig muligheder for at re-politisere cybersikkerhedsdiskursen igennem en mindre teknifiseret debat.

Viden om cybersikkerhed er teknisk – men også politisk

JOHANN OLE WILLERS
research fellow, Norsk Utenrispolitisk Institutt (NUPI) og ph.d.-studerende, Institut for Organisation, Copenhagen Business School, jow.ioa@cbs.dk

Cybereksperten er uden tvivl blevet en central aktør i dagens sikkerhedspolitiske debat, hvor afhængigheden af digitale ydelser og produkter i stigende grad har rettet virksomheders, politikeres og individers opmærksomhed imod digitale sårbarheder og trusler.[1] I dag er cybersikkerhed både en strategisk målsætning og en eftertragtet kompetence.

Men hvem er cybereksperten egentlig? Lene Hansen og Helen Nissenbaum konstaterede i 2009, at kombinationen af den tekniske karakter og hastigheden af forandringsprocesser indenfor cybersikkerhed cementerer ekspertens rolle som en af de centrale aktører, der konstituerer cybersikkerhed som et sikkerhedspolitisk emne (Hansen og Nissenbaum, 2009: 1166). I dag indtager cybereksperter vigtige samfundspolitiske roller gennem blandt andet offentligt-private partnerskaber (Christensen og Petersen, 2017) og i det diplomatiske felt (Segal, 2017). Samtidig er der overraskende lidt enighed om cybereksperternes færdigheder (Shires, 2018: 32). I artiklen tilnærmer jeg mig spørgsmålet, om hvad der karakteriserer cybereksperten, og hvordan cybereksperternes rolle har udviklet sig over tid. Med udgangspunkt i professions- og ekspertsociologien introducerer jeg en ny tilgang til den politiske læsning af cybersikkerhed og dets forhold til vidensdannelsen, som senest har tiltrukket akademisk interesse (Dunn Cavelty og Wenger, 2020).

Det centrale argument er, at ideer om, hvordan vi som samfund skal adressere digitale risici, ikke opstår i et institutionelt vakuum. Tværtimod bliver ideer

udviklet, testet og spredt blandt eksperter på tværs af institutionelle grænser. Om disse ideer følger en økonomisk, teknisk eller geopolitisk logik, kan have stor påvirkning på, hvordan politiske løsninger udformes (Kremer, 2014). Det er derfor nødvendigt at udvikle et analytisk apparat, der gør os i stand til at undersøge ekspertise og ekspertviden indenfor cybersikkerhed. Et forskningsfelt, hvor der historisk er blevet fokuseret på interstatslige konflikter og strategiske dimensioner (Gorwa og Smeets, 2019). Med udgangspunkt i ekspertsociologien sætter jeg fokus på ekspertvidens politiske karakter og kampen om anerkendelse (Reed, 1996; Sending, 2015). Derudover trækker jeg på Andrew Abbott's professionssociologi for at situere cybersikkerhedsarbejdet i et spændingsfelt imellem økonomiske, politiske og tekniske overvejelser (Abbott, 1988; 2005).

Jeg henter derved inspiration i senere strømninger i cybersikkerhedslitteraturen, som undersøger, hvordan cybersikkerhedsspørgsmål relaterer sig til eksisterende, og skaber nye, sociale formationer (McCarthy, 2018: 6). Actor-network-teori og science and technology studies (STS) er blevet brugt til at undersøge relationerne imellem tekniske og sociopolitiske objekter (Dunn Cavelty, 2018; Stevens, 2018). Ligeledes har assemblage teori vist sig at kunne belyse komplekse netværk af materielle og ikke-materielle aktører, som konstituerer cybersikkerhedsdebatten (Collier, 2018). Ligeledes er praksisteorien senest blevet brugt til at undersøge sociopolitiske fordelingsspørgsmål relateret til cybersikkerhedskoncepter (McCarthy, 2018). Fælles for ovenstående nye teoretiske bidrag er et analytisk udgangspunkt, som retter fokus imod, hvordan cybersikkerhed opstår igennem en sammenfletning af mennesker, objekter og ideer (Dunn Cavelty og Wenger, 2020) og hvordan de resulterende socioteknologiske processer konstituterer cybersikkerhedspraksis og -diskurs. Artiklens bidrag til denne diskussion er at udvide det teoretiske apparat ved at introducere professions- og ekspertsociologien som lovende redskaber til at undersøge den politiske karakter af vidensdannelsen i konteksten af definitionen af digitale risici og håndteringen af disse (se også T. Stevens, 2012).

Det næste afsnit introducerer litteraturen om ekspertise og giver eksempler på cybereksperters indflydelse på udformningen af regler og normer inden for cybersikkerhedsområdet. Sektionen er efterfulgt af en diskussion af professionsbegrebet i relation til cybereksperise med et fokus på, hvordan fremvæksten af nye problemstillinger har relateret sig til allerede eksisterende professionelt arbejde. Dernæst illustrerer jeg perspektivet gennem en analyse af danske eksperter i centrale offentlige og private udvalg. Jeg afslutter med en diskussion om implikationerne af en ny ekspertprofil, som både er bredere i fokus og tættere på beslutningstagere end den tidligere tekniske profil.

Ekspertise i fokus

Fra et akademisk perspektiv har vidensproduktion længe tiltrukket interesse. Her er et centralt omdrejningspunkt sammenfletningen af viden og magt (Allan, 2018; Bueger, 2014; CASE Collective, 2006). Eksperten er en person

med særlige kompetencer indenfor et defineret område. Som vi ved fra mange områder såsom økonomisk og sikkerhedspolitik er ekspertviden dog sjældent uanfægtet. Tværtimod ser vi ofte en kamp om anerkendelsen af at besidde overlegen ekspertise (Eyal, 2013a). Litteraturen opererer med udtrykket "the politics of expertise" (Reed, 1996; Sending, 2015) og refererer til "conflicts over the exclusionary jurisdictional domains arising out of the contested monopolization of abstract knowledge and technique" (Reed, 1996: 582). Med andre ord beskriver udtrykket en situation, hvor flere ekspertgrupper konkurrerer om at opnå epistemisk legitimitet til både at definere et problem samt de værktøjer og færdigheder, der skal til for at håndtere problemet. Tyskerne har et passende udtryk til at beskrive denne proces: kampen om *Deutungshoheit* – den eksklusive kapacitet til at fortolke problemer og definere hensigtsmæssige løsninger (Krentz, 2014). Epistemisk legitimitet referer derved til den nødvendige sociale anerkendelse og autoritet for at opnå "Deutungshoheit".

Men hvorfor er det vigtigt at forstå denne proces? Sikkerhed er ikke et selvforklarende koncept. Som Robert McCarthy skriver, handler det først og fremmest om spørgsmålet "sikkerhed for hvem?" (2018: 8). Cybersikkerhed er et anfægtet begreb (Smeets og Shires, 2017) og centrale aspekter såsom, hvad der kategoriseres som et sikkerhedsproblem, og hvem der har ansvaret for at håndtere problemer, forhandles kontinuerligt (Christensen og Liebetrau, 2019: 396). Hvordan sikkerhed konceptualiseres er derfor afgørende for, hvordan sikkerhedsproblemer defineres, fortolkes og håndteres. Ekspertviden står derved altid i relation til de sociale og politiske institutioner, som danner den kulturelle ramme for produktionen af viden (Slayton og Clark-Ginsberg, 2018: 117). Dette åbner op for konflikter mellem epistemer, som arbejder indenfor det samme problemfelt. Jens Kremer benytter sig af begrebet "security mindsets", der identificerer distinkte liberale og militære tænkemåder i den amerikanske tilgang til cybersikkerhed. Disse "mindsets" er afhængige af professionelle og institutionelle baggrunde, politiske overbevisninger og verdensanskuelser (Kremer, 2014). Et andet eksempel stammer ligeledes fra USA, hvor det er blevet dokumenteret, hvordan reguleringen af kritisk infrastruktur har været præget af konflikter mellem eksperter indenfor henholdsvis informationsteknologi (IT) og operationel teknologi (OT) med konsekvenser for både reguleringens form og eksperternes fremtidige profil (Slayton og Clark-Ginsberg, 2018: 124).

Muligheden for at fremme forskellige – og ofte konkurrerende – tilgange til cybersikkerhed er en af årsagerne til eksperternes betydning i feltet. Ekspertviden kan derved fungere som en legitimerende faktor i udarbejdelsen af politiske tiltag (Bueger, 2014). Der er dog også særlige strukturelle karakteristika, som kan give eksperter stor indflydelse i cybersikkerhedsfeltet. Den tekniske karakter og hastigheden af forandringsprocesser er to faktorer, som allerede blev nævnt i introduktionsafsnittet. Den globale mangel på ekspertviden er en yderligere faktor.

Tim Stevens argumenterer for, at den tekniske kompleksitet og den hurtige udvikling i cybersikkerhedsfeltet skaber et spørgsmål om, hvad der er en reel fare, og hvad der ikke er. Dette "epistemologiske problem" danner kernen af cybersikkerhedsnarrativer (T. Stevens, 2016: 155). Et sådant narrativ konstruerer, ifølge Hansen og Nissenbaum, det tekniske som "a domain requiring an expertise that the public (and most politicians) do not have and this in turn allows 'experts' to become securitizing actors [...]" (Hansen og Nissenbaum, 2009: 1167). Lignende tendenser er blevet observeret i andre felter med høj teknisk kompleksitet (Gracia og Oats, 2012; Thistlethwaite og Paterson, 2016; Tsingou, 2014).

» Mange offentlige institutioner oplever stadigvæk store problemer, når de skal hyre cybersikkerhedseksperter. I Tyskland er hver fjerde offentlig cybersikkerhedsstilling stadig ledig i 2020

Samtidig er der en markant mangel på cybereksperter på et globalt plan (Vogel, 2016). Den internationale organisation for IT-professionelle, ISACA, estimerer, at der globalt manglede to millioner cybersikkerhedseksperter i 2019 (ISACA, 2019). En konsekvens heraf er, at mange organisationer hverken har mulighed for eller råd til at ansætte kvalificerede eksperter. I starten af 2010'erne havde de amerikanske myndigheders afhængighed af private cybersikkerhedsleverandør nået et niveau, hvor flere observatører frygtede udviklingen af en strukturel ubalance, der vil muliggøre, at cybersikkerhedseksperter selv kunne definere efterspørgslen og leveringen af løsninger (Deibert, 2013; Lee og Rid, 2014). Mange offentlige institutioner oplever stadigvæk store problemer, når de skal hyre cybersikkerhedseksperter. I Tyskland er hver fjerde offentlig cybersikkerhedsstilling stadig ledig i 2020. Det gælder især stillinger i indenrigsministeriet, som snart står med ansvaret for at sikre enorme nye datamængder som konsekvens af mere offentlig og digital overvågning (Domscheit-Berg, 2020). Vi mangler tilsvarende tal fra den danske offentlige sektor, men intet tyder på en markant bedre situation. Digitaliseringsstyrelsens undersøgelse om implementeringen af internationale cybersikkerhedsstandarder konkluderer for eksempel at områderne "ressourcer, kompetencer og bevidsthed" er blandt de mest problematiske indenfor danske myndigheder (Digitaliseringsstyrelsen, 2019: 5).

Mange lande er begyndt at nævne uddannelse af cybersikkerhedseksperter som et specifikt fokusområde. I USA præsenterede Obama-administrationen den første nationale "Cybersecurity Workforce Strategy" i 2016 og afsatte 62 millioner USD årligt til at støtte uddannelsen af nye eksperter (White House, 2016). Ligeledes har Trump erklæret cybersikkerhedseksperterne "a strategic asset that protects the American people, the homeland, and the American way of life" (Trump, 2019). I Danmark er den første dedikerede kandidatuddannelse i cybersikkerhed blevet etableret på Aalborg Universitet tidligere på året (Aalborg Universitet, 2020). Den danske cyber- og informationssikkerhedsstrategi definerer ligeledes en målsætning om at etablere en bedre forståelse

for digitale risici på tværs af uddannelseskæden (Finansministeriet, 2018: 32). Storbritannien har i sin seneste nationale cyberstrategi sat et eksplicit mål om at udvikle en professionel organiseret gruppe af cybereksperter (Government of the United Kingdom, 2016; 2018).

Opsummerende kan det konstateres, at de usikkerheder der opstår som resultatet af den tekniske udvikling og en global mangel på cyberekspertise, har skabt et felt, som både privilegerer ekspertviden og underminerer muligheden for offentlig og politisk debat. Det åbner et stort spørgsmål: Hvilke metodiske værktøjer kan vi bruge til at studere, hvordan denne ekspertise er organiseret, og hvor den er placeret? I det efterfølgende afsnit introducerer jeg professionsperspektivet som et bud på en mulig tilgang.

Professioner og professionalisering

Om en professionalisering af cybersikkerhedsbranchen er en ønskelig udvikling, har længe været et omdiskuteret spørgsmål (Burley, Eisenberg og Goodman, 2014; Dawson og Thomson, 2018; National Research Council, 2013). Professionalisering bliver i denne debat konceptualiseret som en funktionel proces med formålet at sikre en minimumstandard igennem brugen af blandt andet certificeringer, licenser, fælles uddannelsesforløb og fælles etiske regler (Ford og Gibbs, 1996: 5). Debatten er da fokuseret på, om en professionalisering af cybersikkerhedsbranchen vil skabe en positiv samfundsmæssig effekt eller forværre manglen på kvalificerede eksperter. Abbotts professionssociologi, som danner baggrunden for artiklens analyse, bryder derimod med det instrumentelle fokus og retter blikket mod placeringen af ekspertviden indenfor et system af professioner, som kæmper om kontrol og anerkendelse (Abbott, 1988: 98). I de efterfølgende afsnit diskuteres den funktionelle professionsliteratur indenfor cybersikkerhed og introducerer derefter Abbotts professionssociologi.

Fra et funktionelt perspektiv kan der være klare fordele ved en professionalisering. Kunder er sikret en minimumstandard, den offentlige anerkendelse af arbejdet øges, og professionen har nemmere ved at tiltrække unge talenter gennem etableringen af klare karriereforløb og sikre arbejdsbetingelser. Der er dog også ulemper forbundet med professionalisering. Adgangsbarrierer til professionen gennem for eksempel obligatoriske uddannelsesforløb kan føre til en unødvendig reduktion af den tilgængelige arbejdskraft (Burley et al., 2014). Ligeledes konkluderede det Amerikanske National Research Council i 2013 at "some organizations may find that professionalization provides a useful degree of 'quality control' for those who work in the field, but professionalization also imposes barriers to those who wish to enter the field at a time when demand for cybersecurity workers exceeds supply" (National Research Council, 2013: 2). Professionaliseringen er derved en proces, som indebærer et afgrænsende og et homogeniserende element: en anerkendelse af at have de rigtige værktøjer til at adressere et anerkendt problem, og disse værktøjer er fælles for alle indenfor professionen (Abbott, 1988: 60). Typiske kendetegn

på modne professioner er institutionaliserede dedikerede universitetsuddannelser, professionelle organisationer, certificeringer og en fælles etiske regler (Ford og Gibbs, 1996). En organisk udvikling af disse dimensioner tager tid og professionalisering er derfor typisk en lang historisk proces (Fourcade, 2010).

Cybersikkkerhed er på mange måder en umoden profession. De første antivirusprogrammer blev udviklet i slutningen af 1980'erne, og udviklingen af det nuværende marked for cybersikkerhed skete ikke inden starten af 2010'erne, hvor angrebene blev mere ødelæggende og udbredte (Denning og Frailey, 2011). Der er mange arbejdsopgaver relateret til cybersikkerhed med ofte overlappende og løst definerede ansvarsområder (National Research Council, 2013). I 2001 identificerede Peter Denning "system security" som en af 15 discipliner indenfor IT (Denning, 2001). Begrebet "system security" refererer til en primært teknisk opgave inden for IT-afdelinger. I takt med udviklingen af et i stigende grad komplekst trusselsbillede og en kontinuerlig udvidelse af den underliggende teknologi er der opstået flere opgaver, som kræver forskellige færdigheder, viden og kompetencer (Dawson og Thomson, 2018). I 2017 udgaven af det Amerikanske Nationale Institut for Standarder og Teknologis "Cybersecurity Workforce Framework" er opgaven "system security" bare én blandt 62 "work roles" indenfor cybersikkerhedsfeltet (NIST, 2017). At anskue cybersikkerhed som en homogen profession frem for et løst sammenhængende felt er derfor problematisk. Snarere er cybersikkerhed en umoden profession, som er kendetegnet ved manglen på en fælles uddannelsesbaggrund, løs professionel organisering og eksisterende, men ikke obligatoriske certificeringer og licenser (Ford og Gibbs, 1996).

» **At anskue cybersikkerhed som en homogen profession frem for et løst sammenhængende felt er derfor problematisk. Snarere er cybersikkerhed en umoden profession, som er kendetegnet ved manglen på en fælles uddannelsesbaggrund, løs professionel organisering, og eksisterende, men ikke obligatoriske certificeringer og licenser**

Frem for at fokusere på den funktionelle professionalisering af cybersikkerhed åbner Abbotts professionssociologi for spørgsmål om, hvordan grupper kæmper om at kontrollere bestemte arbejdsopgaver i samfundet (Abbott, 1988: 98). Praktisk betyder det, at håndteringen af digitale risici foregår i et organisatorisk felt af relaterede problemstillinger (Dawson og Thomson, 2018). Er cybersikkerhed et teknisk, organisatorisk, finansielt eller kulturelt spørgsmål? Fordelen ved at bruge Abbotts perspektiv på, hvordan ekspertise organiseres socialt, er, at der tages højde for, hvordan cybersikkerhedsspørgsmål er relateret til forskellige felter: "Cybersecurity is no longer the remit only of private or corporate practitioners but has become a complex site of interaction between a very wide range of people, organizations and technologies" (C. Stevens, 2020: 133). Abbotts professionsbegreb fremhæver, at det er i relationen mellem pro-

fessioner, at kontrollen over problemer defineres. At dominere et problemfelt tillader en profession at definere problemet, at afgrænse handlingsmuligheder og, måske mest afgørende, at bestemme successkriterier (Abbott, 1988: 137).

En profession er derved kendetegnet ved at kontrollere en given opgave gennem brugen af abstrakt viden (Abbott, 1988: 8, 53). Klassiske eksempler er læger, jurister og revisorer. Nogle professioner – såsom økonomer – har markant udvidet deres magt igennem tiden ved at kontrollere flere og flere sociale problemstillinger (Fourcade, Ollion og Algan, 2015). Leonie Maria Tanczer og kollegaer dokumenterer en sådan proces, hvor cybereksperter trænger ind på jurisdiktionen af eksisterende professioner. Deres analyse viser, hvordan Cyber Security Incident Response Teams (CSIRTs) har formået at navigere geopolitiske konflikter. Ved at skabe transnationale netværk af cybersikkerhedseksperter med unikke fordele overfor klassiske politiske aktører har CSIRTs udvidet deres arbejdsfelt fra en teknisk opgave til en diplomatisk rolle (Tanczer, Brass og Carr, 2018).

Clare Stevens viser derudover, hvordan efterforskningen af cyberangreb i private sikkerhedsfirmaer placerer cybereksperten i et spændingsfelt mellem teknisk ekspertise og politiske konsekvenser. Igennem en analyse af Symantecs undersøgelse af Stuxnet-koden dokumenteres det, hvordan det tekniske arbejde blev "entangled in the politics of nuclear proliferation, diplomacy, international law, and the mechanisms of global cybersecurity governance" (C. Stevens, 2020: 130).

Ved at fokusere på professionernes konkrete arbejde frem for deres strukturelle karakteristika åbner professionssociologien en tilgang til spørgsmålet om, hvem der har autoriteten til at definere digitale risici og afgrænse håndteringen af disse. Hastigheden af forandringsprocessen i teknologien og trusselsbilledet bidrager til en afpolitisering af emnet og placerer den epistemiske autoritet fast i hænderne på eksperterne: "[T]he epistemic authority which computer and information scientists hold allow them the privileged role as those who have the authority to speak about the unknown" (Hansen og Nissenbaum, 2009: 1166-7). Offentlige og private råd og udvalg kan være en vigtig indikator på, hvilke professioner der er involveret i denne proces, fordi de fungerer som et samlingssted, hvor anerkendte eksperter samles for at diskutere presserende spørgsmål, ofte med en strukturende effekt på det videre felt (Reed, 1996; van Apeldoorn og Graaff, 2014). Det er mod dem, jeg vender mig i den følgende analyse af danske cybereksperter.

Danske cybersikkerhedeksperter

For at illustrere ovenstående teoretiske overvejelser præsenterer jeg i det følgende en analyse af danske top-cybersikkerhedeksperter. Baggrunden for analysen er en samling af nævnte eksperter i danske komitéer og råd med cybersikkerhed som det eneste fokusområde. Ekspertgrupper kan spille en strategisk rolle i strukturering af professionelt arbejde og kontrol og er derfor velegnet til professionssociologiske analyser (Reed, 1996; Seabrooke og

Tsingou, 2014). Datasættet dækker over 195 poster fordelt på 176 personer. Nogle råd er nedsat af offentlige institutioner (Cybersikkerhedsråd og Erhvervsministeriets IT Sikkerhed Virksomhedsråd). En enkelt er en uafhængig organisation, to er tilknyttet brancheorganisationer og den sidste dækker over de største danske virksomheders' ansvarlige personer for cybersikkerhed (C25-virksomheder). Rådene er blevet udvalgt igennem *purposive sampling* på baggrund af synlighed i den offentlige debat (Tansey, 2007). Analysen har et illustrerende formål og sigter ikke mod at præsentere et repræsentativt billede af alle cybersikkerhedseksperter i Danmark. Alligevel fremvises tendenser blandt Danmarks top cybersikkerhedseksperter. Det skal dog fremhæves, at datasættet har klare begrænsninger og ingen af konklusionerne, som fremgår af analysen, er definitive. Derudover er det vigtigt at understrege, at analysen udelukkende fokuserer på råd og udvalg. Faste institutioner såsom Center for Cybersikkerhed eller Digitaliseringsstyrelsens "Kontor for Cyber- og Informationssikkerhed" er derfor ikke direkte en del af datasættet. Derimod er Center for Cybersikkerhed's Cybersikkerhedsråd en del af analysen.

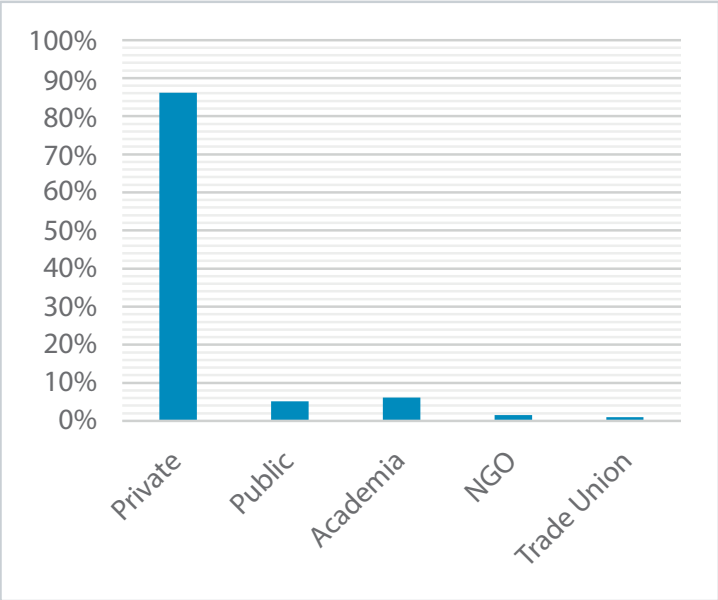
Tabel 1: Oversigt over cybersikkerhedsråd og -udvalg i analysen

Navn	Antal Medlemmer	Offentlig/Privat Styret
Cybersikkerhedsråd	19	Offentligt, Center for Cybersikkerhed
IT-Branchens Sikkerhedsudvalg	53	Privat, IT Branchen
Rådet for Digital Sikkerhed	63	Uafhængig Organisation
Erhvervsministeriets IT Sikkerhed Virksomhedsråd	14	Offentligt, Erhvervsministeriet
Dansk Industri's Udvalg for Informationssikkerhed	16	Privat, Dansk Industri
C25 Danske Virksomheder CISOs eller tilsvarende[2]	30	Privat, ikke formelt organiseret

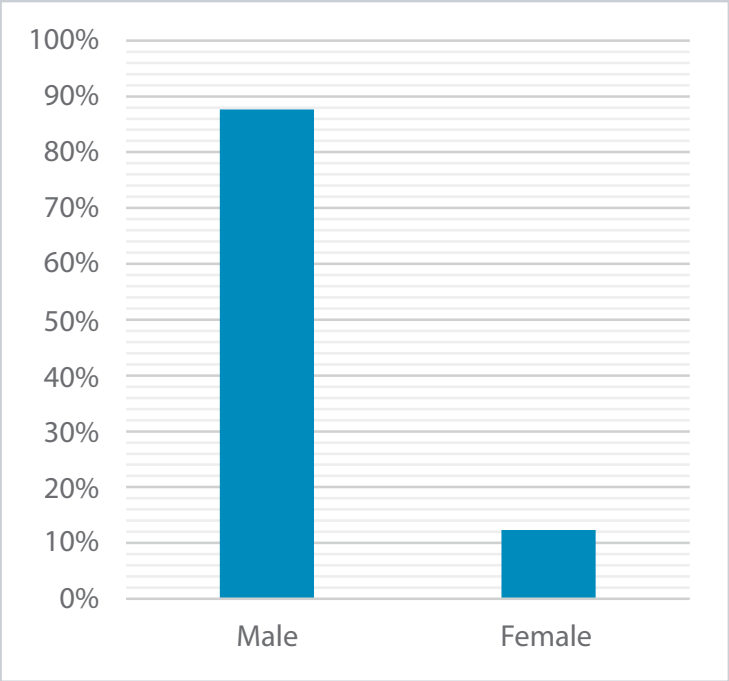
CV'er og uddannelseshistorik blev samlet fra konferencebrochurer og andre offentlige kilder såsom LinkedIn. Resultatet viser først og fremmest en heterogen gruppe af individer. To klare tendenser er, at cybereksperten arbejder i den private sektor, og langt størstedelen af dem er mænd. 86 pct. arbejder i den private sektor, mens henholdsvis 6 pct. og 5 pct. er tilknyttet forsknings- og offentlige institutioner. Kvinder udgør bare 12 pct. Der er en klar fare for "selection-bias" her, i og med at de udvalgte råd og udvalg til dels er private. Studier fra andre lande viser dog lignende resultater. Ifølge ISC²'s 2019 *Cybersecurity Workforce Survey* er 30 pct. af de adspurgte cybereksperter kvinder (ISC2, 2019). Et 2017 "*Global Information Security Workforce Study*" estimerer imidlertid, at på et globalt plan er næsten 90 pct. af cybereksperter mænd (Frost og Sullivan, 2017: 5). At finde data på andelen af offentligt ansatte cybereksperter er mere problematisk (Bate, 2018: 9). En undersøgelse fra Storbritanniens regering viser, at offentlige institutioner har 50 pct. højere sandsynlighed for at outsource cybersikkerhedsopgaver end private virksomheder (Pedley et al., 2020). Det er en indikator for, at offentlige organisationer kan have særlige

problemer med at tiltrække kvalificerede eksperter, blandt andet fordi det kan være svært at konkurrere med lønniveauet i den private sektor (Pollitt, 2010).

Figur 1: Cybereksperter fordelt på sektorer



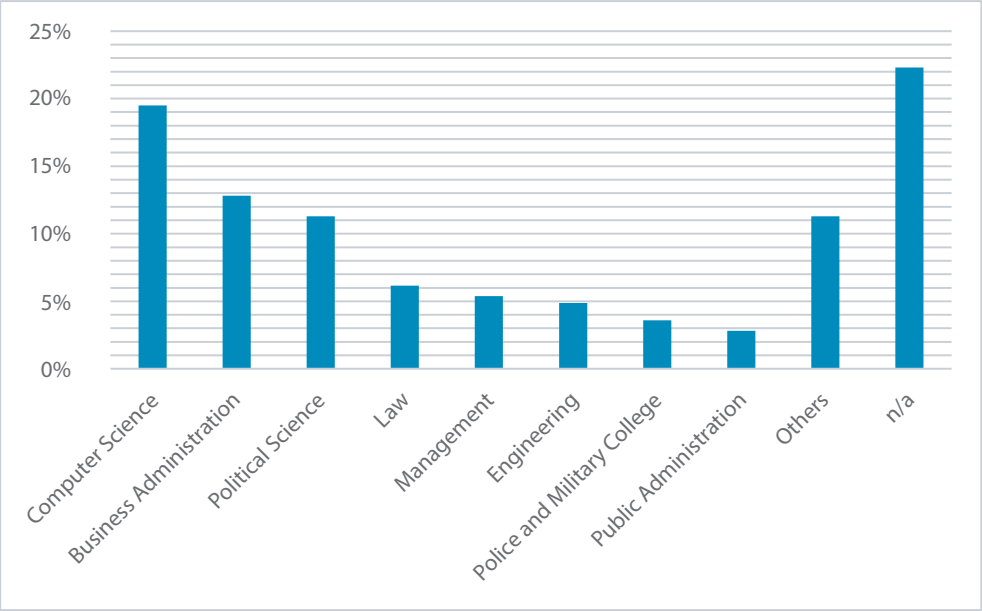
Figur 2: Cybereksperter fordelt efter køn



Uddannelsesmæssigt viser der sig derimod et blandet billede. For hver person i datasættet blev de to seneste videregående uddannelser med minimum to-årig varighed registreret. Det vil sige, at enkeltforløb ikke er blevet registreret. Formålet er at samle sammenhængende uddannelsesforløb, som blev afsluttet med et afgangsbevis. For 19 individer blev der ikke fundet uddannelsesrelate-

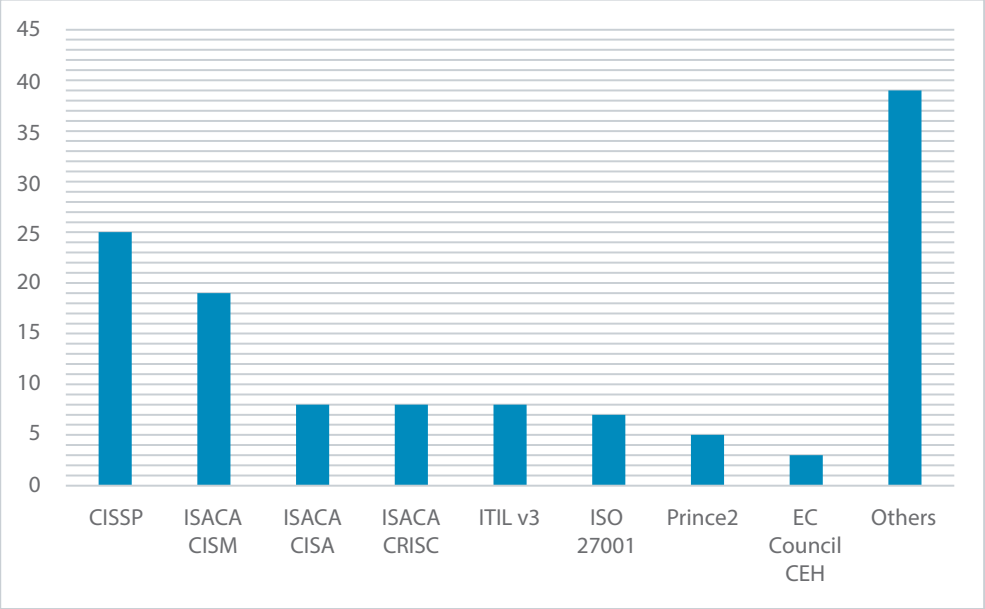
ret information. Yderlige 26 fik kun registreret én uddannelse. Tilsammen svarer de to grupper til de 22 pct. af manglende (n/a) værdier i datasættet. For at give et samlet overblik var det nødvendigt at kategorisere uddannelserne. Det var særligt vigtigt for kategorien computer science. Begrebet dækker i analysen over alle uddannelsestyper indenfor computer, IT, encryption og data science med et overvejende teknisk perspektiv. Computer engineering blev for eksempel kodet som computer science frem for engineering. Til gengæld blev "business og ICT management" kodet som management. Resultaterne skal derfor igen fortolkes som vejledende frem for definitive. Som det fremgår af figur 3 er computer science den hyppigste uddannelsestype blandt de 390 registrerede uddannelser (19 pct.). Business administration (13 pct.) og statskundskab (11 pct.) tager anden- og tredjepladserne. Det kan være overraskende, når der tages udgangspunkt i den klassiske tekniske definition af arbejdet, som diskuteret i Dennings analyse fra starten af 00'erne. En anden måde at illustrere resultatet på er, at næsten en tredjedel (32 pct.) af eksperterne har gennemført minimum én it-specifik uddannelse på universitetsniveau. Samme tendens ses i amerikanske markedsanalyser, som viser, at den hyppigste uddannelsesbaggrund for cybersikkerhedseksperter er computer science og -engineering (Frost og Sullivan, 2017: 5).

Figur 3: Cybereksperters uddannelsesbaggrund, samlede kategorier



Ligeledes er det interessant at se nærmere på de mindre klassiske uddannelser. 19 pct. af eksperterne har som minimum taget en uddannelse i business administration. Hvis vi samler business administration, statskundskab, management, økonomi og public administration i én samlet kategori, kan vi se, at næsten halvdelen (44 pct.) af eksperterne har gennemgået, hvad der kan karakteriseres som en "Djøf-uddannelse".

Figur 4: Certificeringer blandt cybereksperter[3]



Så vidt muligt blev der også taget højde for eksperternes certificeringer. Resultaterne af denne analyse skal læses med den usikkerhed in mente, at der har været et højt antal af manglende værdier (122). To tendenser står dog frem. Både "(ISC)²" CISSP (25) og ISACAs CISM-, CISA- og CRISC-certifikater (35 samlet) dominerer blandt eksperterne. CISSP-certifikatet står for Certified Information Systems Security Professional og bliver udstedt af verdens største medlemsforening af professionelle cybersikkerhedseksperter med over 150.000 certificerede medlemmer verden over (ISC², 2020). At have et CISSP-certifikat er et vigtigt signal, men det fungerer ikke i sig selv som en vej ind i branchen. Derimod er flerårig dokumenteret erfaring en nødvendig forudsætning for at kvalificere som kandidat. CISSP er ofte karakteriseret som den mest anerkendte akkreditering for cybersikkerhedseksperter og signalerer en bred viden på tværs af cybersikkerhedskategorier (Pedley et al., 2020: 14). ISACA er en bredere organisation som dækker over professionelle indenfor IT-branchen generelt og udstiller certifikater blandt andet indenfor cybersikkerhedsfeltet (ISACA, 2020).

Denne illustrerende analyse har vist, at de danske udvalg og råd for cybersikkerhed er domineret af mænd og individer fra den private sektor. Til trods for det begrænsede datagrundlag er konklusionerne på linje med undersøgelser fra USA og Storbritanien. Tekniske it-specifikke uddannelser er hyppige, og mange har også gennemført en lang videregående uddannelse inden for virksomhedsadministration og strategi eller politologi. Certifikater er primært udstedt af private transnationale organisationer med ISACA og "(ISC)²" som dominerende.

En ny ekspertprofil? Fra teknisk fokus til procesorientering

Til trods for en fortsat relativ høj varians blandt de undersøgte eksperters baggrunde ser vi mange af de samme uddannelsestyper og certificeringer. Samtidig er der en klar tendens, som placerer cybereksperten imellem eksisterende felter (Eyal, 2013b). Det tekniske fokus er suppleret med virksomhedsorganisatorisk og politologisk ekspertise. En mulig konsekvens er, at cybersikkerhed ikke længere anses som en ren teknisk kompetence, men snarere som et brobyggende led med et stærkt teknisk fundament. Fra et organisatorisk perspektiv vil en sådan udvikling tage cybersikkerhed fra at være et afgrænset led i driften af en organisation til en mere integreret rolle med en klar procesorientering (Ferdinand, 2015). Hvor den klassiske cybersikkerhedsekspert var en del af IT-afdelingen (Denning, 2001), har den nye profil både et bredere i fokus og befinder sig tættere på direktørniveauet.

Procesorienteringen reflekterer også en mere proaktiv tilgang til cybersikkerhed. I den tidlige profil som en del af IT-afdelingen var cybersikkerhed anset som en del af virksomheds*driften*. Fokus var på en effektiv forbedring af de defensive digitale kapaciteter med en prioritering af at holde omkostningerne nede. Det nye profil ser derimod ud til at være en del af organisations*udviklingen* og dermed ikke primært en omkostningsfaktor. Som en del af governance-ledet handler det om at udvikle en proces omkring organisationens digitale sikkerhed med det formål at segmentere essentielle data fra ikke-essentielle processer (EY, 2019: 7, 25).

Det kræver en ekspertprofil, som kan navigere på tværs af tre dimensioner. Som det første kræver det et intimt kendskab til organisationens opbygning og operationer. Business administration-uddannelsen kan forstås som en del af denne profil. Den anden dimension er en forståelse for det eksterne trusselsbillede. Hvem er vores modspillere, og hvad er tendenserne i den globale cybersikkerhedsarena? Politologiske og militære uddannelser kan placeres i denne type. Den tredje dimension er det tekniske fundament som oversætter operationelle og strategiske overvejelser til tekniske løsninger. Uddannelser indenfor kategorien computer-science i ovenstående analyse er relateret til denne dimension. En lignende udvikling blev dokumenteret for sikkerhedseksperter i private amerikanske virksomheder, hvor stillingen "corporate security officer" gik fra at være en teknisk til en strategisk rolle (Petersen, 2013: 225).

Samtidig kan udviklingen forstås som værende baseret på en ny sikkerhedsforståelse. Hvor den afgrænsede profil med fokus på tekniske løsninger er en refleksion af en forenklet sikkerhedsforståelse med klare linjer mellem trussel og sikkerhed, er den nye profil et tegn på anerkendelsen af, at absolut sikkerhed ikke er tilgængelig i den digitale sfære (Reichborn og Friis, 2016). I stedet er det nødvendigt at skabe processer, som sikrer organisationens modstandskraft i tilfælde af et cyberangreb. I sikkerhedspolitisk jargon kan det siges, at vi ser en udvikling fra en strategi baseret på "deterrence by denial" til en resiliensstrategi (Lasconjarias, 2017). Det vil sige, at en ren teknisk beskyttelse

ikke længere anses som hensigtsmæssigt i en verden, hvor dedikerede hackere altid vil finde en vej ind, hvis de har tilstrækkeligt med ressourcer. Resiliensstrategien prioriterer derimod identifikationen af en organisations essentielle formål – såkaldte kronjuveler – og adskiller dem enten fuldstændigt fra det resterende netværk eller bygger særlige sikkerhedsprocesser rundt om dem (ENISA, 2019: 16).

Den nye hybride profil (Petersen, 2013), som har et bredere i fokus og som er rykket tættere på beslutningstagere, styrker ekspertens rolle i relation til at definere risici og udforme hensigtsmæssige løsninger. Den professionssociologiske analyse fremhæver, hvordan cybersikkerhedsarbejdet foregår på en institutionel arena, hvor sikkerhedsforståelser kontinuerligt forhandles mellem eksperter i et spændingsfelt styret af økonomiske, politiske og tekniske overvejelser. Fra et samfundsmæssigt perspektiv rejser en sådan udvikling nye politiske, demokratiske og økonomiske spørgsmål. Det politisk-administrative system bliver udfordret til at etablere tværfagligt samarbejde både internt og med partnere fra private og civilsamfundsorganisationer (Pollitt, 2010). Fra et demokratisk perspektiv bliver det nødvendigt at skabe et grundlag for offentlig diskussion ved at styrke samfundets viden og bevidsthed om digitale risici og handlingsmuligheder. Her bliver det i stigende grad afgørende at skabe en ramme der styrker civilsamfundsorganisationers kapacitet til at formidle ekspertdreven debat til et bredt publikum. Staten kan understøtte denne proces ved at tilbyde gratis uddannelsesmuligheder indenfor cybersikkerhed. Storbritannien tilbyder for eksempel gratis kurser for unge og voksne med en interesse i cybersikkerhed (UK Cyber First, 2020; UK Cyber Skills Immediate Impact Fund, 2020). En sådan mekanisme kan også bidrage til at rette op på kønsfordelingen og motivere flere kvinder til at komme ind på cybersikkerhedsmarkedet. Målsætningen må være at løfte cybersikkerhedsdiskursen fra en teknificeret til en inkluderende debat, som anerkender den *politiske* kerne af forskellige handlingsmuligheder (Dunn Cavelty og Wenger, 2020).

Målsætningen må være at løfte cybersikkerhedsdiskursen fra en teknificeret til en inkluderende debat, som anerkender den politiske kerne af forskellige handlingsmuligheder

Fra et økonomisk perspektiv er cybersikkerhed et emne, som kun kommer til at vokse i betydning, og håndteringen af digitale risici koster penge. En succesfuld procesorientering kan minimere omkostningerne af cyberangreb betydeligt. Det kræver som diskuteret en ny ekspertprofil, som kan fungere som bindeled mellem tekniske, organisatoriske og strategiske overvejelser. Der er dog ingen tvivl om, at det tekniske element forbliver grundlaget for beslutninger. Derfor må der ydes en ekstra indsats for at øge bevidstheden om digitale trusler og sårbarheder på direktørniveauet, og en basal forståelse for cybersikkerhed bliver i stigende grad afgørende. Ligesom for den brede samfundspolitiske diskussion betyder dette ikke, at alle skal blive eksperter,

men det fordrer en bred anerkendelse af, at digitale risici er en fundamental bestanddel af det digitale samfund og økonomi.

Behov for politisk opmærksomhed og debat

Denne artikel har argumenteret for et stærkere fokus på vidensdannelsen og ekspertprofiler indenfor cybersikkerhedsforskningen. Organisationen og placeringen af ekspertviden inden for modne og umodne professioner kan være en vigtig faktor i udformningen af sikkerhedsforståelser på tværs af offentlige og private organisationer.

Der er en mangfoldighed af analyseredskaber til at analysere dynamiske processer mellem mikro- og makroniveauet. Her har jeg fokuseret på professionsbegrebet inspireret af Andrew Abbotts professionssociologi. Ved at fremhæve den politiske karakter af institutionaliseret viden har jeg rettet fokus imod placeringen af ekspertviden inden for et system af professioner, som står i et konkurrenceforhold til hinanden i kampen om at etablere en eksklusiv autoritet til at definere problemer og komme med legitime løsninger.

Analysen af danske cybereksperter indikerer, at politologisk og virksomhedsadministrativ viden er blevet vigtige referencepunkter for den ellers klassiske tekniske cybersikkerhedsprofil. Denne udvikling kan anskues som manifestationen på en ny sikkerhedsforståelse, som i større grad er fokuseret på organisationers modstandsevne i forhold til cybertrusler. Den nye arbejdsprofil ligger tættere på organisations*udvikling* med et fokus på at segmentere essentielle fra ikke-essentielle processer.

I takt med at cybereksperter udvider deres kontrol gennem en procesorienteret profil, er der brug for at supplere den teknificerede og ekspertdominerede cybersikkerhedsdiskurs med en demokratisk og inkluderende debat. En sådan form for demokratisk kontrol er afgørende i en tid, hvor cybersikkerhed vokser i betydning og er blevet en vigtig faktor i mange politiske og geopolitiske spørgsmål som for eksempel brugen af kryptering og udviklingen af offensive militære cyberkapaciteter.

Noter

1 Funding: Norwegian Research Council (#274740), 'The Market for Anarchy' Project.

2 Enkelte steder har det været nødvendigt at inkludere flere personer fra samme virksomhed.

3 Der findes en lang række certificeringer. ISC2[2]'s CISSP og ISACA's certificeringer er udstilt af den største professionelle organisation for hhv. cybersikkerhedseksperter og IT professionelle. ITIL er en "IT Service Management" certificering udstilt af Office for Government Commerce under det britiske finansministerie. ISO27001-certificeringen er en informationssikkerhedsstandard fra "International Organization for Standardization". Standarden er af stor betydning for virksomheder i forbindelse med cyberforsikringer for at dokumentere risiko managementprocesser.

Referencer

Aalborg Universitet (2020), »Danmarks første uddannelse i cybersikkerhed«, 29. januar www.nyheder.aau.dk/2019/nyhed/danmarks-foerste-uddannelse-i-cybersikkerhed.cid447828

Abbott, A. (1988), *The System of Professions – An Essay on the Division of Expert Labor*, The University of Chicago Press.

Abbott, A. (2005), "Linked ecologies: States and universities as environments for professions", *Sociological Theory*, 23(3): 245–74.

Allan, B.B. (2018), "From subjects to objects: Knowledge in International Relations theory", *European Journal of International Relations*, 24(4), 841–64.

Bate, L. (2018), "Cybersecurity Workforce Development: A Primer", https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_Workforce_Development_A_Primer_2018-10-31_175830_YMwa3ZJ.pdf

Bueger, C. (2014), "From Expert Communities to Epistemic Arrangements: Situating Expertise in International Relations", i Maximilian Mayer, Mariana Carpes og Ruth Knoblich, red., *International Relations and the Global Politics of Science and Technology*, Springer Verlag, pp. 39–54.

Burley, D.L., J. Eisenberg og S.E. Goodman (2014), "Privacy and security: Would cybersecurity professionalization help address the cybersecurity crisis"? *Communications of the ACM*, 57(2): 24–7.

CASE Collective (2006), "Critical Approaches to Security in Europe: A Networked Manifesto", *Security Dialogue*, 37(4): 443–87.

Christensen, K.K. og T. Liebetrau (2019), "A new role for ' the public '? Exploring cyber security controversies in the case of WannaCry", *Intelligence and National Security*, 34(3): 395–408.

Christensen, K.K. og K.L. Petersen (2017), "Public-private partnerships on cyber security: A practice of loyalty", *International Affairs*, 93(6): 1435–52.

Collier, J. (2018), "Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision", *Politics and Governance*, 6(2): 13-21.

Dawson, J. og R. Thomson (2018), "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance", *Frontiers in Psychology*, 9(june): 1–12.

Deibert, R.J. (2013), *Black code: Surveillance, Privacy, and the Dark Side of the Internet*, Signal.

Denning, P.J. (2001), "Who Are We" ? *Communications of the ACM*, 44(2): 15–19.

Denning, P.J. og D.J. Frailey (2011), "The Profession of IT. Who are we – now"? *Communications of the ACM*, 54(6): 27-9.

Digitaliseringsstyrelsen (2019), »ISO 27001-modenhed i staten«. November https://digst.dk/media/21873/iso-modenhed-i-staten-nov-2019.pdf

Domscheit-Berg, A. (2020), »Bundesregierung nimmt das Problem der IT-Sicherheit nicht ernst – Anke Domscheit-Berg", https://mdb.anke.domscheit-berg.de/2020/02/bundesregierung-nimmt-das-problem-der-it-sicherheit-nicht-ernst/

Dunn Cavelty, M. (2018), "Cybersecurity research meets science and technology studies", *Politics and Governance*, 6(2): 22-30.

Dunn Cavelty, M. og A. Wenger (2020), "Cyber security meets security politics: Complex technology, fragmented politics, and networked science", *Contemporary Security Policy*, 41(1): 5-32.

ENISA (2019), *Threat Landscape Report 2018 15 Top Cyberthreats and Trends*.

EY (2019), *EY Global Information Security Survey 2018–19 – Is cybersecurity about more than protection?* https://www.ey.com/en_gl/advisory/global-information-security-survey-2018-2019

Eyal, G. (2013a), "For a Sociology of Expertise: The Social Origins of the Autism Epidemic", *American Journal of Sociology*, 118(4): 863–907.

Eyal, Gil (2013b), "Spaces between fields," *Bourdieu and historical analysis*, pp. 158-82

Ferdinand, J. (2015), "Building organisational cyber resilience: A strategic knowledge-based view of cyber security management", *Journal of Business Continuity & Emergency Planning*, 9(2): 185–95.

Finansministeriet (2018), »National strategi for cyber- og informationssikerhed, https://fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed-2018.pdf

Ford, G. og N.E. Gibbs (1996), *A Mature Profession of Software Engineering*, CMU/SEI-96-TR-004

Fourcade, M. (2010), *Economists and Societies*, Princeton University Press.

Fourcade, M., E. Ollion og Y. Algan (2015), "The Superiority of Economists", *Journal of Economic Perspectives*, 29(1): 89–114.

Frost og Sullivan (2017), *The 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk*.

Gorwa, R. og M. Smeets (2019), *Cyber Conflict in Political Science: A Review of Methods and Literature*.

Government of the United Kingdom (2016), "National Cyber Security Strategy 2016-2021", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Government of the United Kingdom (2018), *Implementing the National Cyber Security Strategy – Developing the Cyber Security Profession in the Uk*. Retrieved from https://extranet.cranfield.ac.uk/government/uploads/system/uploads/attachment_data/file/767427/,DanaInfo=assets.publishing.service.gov.uk,SSL+Government_Response_to_Consultation_on_Developing_the_

Cyber_Security_Profession_in_the_UK_-_21_December_2018.pdf
Gracia, L. og L. Oats (2012), "Boundary work and tax regulation: A Bourdieusian View", *Accounting, Organizations and Society*, 37(5): 304–21.
Hansen, L. og H. Nissenbaum (2009), "Digital disaster, cyber security, and the copenhagen school", *International Studies Quarterly*, 53(4): 1155–75.
ISACA (2019), *State of Cybersecurity 2019 Part 1: Current Trends in Workforce Development*, www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2019-part-1_res_eng_0319.pdf?regnum=500542
ISACA (2020), "IT Certification Programs | Information Technology Certifications | ISACA", www.isaca.org/credentialing
ISC² (2019), "Cybersecurity Workforce Study – Strategies for Building and Growing Strong Cybersecurity Teams".
ISC² (2020), "Cybersecurity Certification and Training | (ISC)², www.isc2.org/about
Kremer, J. (2014), "Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace", *Information and Communications Technology Law*, 23(3): 220–37.
Krentz, N. (2014), *Ritualwandel und Deutungshoheit: Die frühe Reformation in der Residenzstadt Wittenberg (1500-1533)*, Mohr Siebeck.
Lasconjarias, G. (2017), "Deterrence Through Resilience: Nato, the Nations and the Challenges of Being Prepared", i *Eisenhower Paper, Research Division*.
Lee, R.M. og T. Rid (2014), "OMG Cyber!: Thirteen Reasons Why Hype Makes for Bad Policy", *RUSI Journal*, 159(5): 4–12.
McCarthy, D.R. (2018), "Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order", *Politics and Governance*, 6(2): 5–12.
National Research Council (2013), *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making*.
NIST (2017) *National Initiative for Cybersecurity Education (NICE) – Cybersecurity Workforce Framework*, National Institute of Standards and Technology
Pedley, D., T. Borges, A. Bollen, J.N. Shah, S. Donaldson, S. Furnell og D. Crozier (2020), *Cyber security skills in the UK labour market 2020 Findings report*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/869506/Cyber_security_skills_report_in_the_UK_labour_market_2020.pdf
Petersen, K.L. (2013), "The corporate security professional: A hybrid agent between corporate and national security", *Security Journal*, 26(3): 222–35.
Pollitt, C. (2010), "Technological Change: A Central yet Neglected Feature of Public Administration", *NISPAcee Journal of Public Administration and Policy*, 3(2): 31–53.
Reed, M.I. (1996), "Expert power and control in late modernity: An empirical review and theoretical synthesis", *Organization Studies*, 17(4): 573–97. https://doi.org/10.1177/017084069601700402
Reichborn, E. og K. Friis (2016), "From Cyber Threats to Cyber Risks", i K. Friis og J. Ringsmose, red., *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, pp. 27–44.
Seabrooke, L. og E. Tsingou (2014), "Distinctions, affiliations, and professional knowledge in financial reform expert groups", *Journal of European Public Policy*, 21(3): 389-407.
Segal, A. (2017), "Chinese Cyber Diplomacy in a New Era of Uncertainty", *Aegis Paper Series*, 1703.
Sending, O.J. (2015), *The Politics of Expertise. Competing for Authority in Global Governance*, University of Michigan Press.
Shires, J. (2018), "Enacting Expertise: Ritual and Risk in Cybersecurity", *Politics and Governance*, 6(2): 31–40.
Shires, J. og M. Smeets (2017), "Contesting 'cyber'", *New America Foundation*.
Slayton, R. og A. Clark-Ginsberg (2018), "Beyond regulatory capture: Coproducing expertise for critical infrastructure protection", *Regulation and Governance*, 12(1): 115–30.
Stevens, C. (2020), "Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet", *Contemporary Security Policy*, 41(1): 129–52.
Stevens, T. (2016), *Cyber Security and the Politics of Time*, Cambridge University Press.
Stevens, T. (2018), "Global cybersecurity: new directions in theory and methods", *Politics and Governance*, 6(2): 1-4.
Tanczer, L.M., I. Brass og M. Carr (2018), "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy", *Global Policy*, 9(3): 60–6.
Tansey, O. (2007), "Process tracing and elite interviewing: a case for non-probability sampling, "Political Science and Politics", 40(4): 765-72.
Thistlethwaite, J. og M. Paterson (2016), "Private governance and accounting for sustainability networks", *Environment and Planning C: Government and Policy*, 34(7): 1197–1221.
Trump, D.J. (2019), "Executive Order on America's Cybersecurity Workforce | The White House", 2. maj, www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/
Tsingou, E. (2014), "Club governance and the making of global financial rules", *Review of International Political Economy*, 22(2): 225–56.
UK Cyber First (2020), "CyberFirst overview. National Cyber Security Centre United Kingdom", www.ncsc.gov.uk/cyberfirst/overview
UK Cyber Skills Immediate Impact Fund (2020), "Cyber Skills Immediate Impact Fund (CSIIF) – Guidance for Applicants. Government of the United Kingdom",

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/825141/CSIIF_Third_Round_Guidance_for_Applicants.pdf

van Apeldoorn, B. og N. De Graaff (2014), "Corporate Elite Networks and us Post-Cold war Grand Strategies From Clinton to Obama", *European Journal of International Relations*, 20(1): 29–55.

Vogel, R. (2016), Closing the cybersecurity skills gap", *Salus Journal*, 4.

White House (2016), *Federal cybersecurity workforce strategy*, www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf